Log & Event Manager

Version 6.6
© 2019 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.
Table of Contents

LEM setup, configuration, and maintenance ................................................................. 29
Log in to LEM ................................................................................................................. 29
   Log in to the LEM web console ................................................................................. 29
   Supported and unsupported URLs ........................................................................ 30
   To log out of a LEM Manager .................................................................................. 30
Log in to the LEM desktop console ............................................................................. 30
Log in to the LEM admin user interface ..................................................................... 31
Log in to the LEM CMC command line interface ....................................................... 32
   CMC Access Restrictions ......................................................................................... 32
   Log in to the CMC command-line interface using the hypervisor virtual console .. 32
   Log in to the CMC command-line interface using SSH ........................................... 33
Log in to the LEM Events Console .............................................................................. 34
Set up a new LEM installation ...................................................................................... 36
Set up the first LEM Manager instance in the web console ....................................... 36
Install the LEM license using the web console ............................................................ 36
   Verify that the LEM desktop console can connect after you activate the license .... 37
Run the activate command to secure LEM and configure network settings ............... 37
   Prepare to run the Activate command .................................................................. 37
   Run the Activate command .................................................................................... 38
Use the LEM Getting Started wizards ....................................................................... 39
   Open the Getting Started wizards ...................................................................... 39
   Use the Configure Basic LEM Settings wizard to set up Active Directory monitoring and email alerts ................................................................. 40
   Use the Add Nodes wizard to add a syslog node to LEM ....................................... 42
   Use the Add Rules wizard to set up LEM rules ..................................................... 43
Configure LEM settings and services .......................................................................... 45
Start and Stop LEM components .................................................................................. 45
   Stop or restart the LEM Manager ......................................................................... 45
Start and stop the LEM Agent on Windows ................................................................. 45
Set the date, time, and time zone on your LEM VM ..................................................... 45
Manage LEM VMs and appliances in the LEM console ................................................ 47
View LEM license information ....................................................................................... 47
Enable LEM license recycling ......................................................................................... 47
Configure the settings used to log in to the LEM VM .................................................. 48
Add another LEM VM or appliance to the console ..................................................... 49
Copy data about a LEM VM or appliance ..................................................................... 51
Remove a LEM VM or appliance from the console ..................................................... 51
Configure the Email Active Response connector in LEM ........................................... 51
Requirements .................................................................................................................. 51
Configure the Email Active Response connector ........................................................ 52
Test the Email Active Response connector ................................................................... 53
Configure Active Directory and LEM to work with LEM rules and filters ................. 53
Configure the Directory Service Query Connector ....................................................... 54
Enable LEM to receive SNMP traps by turning on the SNMP Trap Logging Service .... 55
To enable or disable the LEM SNMP Trap Logging Service: ...................................... 55
Send SNMP traps from LEM to other applications by turning on the SNMP Request Service .... 56
To enable or disable the SNMP Request Service .......................................................... 57
Configure LEM to store original log messages (nDepth log retention) ....................... 58
About nDepth log retention ............................................................................................. 58
Configure LEM Manager to store original log files in their own database .................. 59
Configure connectors to send original log data to LEM ............................................. 60
View and search your original log messages ............................................................... 60
Configure the LEM event distribution policy .............................................................. 61
Practical uses for event distribution policy ................................................................. 61
Open the Event Distribution Policy window ............................................................... 61
Configure the event distribution policy ........................................................................ 62
Push event policy to lower-level event types .............................................................. 63
Export a Manager event policy ..................................................................................... 63
Collect Windows Filtering Platform (WFP) events in LEM ................................................................. 64
About Windows WFP events and LEM performance .................................................................................. 64
Configure LEM to collect WFP events (Optional) .................................................................................. 64
Manage LEM system resources .............................................................................................................. 66
Allocate CPU and memory resources to the LEM VM .......................................................................... 66
About incoming data traffic ...................................................................................................................... 66
Use the LEM console to view resource allocations and VM details ....................................................... 66
View vSphere reservation settings for LEM .............................................................................................. 68
Change vSphere reservations for LEM .................................................................................................... 68
View reservations settings using the CMC command-line .................................................................... 69
View Hyper-V reservation settings for LEM ............................................................................................ 69
Manage LEM data storage ...................................................................................................................... 70
About the three LEM data stores ............................................................................................................ 70
Strategies for managing your LEM data storage needs ......................................................................... 70
View LEM database usage numbers ....................................................................................................... 71
Create a disk usage alert in LEM to warn you when a disk reaches a set limit ....................................... 72
LEM tuning and periodic maintenance tasks .......................................................................................... 74
Integrate LEM with other SolarWinds products ...................................................................................... 76
Monitor LEM from NPM and the Orion Web Console using SNMP ....................................................... 76
Enable the SNMP Request Service .......................................................................................................... 76
Set up the Orion Web Console for SNMP monitoring ............................................................................ 76
Troubleshooting your Orion connection .................................................................................................. 78
Secure LEM ............................................................................................................................................. 79
LEM security checklists: Ensure that only authorized users can access LEM ........................................... 79
General security tasks ................................................................................................................................ 79
Secure the LEM Manager and the LEM consoles .................................................................................... 79
Secure the CMC command-line interface ............................................................................................... 79
Secure the LEM reports application ......................................................................................................... 79
Restrict SSH access to the LEM CMC interface ...................................................................................... 80
To remove access restrictions from the CMC interface .......................................................................... 80
Restrict access to the LEM reports application ................................................................. 80
Understand your options for securing LEM reports .......................................................... 80
Restrict access to LEM reports to specific computers ...................................................... 81
Remove all LEM reports access restrictions ..................................................................... 81
Enable transport layer security (TLS) in the LEM reports application ............................... 82
Enable TLS on a standalone LEM VM or appliance ............................................................ 82
Set up a dedicated LEM user for accessing reports ............................................................ 82
Configure the Reports application to use TLS ................................................................. 83
Enable TLS on a LEM Manager with a separate database appliance .................................. 84
Import certificates into the LEM Manager and database ................................................... 84
Import a self-signed certificate into the LEM Manager ...................................................... 85

Manage users in LEM ........................................................................................................ 86
Add LEM users .................................................................................................................. 86
About LEM roles ............................................................................................................... 86
About LEM user accounts ............................................................................................... 87
How Active Directory accounts work in LEM ................................................................. 87
Import an Active Directory user into LEM ......................................................................... 88
Create a local LEM user account ...................................................................................... 88
View user accounts in the LEM console .......................................................................... 90
View the system privileges associated with a role ............................................................ 90
Edit user account settings ............................................................................................... 91
Delete a user account from a LEM Manager instance .................................................... 91
Set the global password policy for LEM users ................................................................. 92
Set up Active Directory authentication in LEM ............................................................... 92
Gather required information ............................................................................................ 92
Create a user in Active Directory that LEM can use to log in ......................................... 93
Create custom security groups in Active Directory for LEM to use ............................... 93
Configure or view Active Directory authentication settings in LEM .............................. 94
Add an Active Directory user to LEM .............................................................................. 97
Set up Active Directory authentication in LEM 6.3.0 and older ....................................... 97
Configure the Directory Service Query connector ................................................................. 97
Test the Directory Service Query connector settings .......................................................... 99
Import your Active Directory organizational groups into LEM ......................................... 99
Import an Active Directory user and assign the user LEM login rights ............................ 99
Set up single sign-on in LEM .................................................................................................. 100
Set up Active Directory authentication in LEM ................................................................. 100
Generate a keytab file using Ktpass ....................................................................................... 100
Configure SSO settings in LEM using the Admin web console ........................................ 102
Configure web browser settings for SSO ............................................................................ 103
  Internet Explorer ................................................................................................................. 103
  Mozilla Firefox .................................................................................................................... 104
  Google Chrome and Opera .................................................................................................. 104
Configure LEM for either SSO-only authentication, or SSO and local authentication ....... 105
Configure SSO settings in LEM using the command-line .................................................. 106
Change the LEM CMC password ......................................................................................... 108
Recover a lost CMC password ............................................................................................. 108
Specify the filters that users assigned the Monitor role can use in the LEM console ........ 108

**Send event data to LEM via Agents, syslog, and SNMP** .................................................. 111
Get started adding systems and devices to LEM ............................................................... 111
  About the LEM Agent .......................................................................................................... 111
  About sending log events directly to LEM ......................................................................... 112
Configure LEM Agents after they are installed .................................................................. 112
  View the LEM Agents monitored by each LEM Manager ............................................... 112
  About the LEM Agent for Windows connectors ............................................................... 112
  Enable additional connectors to add extra log sources to LEM .................................... 113
Create connector profiles to manage and monitor LEM Agents ........................................ 113
  About connector profiles .................................................................................................... 113
  About the connector-profile group type .......................................................................... 114
  Connector profile guidelines ............................................................................................. 114
  Create a connector profile: process overview .................................................................. 114
Create a connector profile: detailed steps ................................................................. 115
Task 1: Configure the Agent that will serve as a template for your connector profile .... 115
Task 2: Select the Agents that are members of the profile ........................................ 116
Task 3: Verify the connector status ............................................................................ 116
Edit LEM Agent connector-profile settings ............................................................... 117
Open the connector profile settings for editing ......................................................... 117
Clone a connector-profile instance .......................................................................... 117
Editing a connector profile instance ......................................................................... 117
Edit the connector-profile settings .......................................................................... 118
Add additional connectors to a connector profile ..................................................... 120
Add syslog and Agent nodes to LEM ......................................................................... 120
  Add a syslog node to LEM using the Add Node wizard ............................................. 120
  Use Scan for New Nodes to find new syslog sources and add connectors .......... 120
  Manually add a new Agent or syslog node connector ............................................. 122
  Other ways to add nodes to LEM ........................................................................... 122
Update LEM Agents .................................................................................................. 123
  Manually update LEM Agents on Windows installations using the LEM Local Agent Installer ... 123
  Manually upgrade LEM Agents on Unix, Linux, Mac, and Windows hosts using LEM Remote Agent Installers ................................................................. 124
    Download the LEM Remote Agent Installer ......................................................... 124
    Run the LEM Remote Agent installer ................................................................ 124
Set up a separate syslog server for use with LEM ..................................................... 126
LEM connectors: Normalize events sent from specific products on your network .......... 129
Configure LEM connectors for Agent and non-Agent devices .................................. 129
Configure connectors for the devices that you want to monitor with LEM ............... 129
Configure LEM Manager connectors ....................................................................... 130
Configure the sensor and actor connectors for each LEM Agent ............................. 130
  Connectors grid icons ......................................................................................... 130
Configure Agent connectors ................................................................................... 131
Use connector profiles to configure multiple Agents ................................................. 131
常委 LEM connectors .......................................................... 131
Open a connector configuration form ..................................... 132
Open a Manager connector configuration form ......................... 132
Open an Agent's connector configuration form ......................... 132
Find a connector ................................................................. 132
Add a new connector instance .............................................. 133
Start a connector instance ................................................... 134
Stop a connector instance ................................................... 134
Edit a connector instance ................................................... 134
Delete a connector instance ................................................ 135
Apply a LEM connector update package .................................. 135
Enable global automatic connector updates ............................. 135
Update connectors on-demand ............................................. 135
Update LEM connectors manually using the CMC interface ......... 136
Troubleshooting LEM connector upgrades .............................. 137
LEM connector categories .................................................... 137

**Configure LEM to monitor firewalls, proxy servers, domain controllers, and more** .............................. 143

Configure LEM to monitor firewalls for unauthorized access ........ 143
Configure a firewall to log to a LEM appliance ......................... 143
Configure a firewall connector on a LEM Manager .................... 143
View network traffic from specific computers ......................... 144
Clone and enable a LEM rule to identify port scanning traffic ...... 145
Configure LEM to monitor proxy servers for suspicious URL access in LEM ........................................ 145
Set your proxy server to log to a virtual appliance .................... 145
Configure a proxy server connector on a LEM Manager ............... 146
Clone and enable the Known Spyware Site traffic rule ................ 146
Configure LEM to monitor anti-virus software for viruses that are not cleaned ........................................ 147
Configure antivirus software to Log to a LEM appliance ............. 147
Configure the antivirus connector on the LEM Manager ............. 147
Create a LEM rule to track when viruses are not cleaned .......... 147
Configure LEM File Integrity Monitoring (FIM) to monitor Windows files, folders, and registry keys …148

Features of FIM ............................................................................................................................................. 148

Add a FIM connector to an Agent to monitor a node .................................................................................. 148

  Task 1: Add a FIM connector to a node ...................................................................................................... 149

  Task 2: Configure rules and specific actions for your monitored files ................................................... 149

Edit a Monitor .................................................................................................................................................. 149

Promote a Monitor to a Template ................................................................................................................ 149

Delete a Monitor .............................................................................................................................................. 150

Add conditions to a directory that FIM is watching .................................................................................... 150

Edit Conditions .............................................................................................................................................. 150

Delete Conditions ........................................................................................................................................... 151

FIM connector advanced settings .................................................................................................................. 151

Enable Windows file auditing for use with LEM ............................................................................................ 152

  Enable object auditing in Windows .......................................................................................................... 152

  Enable file auditing on a file or folder in Windows ................................................................................... 153

Configure Windows audit policy for use with LEM ..................................................................................... 153

Requirements .................................................................................................................................................. 154

Windows Audit Policy .................................................................................................................................. 154

  Best practice .................................................................................................................................................. 155

  Set the Windows audit policy ...................................................................................................................... 155

  Default Domain Controllers Policy ........................................................................................................... 155

  Default Domain Policy ............................................................................................................................... 155

Configure the USB Defender local policy connector in LEM ........................................................................ 158

Configure LEM to monitor Microsoft SQL databases for changes to tables and schemas ...................... 159

  Configure your database servers ................................................................................................................ 159

  Install MSSQL Auditor on a LEM Agent .................................................................................................... 160

  Configure MSSQL Auditor on your servers .............................................................................................. 160

  Configure the MSSQL Auditor Connector on a LEM Agent .................................................................... 160

  Send notifications of Microsoft SQL database change attempts ............................................................ 161

  Configure LEM to monitor Windows domain controllers for brute force hacking attempts ................ 161
Install and configure the LEM Agent ................................................................. 162
Install a LEM Agent on a single Windows domain controller ........................... 162
Configure additional connectors on your LEM Agent .................................... 163
Create a filter for all activity in a Connector Profile ...................................... 164
Clone and enable the Critical Logon Failures rule ......................................... 164
Tune Windows Logging for LEM implementation .......................................... 165
Configure LEM to track Cisco buildup and teardown events ......................... 165
Tracking Buildup Events ............................................................................... 165
Tracking tear-down Events .......................................................................... 165
Enabling LEM to track buildup and teardown events ................................. 166
LEM groups: Organize data elements for use with rules and filters .............. 167
About LEM groups ....................................................................................... 167
About LEM Group Types ............................................................................. 167
User-defined groups ...................................................................................... 167
Event groups ................................................................................................. 168
Directory Service groups ............................................................................. 168
Time-of-day sets ........................................................................................... 168
Connector profiles ......................................................................................... 168
Email template ............................................................................................... 168
State variables .............................................................................................. 168
How groups are added to filters and rules in the LEM console .................... 169
Manage LEM groups: Add, edit, view, and more ....................................... 170
Open the Groups View in the LEM console ............................................... 170
Find a group with the Refine Results pane ............................................... 171
Add a new group .......................................................................................... 172
Edit a group ................................................................................................. 172
Clone a group .............................................................................................. 173
Export a group ............................................................................................. 173
Import a group ............................................................................................. 173
Delete a group ............................................................................................. 174
Import a filter ................................................................................................................. 201
Delete a filter .................................................................................................................. 201
Send a filter to nDepth ................................................................................................... 202
Start, stop, and pause filters in LEM ............................................................................ 202
About starting, stopping, and pausing filters ................................................................. 202
Turn a LEM filter on ......................................................................................................... 202
Turn a LEM filter off ......................................................................................................... 202
Pause one LEM filter ....................................................................................................... 203
Pause all LEM filters ....................................................................................................... 203

**LEM widgets and the Ops Center: Visually monitor network events in LEM** ........... 204
About LEM widgets ......................................................................................................... 204
Widget icons ...................................................................................................................... 204
View specific widget data ............................................................................................... 205
Refresh widget data ......................................................................................................... 205
View a widget legend ....................................................................................................... 206
Widgets that ship with the LEM console ......................................................................... 206

Manage LEM widgets with Widget Manager: Add, edit, and more ............................. 208
About the Widget Manager .............................................................................................. 208
Locate widgets ................................................................................................................ 209
Add a master widget to the dashboard ............................................................................ 209
Edit a dashboard widget ................................................................................................ 210
Delete a dashboard widget ............................................................................................. 210
Open a filter from a widget ............................................................................................. 210
Move (relocate) a widget ................................................................................................ 210
Resize a widget ................................................................................................................ 211
Create and edit widgets with Widget Builder ................................................................. 211
Create a new widget ....................................................................................................... 211
Edit a master widget ..................................................................................................... 212
Edit a dashboard widget ............................................................................................... 212
Configure the Widget Builder form ................................................................................ 213
Enter the general widget settings .......................................................... 213
Enter the visual configuration settings .................................................. 214
Enter the data configuration settings .................................................... 214

Using nDepth widgets in LEM ............................................................... 215
About nDepth widgets ........................................................................ 215
View nDepth widget details .................................................................. 216
Create a search string from a widget item .......................................... 216
Add a new nDepth widget .................................................................... 216
Edit an nDepth widget ........................................................................ 217
Add a chart widget to the nDepth dashboard ...................................... 217

LEM rules: Automate how LEM responds to events ............................... 218
About LEM rules ................................................................................ 218
LEM rule scenarios ............................................................................ 218
View rules, rule categories, and rule templates in the LEM console .......... 219
Rule configuration requirements and best practices ............................ 219
Use descriptive rule names .................................................................. 219
Set the Correlation, Correlation time, and Action ............................... 219
Activate a rule to upload local changes .............................................. 219
Check the rule status for errors .......................................................... 219
Verify that a rule fired ........................................................................ 220
Test new rules before putting them into production ............................ 220

Create email templates for use with LEM rules .................................. 220
About LEM email templates ............................................................... 220
Managing email templates and template folders ............................... 221
Best practices to keep rules, events, and emails simple to manage ........ 221
Create or edit an email template ......................................................... 221

Find and add LEM rules ...................................................................... 223
Find and add rules based on categories of interest ............................. 223
Clone, customize, and enable a specific preconfigured rule ............... 224
Change Management rule example .................................................... 225
Create a new LEM rule to monitor and respond to events ................................................................. 226
Create a new rule .......................................................................................................................... 226
Example: Create a Change Management rule ............................................................................... 229
About the Change Management rule example .............................................................................. 229
Create the example Change Management rule ............................................................................. 229

Manage LEM rules: Edit, view, export, and more ............................................................................. 230
Activate a rule .................................................................................................................................. 231
Add tags to a rule ............................................................................................................................ 231
Edit a rule ........................................................................................................................................ 231
Edit a locked rule ............................................................................................................................ 232
Clone a rule ....................................................................................................................................... 232
Share a rule with another user ........................................................................................................ 232
Create a backup copy of a rule for archival purposes .................................................................... 232
Export a rule ...................................................................................................................................... 232
Import a rule ...................................................................................................................................... 233
Delete a rule ....................................................................................................................................... 234

Test, enable, and disable rules in LEM .............................................................................................. 234
About selecting multiple rules to test, enable, or disable ................................................................. 234
Enable and activate rules prior to testing ......................................................................................... 234
Enable rules from the Rules grid ....................................................................................................... 235
Enable rules from the Rule Creation screen .................................................................................... 235
Testing rules in LEM .......................................................................................................................... 235
Enable test mode in the Rules grid ................................................................................................... 236
Disable test mode in the Rules grid .................................................................................................. 236
Enable test mode from the Rule Creation screen ............................................................................... 236
Disable test mode from the Rule Creation screen .......................................................................... 237
Disable rules in LEM to stop them from processing ...................................................................... 237
Disable rules from the Rules grid ..................................................................................................... 237
Disable rules from the Rule Creation screen .................................................................................. 238
Use the Send Email Message action in LEM rule creation ............................................................... 238
Add or edit a Send Email Message action ............................................................. 238
Notify a LEM user when a rule triggers an alert (Subscribe a user to a rule) .......... 239
Subscribe users from the Rules grid .................................................................. 239
Subscribe users from the Rule Creation screen .................................................. 240

**LEM response actions: Respond to network and system events in LEM** .................. 241

- About LEM response actions ............................................................................. 241
- About LEM active response ............................................................................... 241
- Select an event response ................................................................................... 241
- Select an event response using drag-and-drop text ........................................... 242
- Use LEM active responses to perform Windows actions related to users, groups, and domains ... 243
  - Configure an active response connector on a LEM Agent .................................. 244
- Actions LEM can take to respond to events ....................................................... 244
- Use Computer-based active responses in LEM .................................................. 253
  - Requirements .................................................................................................. 254
  - To configure the Windows active response connector on a LEM Agent .......... 254
  - Create or clone rules to perform the action: ..................................................... 254
- Use the Append Text to File active response in LEM .......................................... 254
  - Requirements ................................................................................................. 254
  - To configure the Windows active response connector on a LEM Agent: ........... 256
- Auto-populate user-defined groups using a LEM rule ......................................... 256
- Use the Block IP active response in LEM ........................................................... 257
  - Requirements .................................................................................................. 257
- Configure the Detach USB Device active response in LEM ............................... 259
  - Verify that USB Defender is installed on a LEM Agent .................................... 259
  - Configure the Windows Active Response connector on a LEM Agent ............ 259
  - Detach USB devices ......................................................................................... 260
- Configure the Disable Networking active response in LEM ............................... 260
  - Re-enable networking on a computer affected by the active response .............. 260
- Configure the Kill Process active response in LEM ............................................ 261
  - Configure a Kill Process active response rule ................................................ 261
Building custom filter and rule expressions in LEM ................................................................. 263
  Comparing values with operators in LEM filters and rules ......................................................... 263
  About operators in LEM ................................................................................................................. 263
  Select a new operator ...................................................................................................................... 263
  Operator tips .................................................................................................................................. 263
  Table of operators .......................................................................................................................... 264
  Examples of AND and OR conditions .............................................................................................. 265
Get started building custom filter expressions in LEM ................................................................. 265
  About custom filter expressions .................................................................................................... 266
  Examine the default filters included with LEM ............................................................................. 267
  Create conditions to filter event reporting .................................................................................... 267
Configure event filter notifications in LEM ..................................................................................... 269
  Selecting the notification method .................................................................................................. 269
  Notifications table .......................................................................................................................... 269
Get started building custom rule expressions in LEM ................................................................. 271
  About custom rule expressions ...................................................................................................... 271
  Use the ToolAlias field in LEM rules and filters to capture traffic from a specific device ........... 272
  Create a filter to capture events from a specific device ................................................................. 272
  Verify that the correct Alias value is associated with the connector ........................................... 273

nDepth search: Explore event history using nDepth and other LEM utilities ................................. 274
  About LEM nDepth search ........................................................................................................... 274
  nDepth visual tools ......................................................................................................................... 274
  nDepth primary uses ...................................................................................................................... 274
  Events and Log Messages ............................................................................................................. 275
  Common data fields in nDepth search ........................................................................................... 275
Open nDepth search in LEM ........................................................................................................... 275
  Open nDepth from another data source ....................................................................................... 277
Search normalized data using nDepth search in LEM ................................................................. 277
  Create an nDepth query .................................................................................................................. 278
  Choose an event in Monitor view to send to nDepth for historical search ................................. 278
Choose a filter in Monitor view to send to nDepth for historical search ................................................. 278
Create an nDepth query for all activities by a single user ................................................................. 279
Delete items from search strings ..................................................................................................... 279
Adjust the time frame for your nDepth query .................................................................................. 280
Search raw log messages using nDepth search in LEM ................................................................. 280
To view and search original log messages using nDepth .................................................................... 280
Manage nDepth search queries in LEM: Save, schedule, run on-demand, and more ................. 281
Save an nDepth search query ............................................................................................................. 281
Edit a saved nDepth search query .................................................................................................... 282
Run a saved nDepth search query on demand .................................................................................. 282
Schedule a saved nDepth search query ............................................................................................. 282
Delete a saved nDepth search query ................................................................................................ 283
Export nDepth search results in CSV format ..................................................................................... 283
Export nDepth search results in PDF format ...................................................................................... 284
Visualize search results and take action with nDepth widgets and the Respond menu in LEM .... 285
About the Explore and Respond menus ............................................................................................ 285
Respond to an event with the nDepth Respond menu ........................................................................ 285
About nDepth widgets ........................................................................................................................ 286
View widget details ............................................................................................................................. 286
Create a search string from a widget item .......................................................................................... 287
Create a new nDepth widget with nDepth Widget Builder .................................................................. 287
Edit an nDepth widget ........................................................................................................................ 287
Add a chart widget to the nDepth dashboard ..................................................................................... 288
Use the explorer utilities in LEM to search or analyze nDepth query results ................................ 288
About the Explorer utilities ............................................................................................................... 288
Open the explorer utilities from the nDepth view to investigate event details .............................. 289
Open the explorer utilities from Monitor view or the Utilities view ................................................. 289
Collect and view NetFlow and sFlow data in LEM .................................................................................. 289
About the Flow explorer .................................................................................................................... 289
Enable Flow collection and analysis in LEM ...................................................................................... 290
View Flow data in the LEM console ................................................................. 290

**LEM reports: Create reports for regulatory and compliance purposes** .......................... 291

About LEM reports ............................................................................................. 291

- LEM reports overview ...................................................................................... 291
- About report categories .................................................................................... 291
- About report levels ............................................................................................ 291
- About scheduled and on-demand reports .......................................................... 292

Open the LEM reports application ........................................................................ 292

- To automatically Run as administrator every time you run Reports .................. 292

Setting up the LEM reports application ............................................................... 292

- Configure the LEM reports application to communicate with the LEM database .......................................................... 292
- Secure the LEM reports application .................................................................. 293
- Select a default primary data source .................................................................... 294
- Configure a syslog server (optional) .................................................................... 294

The LEM reports application interface ............................................................... 295

- The Reports application features ........................................................................ 296

- Menu button ....................................................................................................... 297

- Quick Access toolbar .......................................................................................... 298
  - Default commands ............................................................................................. 298
  - Customize the Quick Access Toolbar ................................................................. 299
  - Move the Quick Access Toolbar ....................................................................... 299
  - Minimize the ribbon ........................................................................................... 300

The Preferences group .......................................................................................... 300

- Find, filter, and group LEM reports ...................................................................... 301
  - Find a LEM report by title .................................................................................. 301
  - Find reports for specific industries ..................................................................... 302
    - Industry Options ............................................................................................... 302

- View LEM report properties ................................................................................ 304

- Filter and sort LEM report lists in the reports application .................................... 304
  - Filter the report list to reduce the number of listed reports ............................... 305
Change a filter setting ................................................................. 305
Sort the report list .................................................................. 305
Turn off report filters ............................................................... 306
Manage report categories ......................................................... 306
Create a favorite LEM reports list ............................................ 307
Step 1: Search the reports ....................................................... 307
Step 2: Add a report to your Favorites tab .............................. 308
Remove a report from the Favorites tab ................................. 308
Search LEM reports for specific text ..................................... 308
View the text-based details of a report ................................... 309
Use the Search tool .................................................................. 309
Customize and share report filters in the LEM reports application ......................................................... 309
Create a custom report filter in the LEM reports application ......................................................... 310
Save a custom report filter in the LEM reports application ...................................................................... 310
Open a saved custom report filter in the LEM reports application .............................................................. 311
Categorize and display LEM reports by group .......................... 312
Create a report group in the LEM reports application ............ 312
View the reports within a group in the LEM reports application ...................................................................... 313
Create a sub-group in the LEM reports application .................. 313
Run a LEM report on-demand or schedule a LEM report to run later ......................................................... 314
Run an on-demand report in the LEM reports application .................................................................................. 314
Create a scheduled report in the LEM reports application ...... 316
Step 1: Selecting the report you want to schedule .................... 316
Step 2: Add a new scheduled report task ................................. 317
Step 3: Schedule the report ....................................................... 318
Step 4: Select the advanced scheduling options ....................... 319
Step 5: Stating when the system can or cannot run the task ............................................................................. 321
Step 6: Assign the data source and scope ............................... 322
Assign the task scope ............................................................... 323
Step 7: Export a scheduled report ............................................ 324
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove a report from the report scheduler</td>
<td>324</td>
</tr>
<tr>
<td>Configure Windows Task Scheduler to run the default LEM Batch Reports</td>
<td>325</td>
</tr>
<tr>
<td>Prepare the INI file</td>
<td>325</td>
</tr>
<tr>
<td>Schedule the Reports to Run using Windows Task Scheduler</td>
<td>325</td>
</tr>
<tr>
<td>Default Report Schedules</td>
<td>326</td>
</tr>
<tr>
<td>Edit a scheduled report in the Task Scheduler</td>
<td>327</td>
</tr>
<tr>
<td>Create a custom LEM report</td>
<td>328</td>
</tr>
<tr>
<td>Create a custom report in the LEM reports application</td>
<td>329</td>
</tr>
<tr>
<td>Export and save a copy of the filtered LEM report with a new name</td>
<td>330</td>
</tr>
<tr>
<td>Open a custom report in the LEM reports application</td>
<td>331</td>
</tr>
<tr>
<td>Use the Select Expert tool to create a more focused LEM report</td>
<td>331</td>
</tr>
<tr>
<td>View the text-based details of a report</td>
<td>332</td>
</tr>
<tr>
<td>Run a report query using the Select Expert tool</td>
<td>332</td>
</tr>
<tr>
<td>Restore the original report after using the Select Expert tool</td>
<td>333</td>
</tr>
<tr>
<td>Manage LEM reports: Open, print, and more</td>
<td>334</td>
</tr>
<tr>
<td>Open your saved reports</td>
<td>334</td>
</tr>
<tr>
<td>View the master report sections</td>
<td>335</td>
</tr>
<tr>
<td>Hide and show a master report subtopic pane</td>
<td>335</td>
</tr>
<tr>
<td>View the report pages</td>
<td>337</td>
</tr>
<tr>
<td>Magnify and reducing report pages</td>
<td>337</td>
</tr>
<tr>
<td>Stop a report in progress</td>
<td>338</td>
</tr>
<tr>
<td>Edit a scheduled report task</td>
<td>338</td>
</tr>
<tr>
<td>Export a report</td>
<td>339</td>
</tr>
<tr>
<td>Print reports</td>
<td>340</td>
</tr>
<tr>
<td>Set up your printer preferences</td>
<td>340</td>
</tr>
<tr>
<td>Set up your printer preferences</td>
<td>340</td>
</tr>
<tr>
<td>Default reports included with LEM</td>
<td>341</td>
</tr>
<tr>
<td>Scheduling terminology used in this topic</td>
<td>341</td>
</tr>
<tr>
<td>Audit reports included with LEM</td>
<td>341</td>
</tr>
<tr>
<td>Security reports included with LEM</td>
<td>363</td>
</tr>
</tbody>
</table>
## Support reports included with LEM

The LEM command-line interface: Using the CMC

- About the CMC command line
  - Special characters allowed in CMC commands and passwords
- LEM CMC main menu
- Top-Level CMC commands
- LEM CMC appliance menu
- LEM CMC manager menu
- LEM CMC nDepth menu
- LEM CMC service menu

## LEM console help

- About the LEM console
  - Console Views
  - Grids
    - Rearrange grid columns
    - Sort a grid by columns
  - LEM console grid column and data field descriptions
- Ops Center view in the LEM console
  - The User Details widgets
    - The User: Details widget
    - The User: All Events widget
  - The Node Details widgets
    - The Node: Details widget
    - The Node: Connectors applied widget
    - The Node: All events widget
  - The Widget Manager and Widget Builder
    - The Widget Manager UI
    - The Widget Builder UI
- Monitor view in the LEM console
  - The Filters pane
The nDepth view ................................................................. 418
The nDepth search view ....................................................... 418
The nDepth history pane ..................................................... 419
The nDepth filters and groups list pane ................................. 420
The nDepth search bar ....................................................... 421
The nDepth histogram ...................................................... 424
The nDepth explorer toolbar .............................................. 426
The nDepth word cloud .................................................... 427
The nDepth tree map ....................................................... 429
The Result Details view ................................................... 430
Search Builder ............................................................. 433
Manage nDepth search queries in LEM: Save, schedule, run on-demand, and more .......................... 435
The Utilities view ............................................................ 438
The Event explorer utility .................................................. 440
The Whois explorer utility ................................................ 442
nDepth explorer ............................................................ 442
The NSLookup explorer utility ........................................... 443
The Traceroute explorer utility ......................................... 443
The Flow explorer utility .................................................. 444
Execute a Whois, NSLookup, or Traceroute task from an event or search result ........................ 444
Execute a blank Whois, NSLookup, or Traceroute task ............ 444
Display flow data ........................................................... 444
Common data field categories in LEM nDepth search .............. 445
Common data field categories in Events Mode ......................... 445
Common data field categories in Log Messages mode ................. 446
Build view in the LEM console .......................................... 447
The Groups view .......................................................... 447
The Refine Results form in the Groups sidebar ....................... 448
The Rules view ............................................................ 449
The Rules grid ............................................................. 450
Configure connectors to send original log data to LEM ........................................... 494
Establish log forwarding settings .................................................................................. 495
Node management .......................................................................................................... 497
Add an agent node .......................................................................................................... 497
Start the FIM driver ......................................................................................................... 498
Add and modify connectors for agent devices ............................................................... 500
Create filters in the LEM Events Console ..................................................................... 503
Edit filters ......................................................................................................................... 505
Set maximum number of search results ....................................................................... 507
Filter and monitor events in Live Mode .......................................................................... 507
Search and filter historical event logs ........................................................................... 508
View multiple console tabs ............................................................................................. 509
Remote database (L4) configuration ............................................................................... 509

**LEM troubleshooting** .................................................................................................. 510

Troubleshoot alerts in the LEM console ....................................................................... 510
Task 1: Troubleshoot syslog devices ............................................................................... 510
Task 2: Troubleshoot device logging ............................................................................. 511
   Troubleshoot conflicting devices ................................................................................. 511
Task 3: Troubleshoot Agent devices and connectors ..................................................... 512
Task 4: Apply the latest connector update package .......................................................... 513
Task 5: Contact SolarWinds Technical Support ............................................................... 513
   Generate a syslog sample from the LEM appliance .................................................... 513

Troubleshoot the LEM desktop console ........................................................................... 513
   The LEM desktop console cannot resolve the LEM VM hostname .............................. 513
   The LEM desktop console cannot connect after you activate the license or change the LEM VM hostname ................................................................................................................................. 514

Troubleshoot LEM Agents and network devices ............................................................. 514
   Determine if LEM is receiving data from the device that you are troubleshooting .......... 514
   Troubleshoot devices not logging to a log file ............................................................. 515
   Troubleshoot devices logging to a log file .................................................................... 515
Troubleshoot a LEM Agent ................................................................. 515
Troubleshoot a missing LEM Agent .................................................. 516
Troubleshoot a disconnected LEM Agent ........................................... 516
  Edit or delete the spop.conf file ..................................................... 516
Troubleshoot a connected LEM Agent .............................................. 517
Contact SolarWinds Customer Support ............................................. 517
Troubleshoot syslog error messages in LEM ...................................... 517
  LEM console does not display syslog data ....................................... 517
    Identify your syslog data facilities containing log data .................. 518
    Configure a connector from the facility to the device .................... 519
    View the data from the device ................................................. 520
Troubleshoot LEM rules and email responses .................................... 521
  General rule troubleshooting ....................................................... 521
    The rule fires but you do not receive an email .............................. 522
    The rule does not fire and expected alerts do not display ............... 522
    Alerts display but the rule does not fire .................................. 524
    The rule fires but the email is blank ........................................ 524
      View and modify the time on your LEM appliance ....................... 525
    The rule is not triggered when it should be ................................ 525
Troubleshoot the LEM reports application ....................................... 526
  Troubleshoot the LEM reports application database connection ........... 526
  Repair the LEM reports application ............................................. 527

Glossary of LEM terms .................................................................. 528
LEM setup, configuration, and maintenance

This section describes how to set up LEM following installation, and how to configure LEM to interact with other services in your IT environment.

Log in to LEM

This section describes how to log in to the various user interfaces that you will need to work with LEM.

Log in to the LEM web console

Use the web console to manage and monitor the LEM application.

1. Open a web browser and enter the web console URL that was provided when you configured the LEM VM on either VMware vSphere or Microsoft Hyper-V, for example:
   http(s)://<IP address of LEM VM>:8080/lem/

2. Enter your user name and password.

3. Click Connect.

Only existing administrator, auditor, and monitor users can log in to LEM. Contacts cannot log in. See About LEM roles for details.
The connected icon 🔄 displays in the Status column to indicate that you are logged in to the selected Manager.

The console restores the view that was open the last time you closed the console.

- To add an additional LEM Manager instance to the console, see Add another LEM VM or appliance to the console.

When you connect to the web console for the first time, LEM prompts you to authenticate to the host Manager. If you have additional Managers associated with the console, log in to configure each Manager or view their events. When you log out, you are disconnected from additional Managers in the web console. To disconnect from the host Manager, close the browser window.

Supported and unsupported URLs

If you are using the hostname for the URL, add the LEM hostname or IP address into DNS.

- Port 8080 is unsecure and is automatically disabled after activation has been completed. Port 8443 is always available.

<table>
<thead>
<tr>
<th>SUPPORTED URLs</th>
<th>UNSUPPORTED URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>http://&lt;your_ip_address&gt;</td>
<td>https://&lt;your_ip_address&gt;</td>
</tr>
<tr>
<td>http://&lt;your_ip_address&gt;:8080/lem</td>
<td>https://&lt;your_ip_address&gt;:8443/lem</td>
</tr>
<tr>
<td>http://&lt;your_hostname&gt;</td>
<td></td>
</tr>
<tr>
<td>https://&lt;your_hostname&gt;:8080/lem</td>
<td></td>
</tr>
<tr>
<td>https://&lt;your_hostname&gt;:8443/lem</td>
<td></td>
</tr>
</tbody>
</table>

To log out of a LEM Manager

1. On the LEM toolbar, navigate to Manage > Appliances.
2. In the Appliances grid, click ⚒. next to the appliance, and then select Log out.

   The disconnected icon 🔄 displays in the Status column to indicate that you are logged out of the selected Manager.

Log in to the LEM desktop console

The optional desktop console provides the same functionality of the LEM web console in a Windows-only native app. The desktop console is used to manage and monitor LEM (same as the web console), however, the desktop console requires that you install the free Adobe AIR runtime on your computer. To learn how to install the LEM desktop console and the Adobe AIR runtime, see Install the LEM desktop console in the LEM Installation Guide.
To learn more about Adobe AIR, visit the [What is Adobe Air](#) page.
After logging in, see [About the LEM console](#) for additional console help.

1. Open the console application on your local system.
2. Enter your user name and password.
   
   Only existing administrator, auditor, and monitor users can log in to LEM. Contacts cannot log in. See [About LEM roles](#) for details.
3. Click Connect.

The console restores the view that was open the last time you closed the console.

**Log in to the LEM admin user interface**

Use the LEM admin user interface to perform the following administrator functions:

- Configure and manage LDAP and SSO settings
- Look up which Active Directory group are mapped to LEM roles.
- Enable or disable user access to the console

Use a login account in the Admin Group to log in to the LEM admin user interface.

1. Open a web browser and connect to the LEM admin user interface using the following URL:
   
   https://<lem_manager_IP_address>:8443/mvc/login

   If you have not yet activated LEM, or if you reopened port 8080, use the following URL:
   
   http://<lem_manager_IP_address>:8080/mvc/login

   You can use the command line to configure these settings by entering admin at the cmc> prompt.

2. Log in using your Active Directory credentials, or enter administrator credentials in the user name and password fields, and then click Login.

   The default user name and password is admin.
Log in to the LEM CMC command line interface

Use the CMC command-line interface (CLI) to perform administrative tasks such as:

- Rebooting or shutting down the LEM VM
- Upgrading the LEM Manager software
- Applying connector updates
- Deploying new connector infrastructure to LEM Managers and Agents

There are two ways to log in to the CMC CLI:

- Connect using the console provided with your hypervisor
- Connect using a secure shell (SSH) client such as PuTTY

CMC Access Restrictions

The following access restrictions apply to the CMC command-line interface:

- You do not need an account with root access to administer LEM from the CMC command line.
- You do not need to enter the CMC user name and password to log in to the CMC command line using the hypervisor virtual console.
- You do need to enter the CMC user name and password to log in to the CMC command line using SSH. The user name is `cmc` and the default CMC password is `password`. See [Change the LEM CMC password](#) to change it.
- SSH access to the CMC interface can be restricted by IP address or host name. If enabled, this security feature blacklists everyone from logging in to the CMC interface except those users who connect from an explicitly allowed IP address or host name. See [Restrict SSH access to the LEM CMC interface](#) for details.

Log in to the CMC command-line interface using the hypervisor virtual console

1. Open your hypervisor and connect to the LEM VM:
   - For VMware vSphere, click the Console tab, select Advanced Configuration on the main console screen, and then press Enter to access the command prompt.
   - For Hyper-V, click Action > Connect, and then click the Console tab.

   ![See your hypervisor documentation for additional information about using the virtual console.](image)

2. Use the arrow keys to navigate to Advanced Configuration and press Enter.
   The CMC menu displays with a `cmc>` prompt.

Next steps:

- See [The LEM command-line interface: Using the CMC](#) for a list of supported commands.
Log in to the CMC command-line interface using SSH

See CMC Access Restrictions for information about credentials and SSH access restrictions.

You can connect to LEM using a secure shell (SSH) client (such as PuTTY). The following steps show how to configure PuTTY to open the CMC command line, but these settings will work in any SSH client.

1. Open PuTTY and verify that Session is selected in the Category section.

![PuTTY Configuration](image)

2. Enter the following:
   - Host Name (or IP address) – Enter the IP address of the LEM VM. In this example, the IP address is 10.1.1.200.
   - Port – Enter 32022 or 22.
   - Protocol – Select SSH.
   - Saved Sessions – Enter LEM Manager, and then click Save.

3. Click Open.

   The next time, double-click LEM Manager in the Saved Session box to open the connection.

4. Log in to the appliance:
   a. At the log in as prompt, type `cmc`, and then press Enter.
   b. At the password prompt, type your password, and then press Enter.

   The default CMC password is `password`. See Change the LEM CMC password to change it. For help recovering a lost CMC password, contact SolarWinds Support.
The `cmc>` prompt opens with a list of available commands.

Next steps:
- See The LEM command-line interface: Using the CMC for a list of supported commands.

Log in to the LEM Events Console

Once LEM is set up and configured in your environment, you can access the LEM Events Console from LEM, or log in directly.

1. Open a web browser and connect to the LEM Events Console using the URL you were provided. For example, `http://10.199.129.1:8080/webui/#/auth`.

2. Enter your user name and password, and then click Login.

   If SSO is enabled, you can log in using your Windows credentials. Clear the Login using SSO Key check box to access the console via user/password authentication.
Login using SSO Key

SSO Key allows you to log in using your Windows credentials. » Learn more
Set up a new LEM installation

Set up the first LEM Manager instance in the web console

Follow this procedure to set up the initial LEM Manager instance in the console. To add additional LEM Manager instances to LEM, see Add another LEM VM or appliance to the console.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   When you start the console for the first time, the Manage > Appliances view opens so that you can configure the LEM Manager instance.
   If the Appliances view did not open, navigate to Manage > Appliances.
2. Add the LEM Manager instance to the Console.
3. Log in to the LEM Manager through the Console.
4. Configure the Manager properties by completing the Properties form.
5. Configure the Manager connectors with the Connector Configuration window.
6. (Optional) Assign the Manager alert distribution policy with the Event Distribution Policy window.

Install the LEM license using the web console

This section describes how to install the license in LEM.

See Choose a licensing method for your LEM deployment in the LEM Installation Guide to learn how LEM is licensed.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in with Administrator privileges.
2. On the LEM toolbar, navigate to Manage > Appliances, and then click the License tab in the Properties area.
3. Select the LEM Manager to be licensed in the Appliances grid.
4. Enter the License Key in the Key field.
5. Enter your name, email address, and phone number in the appropriate fields.
6. Click Activate.
7. When prompted, click OK to activate your license.

See also:

- View LEM license information
- Enable LEM license recycling
Verify that the LEM desktop console can connect after you activate the license

If you are using the optional LEM desktop console, the console automatically tries to reconnect to the LEM Manager after you activate the license.

If the desktop console cannot connect, see Troubleshoot the LEM desktop console for troubleshooting steps.

**Next steps:**

- See Run the activate command to secure LEM and configure network settings

Run the activate command to secure LEM and configure network settings

You can still evaluate LEM without running the activate command. You can also turn off HTTP.

Run the Activate command after you install the license (see install the LEM license using the web console for help). This command will help secure LEM from unauthorized users.

The activation procedure prompts you to complete the following tasks:

- Configure a static IP address and hostname for the LEM VM
- Configure a secure password
- Lock down web port 8080 and redirect access to port 80 for increased security
- Verify your network configuration
- Specify a list of IP addresses that can access LEM reports (optional)
- Export the SSL certificate that ensures secure communications between the LEM desktop console and the LEM Manager

Port 8080 is unsecure and is automatically disabled after activation has been completed. Port 8443 is always available.

Prepare to run the Activate command

If you plan to use the LEM desktop console, copy the LEM CA SSL certificate to the Trusted Root Certification Authorities certificate store prior to running the Activate command.

By default, LEM uses a pre-made, self-signed certificate.

When the activation is complete, the LEM VM automatically exports the SSL certificate, and the LEM desktop console connects with the LEM Manager using secure communications on port 8443.

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
   The default password is password.
2. At the cmc> prompt, type manager.
3. At the cmc::manager> prompt, type exportcert.
This command exports the CA certificate so that you can import it into a computer running the LEM console.

4. Follow the prompts to export the LEM Manager CA certificate.
   An accessible network share is required. Once the export is successful, you will see the following message: *Exporting CA Cert to \server\share\SWICAer -hostname.crt ... Success.*

5. Locate and double-click the certificate on the network share.

6. Click Next, and then select Place all certificates in the following store.

7. Click Browse.

8. Select Trusted Root Certification Authorities, click OK, and then click Next.

9. Click Finish.

10. Click Yes to confirm that you trust the certificate.

Run the Activate command

1. Open the CMC command line. See [Log in to the LEM CMC command line interface](#) for steps. The default password is password.

2. Configure LEM to use a static IP address:

   SolarWinds recommends configuring a static IP address for the LEM VM. If you use DHCP instead and your IP address changes, your deployed Agents may be disconnected and require additional troubleshooting to resolve.

   a. At the `cmc> prompt, type appliance, and then press Enter.`
      The prompt changes to `cmc::appliance>` to indicate that you are in the appliance configuration menu.

   b. Type `activate`, and then press Enter.
      The Activation splash screen opens.

   c. To go to the next screen, press Enter.

   d. When prompted, select Yes to configure a static IP address for the LEM VM.

   e. At the `cmc::appliance> prompt, type netconfig, and then press Enter.`

   f. At the prompt, type `static`, and then press Enter.

   g. Follow the steps on your screen to configure the Manager Appliance network parameters.

      Be sure to enter a value for each prompt. Leaving blank entries results in a faulty network configuration that requires you to rerun `netconfig`.

   h. Record the IP address assigned to the LEM VM. You will use this IP address to log in to the LEM console.

3. When prompted to change the hostname, select either Yes to specify a hostname, or No to accept the default hostname. To specify a hostname, use the following naming conventions:
- Hostname labels can only contain the following:
  - ASCII letters A through Z (letters are not case sensitive)
  - Digits 0 through 9
  - Hyphens (-)

- Hostnames cannot start with a digit or a hyphen, and must not end with a hyphen.
- No other symbols, punctuation characters, or white spaces are permitted.

4. When prompted to specify a list of IP addresses that can access reports, SolarWinds recommends selecting Yes.

5. Confirm your network configuration.
   a. To confirm your network configurations, enter `viewnetconfig at the cmc::appliance>` prompt.

   To ensure secure communications between LEM and the LEM desktop console, the LEM VM automatically exports an SSL certificate when the activation completes. Following activation, the LEM desktop console securely connects with the LEM VM on port 8443.

   b. Follow the prompts to export the certificate to a network share.

**Use the LEM Getting Started wizards**

The LEM Getting Started wizards guides you through a series of setup tasks, including:

- Mail server integration
- Active Directory monitoring
- Adding additional devices and systems that LEM should monitor, such as firewalls and user workstations
- Basic rules setup that defines how LEM alerts you when specific conditions occur on your network

**Open the Getting Started wizards**

1. Open the LEM web console. See [Log in to the LEM web console](#) for steps.
2. On the LEM toolbar, click Ops Center.
   By default, the Getting Started widget is on the top left part of the page.
3. Choose from the following:

- To connect LEM to your mail server and Active Directory, click Configure Basic LEM Settings. See Use the Configure Basic LEM Settings wizard to set up Active Directory monitoring and email alerts for details.
- To open the Add Node(s) wizard, click Add Nodes to Monitor. See Use the Add Nodes wizard to add a syslog node to LEM for details.
- To open the Add Rules wizard, click Define Rules and Configure Alerts. See Use the Add Rules wizard to set up LEM rules for details.
- To watch instructional videos about filters, reports, nDepth searches, custom rules, and more, click Advanced LEM Tools.

Use the Configure Basic LEM Settings wizard to set up Active Directory monitoring and email alerts

Use this wizard to connect LEM to:

- Your mail server so that LEM can send out email alerts
- Active Directory so that LEM can alert you to changes in your AD groups and also monitor AD accounts

Set up LEM to send Email Alerts

Configure email alerting so that users receive email alerts when assigned alert events occur. LEM can connect to an email server or SMTP relay server to forward email notifications. If you already configured email alerts, click Skip to go to the Configure Active Directory Connection screen.

You will need the following information to complete this task:

- The IP address or hostname of your primary or relay email server
- A valid email address you can use for testing
1. If you have not yet done so, open the Configure Basic LEM Settings wizard so the Configure Email Alerting screen is displayed. See Open the Getting Started wizards for help.

2. Complete the form:

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Host</td>
<td>Enter the name or IP address of your SMTP mail server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number your SMTP server uses if it does not use port 25.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Enter the protocol for sending outbound email messages from LEM Manager to the email server. Choose from SMTP, SSL, or TLS.</td>
</tr>
<tr>
<td></td>
<td>If you choose SSL or TLS, be sure to enter the correct port number in the port field. SolarWinds strongly recommends using TLS or SSL if you use a third-party email server.</td>
</tr>
<tr>
<td>Return Address</td>
<td>Enter a return email address that is appropriate for your domain, for example <a href="mailto:noreply@example.com">noreply@example.com</a>,</td>
</tr>
<tr>
<td>Return Display Name</td>
<td>Enter an appropriate display name for email messages sent from LEM Manager. For example, you can enter System Alert or Security Alert.</td>
</tr>
<tr>
<td>Authentication Server User Name</td>
<td>If your email server requires you to authenticate before you send an email, or if you use a third-party service such as Microsoft Office 365, enter the user account that LEM Manager can use to authenticate to your email host.</td>
</tr>
<tr>
<td>Authentication Server Password</td>
<td>Enter the password for the user account.</td>
</tr>
</tbody>
</table>

3. If you are using a secured email server, add the LEM VM IP address as an authorized source.

4. To test your settings, click Test Connection.

   Email alerting is properly configured if you receive a SolarWinds test message.

5. To go to the Configure Active Directory Connection screen, click Next.

See also:
- Troubleshoot LEM rules and email responses

Set up LEM to monitor Active Directory Accounts

Complete this configuration so that LEM can monitor Active Directory (AD) accounts and alert you to changes to AD accounts and groups. After completing the form, LEM will establish an LDAP connection to your Active Directory server and import your organizational groups.
This configuration step allows LEM to monitor Active Directory accounts. It does not allow users to log in to LEM with their Active Directory credentials. See Set up Active Directory authentication in LEM to configure LEM for Active Directory authentication.

1. Be sure that the Configure Basic LEM Settings wizard is open and the Configure Active Directory Connection screen is displayed. See Open the Getting Started wizards for help.

2. Complete the form:

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Enter the fully-qualified domain name of the Active Directory server.</td>
</tr>
<tr>
<td>Directory Service Server</td>
<td>Enter the IP address or host name of the Active Directory server. This server is commonly the domain controller.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the user account that LEM Manager should use to authenticate to Active Directory if authentication is required to connect to the server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the account.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Choose &quot;TLS&quot; or &quot;SSL&quot; if the Active Directory server supports encryption. Otherwise, choose &quot;No SSL&quot; to leave communications unencrypted.</td>
</tr>
<tr>
<td>Custom Port</td>
<td>If using a non-standard port number, enter it here.</td>
</tr>
</tbody>
</table>

3. To test your settings, click Test Domain Connection.
   If the test is successful, the Active Directory connection is now enabled.

4. Click Finish.

Use the Add Nodes wizard to add a syslog node to LEM

The Add Nodes wizard steps you through adding a network device node to LEM.

1. In the Getting Started wizards section, click Add Nodes to Monitor. See Open the Getting Started wizards for help.

2. Select syslog from the Select node type menu.

   The Add Node(s) screen appears.

3. Complete the form:
   a. Provide node information. Enter either the IP address or the hostname of the syslog node that you are adding to LEM, then select a name from the Vendors list.
   b. Configure node so LEM can receive its Syslog messages. Follow the onscreen steps and select the I have configured this node so that LEM can receive its Syslog messages check box.
   c. Click Next.

   LEM scans for new devices and the Nodes Found tab opens.

   See Add syslog and Agent nodes to LEM for information about adding other types of nodes.
See also:

- Troubleshoot syslog error messages in LEM

Use the Add Rules wizard to set up LEM rules

The Add Rules wizard guides you through the following tasks, which are required to enable bulk basic rules:

- Set up email actions
- Set up email alert recipients
- Set up rule categories. The wizard suggests important rules to enable.

Add a rule with the Add Rules Wizard

1. Click Define Rules and Configure Alerts to open the wizard. See Open the Getting Started wizards for help.

   ![Add Rules wizard](image)

   You can also open the LEM rules wizard by choosing Build > Rules and clicking Add Rules in the Rules area.

2. Select the rules categories you wish to use from the Rules Category screen, and then click Next.
3. Select the rules to add within the chosen categories, and then click Next.

4. Configure your Email Server Settings if you have not already done so previously. See Set up LEM to send Email Alerts for more information.

5. Select the email recipients, and then click Next.

6. Review the rules summary page for all rule categories, and then click Finish.

See Find and add LEM rules for more information about adding rules.
Configure LEM settings and services

This section describes how to configure LEM to interact with the other systems and services in your IT environment.

See [Send event data to LEM via Agents, syslog, and SNMP](#) to learn how to configure LEM to receive log events from other systems and services in your IT environment.

Start and Stop LEM components

Follow these procedures to start and stop the LEM Manager and the LEM Agents.

Stop or restart the LEM Manager

These steps also apply to the LEM VM and LEM appliance.

![Warning](https://via.placeholder.com/150)

Do not right-click the host and choose power off or shutdown guest. You can corrupt the LEM database and file system if you do not shut down LEM properly.

1. Open the CMC command line. See [Log in to the LEM CMC command line interface](#) for steps.
2. Type `appliance` at the `cmc>` prompt.
3. Choose from the following:
   - To shut down the VM:
     a. At the `cmc::appliance>` prompt, type `shutdown`.
     b. Follow the commands to shut down the LEM VM.
   - To restart the VM:
     a. At the `cmc::appliance>` prompt, type `reboot`.
     b. Follow the commands to restart the LEM VM.

Start and stop the LEM Agent on Windows

1. Press the Windows key + R to open the Run dialog box.
2. Type `services.msc`, and then press Enter.
   The Services window opens.
3. Scroll down and select SolarWinds Log and Event Manager Agent.
4. To stop or start the service, click the Stop or Start buttons near the top of the window.

Set the date, time, and time zone on your LEM VM

This topic describes how to synchronize the date and time settings on the hypervisor and the LEM VM.

The LEM VM is configured to synchronize with the hypervisor date and time by default. If the time is off by more than five minutes, the LEM rules will not operate properly.
1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.

2. Update the time zone in your LEM Manager.
   a. At the `cmc>` prompt, type `appliance`, and then press Enter.
   b. At the `cmc::appliance>` prompt, type `dateconfig`, and then press Enter.
   c. Press Enter, and then enter the current date in month/day/year format (MM/DD/YYYY).
   d. At the `cmc::appliance>` prompt, type `tzconfig`, and then press Enter.
   e. To configure the time zone, press Enter, and then follow the onscreen prompts.
   f. At the `cmc::appliance>` prompt, type `exit`, and then press Enter to return to the main menu.

3. Update the time in your hypervisor.
   a. At the `cmc>` prompt, type `manager`, and then press Enter.
   b. At the `cmc::manager>` prompt, type `viewsysinfo`, and then press Enter.

   The system information info displays.

<p>|</p>
<table>
<thead>
<tr>
<th>Virtualization Platform: VMware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock</td>
</tr>
<tr>
<td>Synchronization : Enabled</td>
</tr>
<tr>
<td>Hypervisor Time : 6 May 2016 09:07:31</td>
</tr>
<tr>
<td>Guest Time : Fri May 6 09:07:31 2016</td>
</tr>
</tbody>
</table>

   c. Using the keyboard, scroll down to Hypervisor Time and change the date and time so they match the date and time in the LEM Manager.

   ➨ Press h for help with moving and line editing commands.

   d. Using the keyboard, scroll down to Guest Time and ensure that the date and time matches the same settings in the LEM appliance.

4. Type `Exit`, and then press Enter.

5. To exit the CMC interface, type `Exit`, and then press Enter again.
Manage LEM VMs and appliances in the LEM console

This section describes how to use the console to manage one or more LEM Managers or LEM VMs.

View LEM license information

Use the following steps to view LEM license information.

See Choose a licensing method for your LEM deployment in the LEM Installation Guide to learn how LEM is licensed.

Each time you create a VM desktop, an Agent connects to LEM and allocates a license. This process repeats as desktops are added or removed.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. In the Appliances grid, select a LEM Manager (LEM VM instance).
4. In the Properties pane, click the License tab.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Nodes</td>
<td>Displays the total number of nodes allowed by your SolarWinds LEM license.</td>
</tr>
<tr>
<td>Total Unused Nodes</td>
<td>Displays the number of unallocated nodes.</td>
</tr>
<tr>
<td>Total Agent Nodes</td>
<td>Displays the number of nodes allocated to LEM agent devices (such as workstations or servers).</td>
</tr>
<tr>
<td>Total Non-Agent Nodes</td>
<td>Displays the number of nodes allocated to non-agent devices (such as firewalls and switches).</td>
</tr>
<tr>
<td>Maintenance Expiration Date</td>
<td>Displays the date your current maintenance contract with SolarWinds Support expires.</td>
</tr>
</tbody>
</table>

The Properties pane refreshes automatically when the LEM Manager is updated. This ensures that you are looking at the most current information.

Enable LEM license recycling

License recycling allows you to collect and reuse licenses from nodes that have not sent an event to the LEM Manager within a specified amount of time.

1. Go to the LEM license tab as described in the previous task (view LEM license information).
2. Select the Enable license recycling check box, and then complete the form.
3. Select a defined time frame to recycle the license when a node has not sent an event.
4. Select the time and day to check for recyclable licenses.
5. Click the Nodes to check drop-down list and select an option.
6. Click Update License.

Configure the settings used to log in to the LEM VM

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. In the Appliances grid, select a LEM Manager (LEM VM instance).
4. In the Properties pane, click the Login tab.
5. Edit the form fields and click Save.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the user name to log in with if configuring the console to log in automatically.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password if configuring the console to log in automatically. Leave this field empty if you want the console to prompt for a password when logging in.</td>
</tr>
<tr>
<td>Login Automatically Next Time</td>
<td>Automatically log in to the Manager when you open the console. Clear this check box if you prefer to log in manually.</td>
</tr>
<tr>
<td>Save Credentials</td>
<td>Enable the console to save the LEM Manager user name and password locally. If the Login Automatically Next Time check box is selected, the console will automatically log on to the Manager when the console is started. Otherwise, the console automatically provides the user name and password when you manually log in to the Manager.</td>
</tr>
<tr>
<td>Reconnect on disconnection</td>
<td>Enable the console to reconnect with the LEM Manager when the Manager is disconnected for any reason.</td>
</tr>
<tr>
<td>/ Try to reconnect every n</td>
<td></td>
</tr>
<tr>
<td>seconds</td>
<td></td>
</tr>
<tr>
<td>Timeout reconnection attempts after n tries</td>
<td>Select to have the Console quit its reconnection attempts with the LEM Manager after a given number of tries, especially if the previous connection attempts were unsuccessful.</td>
</tr>
</tbody>
</table>
Add another LEM VM or appliance to the console

See Set up the first LEM Manager instance in the web console if you are configuring LEM for the first time.

- If your deployment requires multiple Managers, use a unique hostname for each instance to ensure proper event flow and console function. SolarWinds recommends giving each Manager a unique name before adding it to your LEM system.
- Completing these steps will add the LEM VM or appliance to both the web console and the desktop console.

1. If adding a physical LEM appliance, locate and record the appliance serial or registration number. This information is required for a future step.
2. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
3. On the LEM toolbar, navigate to Manage > Appliances.
4. On the Appliances toolbar, click +.
   The Connect to SolarWinds Log & Event Manager Appliance form opens.

5. Complete the fields in the form.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name or IP</td>
<td>Enter the LEM VM name or IP address.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user name to log in with.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the account.</td>
</tr>
<tr>
<td>Login on console startup</td>
<td>Select to automatically log in to LEM when the console is started.</td>
</tr>
<tr>
<td>Save Credentials</td>
<td>Select to save the login user name and password.</td>
</tr>
<tr>
<td>Appliance Type</td>
<td>Select the appropriate LEM Manager or server.</td>
</tr>
</tbody>
</table>
| Connection Port              | Enter the port number used by the console to communicate with the Manager network appliance or database. 
The secure port number is 8443. This value defaults to 8080 for virtual appliances in the evaluation phase. This field only applies when the Appliance Type is Manager. |
| Model                        | Select Virtual if LEM is deployed as a VM, or select the appropriate appliance model (applies to older versions of LEM). 
If you don't know the model type, select Unknown. If your model type does not appear in the drop-down list, select Other. Your selection will not impact Manager operations. If you selected a listed model type, an image of the appliance displays in the Details pane. |
| Level                        | This option does not apply if LEM is deployed as a VM. If you are adding a physical appliance, select the appliance level. This value is related to the appliance capacity and performance. If you are not sure which level to choose, select Unknown. |
| Service Tag                  | Enter the LEM appliance serial or registration number. This number uniquely identifies this piece of equipment and its specific configuration properties. |
| Icon Color                   | Select the desired color for your icon.                                     |

6. To add the appliance and close the form, click Connect.

7. Enter the virtual appliance IP address, and then click Connect.

8. When the installation is complete, change your LEM password.

   The LEM desktop software requires that you change your LEM password after installation. This password must be between 6 and 40 characters, and must contain at least one capital letter and one number. The default user name is Admin and the password is Password.

   See Set the global password policy for LEM users to learn about minimum password requirements in LEM.

9. Click OK.

   The VM or appliance is added to the console.
Copy data about a LEM VM or appliance

To copy data about a LEM instance to your computer's clipboard, complete these steps. You can paste the data into another application for analysis (Microsoft Excel, for example), or the Remote Agent Installer for updates.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. In the Appliances grid, select the appliances you want to copy.
4. Click in the Appliances toolbar and select:
   - Copy Selected: Copy the data for the selected appliances
   - Copy All: Copy the data for every appliance in the grid

   The appliance data is copied to your clipboard and can now be pasted into another application.

Remove a LEM VM or appliance from the console

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. In the Appliances grid, select the appliance you want to remove.
4. Click , and then select Delete.
5. At the confirmation prompt, click Yes to remove the VM/appliance.

   The VM/appliance is removed from the Appliances grid.

Configure the Email Active Response connector in LEM

Configure the Email Active Response connector in your LEM Manager to send automated emails to console users when a rule is triggered. This connector specifies the SMTP Relay mail host that your Manager uses to send emails and provides the requisite server credentials.

If you used the LEM Getting Started Wizard to set up your LEM environment, then the Email Active Response connector is already configured. See Set up LEM to send Email Alerts for more information.

Requirements

- An email server that allows LEM Manager to relay email messages through it
- IP address or hostname of your email server
- A return email address for bounced messages and replies
User credentials for your email server, only if your email server requires internal users to authenticate to send email

To configure LEM to use Office 365 as a mail host, see Configure LEM to send email via Office 365 in the SolarWinds Success Center.

Configure the Email Active Response connector

1. Log in to your LEM console as an administrator.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. Next to your LEM Manager, click , and then select Connectors.
4. In the Refine Results search box, enter Email Active Response.
5. Next to the master connector, click , and then select New.
6. Complete the fields in Email Active Response window.

<table>
<thead>
<tr>
<th>Email Active Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias: Email Active Response</td>
</tr>
<tr>
<td>Mail Host:</td>
</tr>
<tr>
<td>Port:</td>
</tr>
<tr>
<td>Transport Protocol: SMTP</td>
</tr>
<tr>
<td>Return Address: <a href="mailto:noreply@solarwinds.com">noreply@solarwinds.com</a></td>
</tr>
<tr>
<td>Return Display Name: SolarWinds</td>
</tr>
<tr>
<td>Authentication Server Username:</td>
</tr>
<tr>
<td>Authentication Server Password:</td>
</tr>
<tr>
<td>Test E-mail Address:</td>
</tr>
</tbody>
</table>

a. In the Alias field, enter a connector name.
b. In the Mail Host field, enter the mail host IP address.
   If you use a hostname in the Mail Host field, LEM Manager must be able to resolve the mail host from the DNS entries you entered during your LEM network configuration.
c. In the Port field, enter 25.
d. From the Transport Protocol drop-down list, select SMTP.
e. In the Return Address field, enter a return address.

This field is pre-populated with noreply@solarwinds.com. Be sure to change this email address.
f. If the email server requires an Active Directory user to send email, enter the authentication
server username and password in the appropriate fields.

If the email server requires an email to be sent from a computer within the domain, the email server must have an exception created for the LEM hostname. LEM cannot join the domain.

g. In the Test Email Address field, enter a valid email address.

You can click and generate a test email after you configure and start the connector.

7. Click Save.
8. In the Connector window Status column, locate the new connector.
9. Next to your connector, click , and then select Start.

A indicates that the connector is running.

Test the Email Active Response connector

Send a test email to verify that the connector is working properly.

- If you receive an email, the connector is working properly.
- If you do not receive an email, the LEM Internal Events filter provides the following information:
  - Event Name: InternalInfo
  - Event Info: Email notification failed
  - Extraneous Info: Information about the failure. For example, server not reachable, authentication issue, and so on.

Modify the connector configuration as required and then resend a test email.

See also:

- Troubleshoot LEM rules and email responses

Configure Active Directory and LEM to work with LEM rules and filters

This section describes how to set up LEM to connect with Active Directory so that you can use Active Directory groups containing user and computer accounts with LEM rules and filters.

LEM groups that synch with Active Directory are called directory service groups (or DS groups). DS groups are only available on LEM Manager instances that complete the following integration steps.

After you complete these integration steps, see Configure directory service groups in LEM to learn how to manage DS groups.
Configure the Directory Service Query Connector

Complete these steps on the LEM Manager that will implement DS groups.

Before you begin, gather the following information to configure the Directory Service Query Connector:

- Either the IP address or fully-qualified domain name (FQDN) of the Active Directory server.
- The domain credentials for an account that the Directory Service Query connector can use. SolarWinds recommends using a service account with a non-expiring password. This account does not need elevated privileges (such as Domain Admin privileges).

To get directory server details, open a Windows command prompt on a computer on the correct network and type `nslookup`.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. Next to the LEM Manager, click the gear icon, and then select Connectors.
4. In the search box in the Refine Results pane, enter Directory Service Query.
5. Next to the master connector, click the gear icon, and then select New.
   a. In the Domain Name field, enter the fully-qualified domain name for your directory service server using lowercase characters. For example, `solarwinds.com`.
   b. In the Directory Service Server field, enter the IP address or hostname of your directory service server. SolarWinds recommends using the IP address to avoid possible DNS issues. The LEM network configurations (netconfig) allow for setting or changing the DNS server to resolve the host.
   c. Enter the domain credentials for a user account that the connector can use. SolarWinds recommends using a service account with a non-expiring password, otherwise you will have to manually update the connector every time the password expires. This account does not need elevated privileges. When entering domain credentials, provide only the user name.
   d. Enter the domain credentials for a user account that the connector can use. SolarWinds recommends using a service account with a non-expiring password, otherwise you must manually update the connector every time the password expires. This account does not need elevated privileges. When entering domain credentials, provide only the user name.
7. When finished, click Save.
8. Locate the new instance of the connector. The gray icon in the Status column indicates that the connector is not running.
9. Next to the new connector, click 📅, and then select Start. A green icon in the Status column indicates that the connector is running.
To test the connector settings, click the Test Domain Connection button. Test results are displayed as an alert in the SolarWinds Alerts filter. The test does not display a pop-up message.

**Next steps:**
See [Configure directory service groups in LEM](#) to learn how to sync Active Directory groups with DS groups.

Enable LEM to receive SNMP traps by turning on the SNMP Trap Logging Service

Turn on the SNMP Trap Logging Service to enable LEM to receive SNMP traps from devices and applications on your network. LEM can correlate events sent as SNMP traps from devices that have a device-specific connector.

LEM can also correlate performance alerts sent as SNMP traps from the following SolarWinds solutions:

- Network Performance Monitor (NPM)
- Server & Application Monitor (SAM)
- Virtualization Manager (VMan)

The SNMP Trap Logging Service must be enabled to correlate events sent by these SolarWinds products.

- LEM receives SNMP traps on port 162.
- The SNMP Trap Listening Service was renamed to the SNMP Trap Logging Service in LEM version 6.3.0.

**See also:**
- To configure LEM to output SNMP traps, turn on the SNMP Request Service. See [Send SNMP traps from LEM to other applications by turning on the SNMP Request Service](#) to learn how.
- To configure LEM to communicate with NPM and the Orion Web Console, see [Monitor LEM from NPM and the Orion Web Console using SNMP](#).

Complete the following steps to enable (or disable) the SNMP Trap Listening Service in LEM.

**To enable or disable the LEM SNMP Trap Logging Service:**

1. Open the CMC command line. See [Log in to the LEM CMC command line interface](#) for steps.
2. At the cmc> prompt type:
   ```
   service
   ```
3. At the cmc::service> prompt type:
   ```
   snmp
   ```
   A prompt like the following appears:
   ```
   SNMP Trap Logging Service is DISABLED
   Would you like to ENABLE the SNMP Trap Logging Service? [Y/n]
   ```
If the service is running, the prompt displays:
SNMP Trap Logging Service is RUNNING
Would you like to STOP the SNMP Trap Logging Service? [Y/n]

4. Type Y or n, and then press Enter.
The SNMP Trap Logging Service is configured.

5. Next, a prompt similar to the following appears:
SNMP Request Service is DISABLED
Would you like to ENABLE the SNMP Request Service? [Y/n]

The SNMP Request Service is not the same as the SNMP Trap Logging Service:
- The LEM SNMP Request Service sends SNMP traps outside of LEM
- The LEM SNMP Trap Logging Service receives SNMP traps from other devices. See Send SNMP traps from LEM to other applications by turning on the SNMP Request Service for more information.

Type Y or n, and then press Enter.
- If you enabled the SNMP Trap Logging Service, the following message appears:
The SNMP Trap Logging Service is started.
- If you disabled the SNMP Trap Logging Service, the following message appears:
The SNMP Trap Logging Service is stopped.

6. At the cmc::service> prompt, type exit.
7. To log out and close the CMC command-line, type exit again.

Send SNMP traps from LEM to other applications by turning on the SNMP Request Service

Turn on the SNMP Request Service to allow LEM to output SNMP traps to one or more applications on your network. Starting with version 6.3.0, LEM supports SNMP version 2 and SNMP version 3.

The SNMP Request Service must be turned on in LEM to do the following:
- Send SNMP traps to devices when LEM rules fire.
- Use NPM and the SolarWinds Orion Web Console to monitor LEM system resources such as CPU and memory.

- If you use SolarWinds Network Performance Monitor (NPM) in your environment:
  1. Enable the SNMP Request Service using the steps on this page.
  2. See Monitor LEM from NPM and the Orion Web Console using SNMP to set up the Orion Console for SNMP monitoring.
- To configure LEM to receive SNMP traps, see Enable LEM to receive SNMP traps by turning on the SNMP Trap Logging Service for steps.
To enable or disable the SNMP Request Service

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. At the cmc> prompt type:
   service
3. At the cmc::service> prompt type:
   snmp
   A prompt like the following appears:

   SNMP Trap Logging Service is DISABLED
   Would you like to ENABLE the SNMP Trap Logging Service? [Y/n]

   The SNMP Trap Logging Service is not the same as the SNMP Request Service. The LEM SNMP Trap Logging Service receives SNMP traps from other devices, whereas the LEM SNMP Request Service outputs SNMP traps outside of LEM. See Enable LEM to receive SNMP traps by turning on the SNMP Trap Logging Service for more information.

4. Do not change the status of this service unless you know what you are doing.
   To go to the next step, type Y or n, and then press Enter.
   A prompt like the following appears:

   SNMP Request Service is DISABLED
   Would you like to ENABLE the SNMP Request Service? [Y/n]

5. To enable or disable the service, type Y or n, and then press Enter.
   If you enabled the SNMP Request Service, the following prompt appears:

   Enter the port number to access SNMP on LEM (default: 161):

6. Type the port number that LEM should use to communicate with SolarWinds Network Performance Manager (NPM), and then press Enter.
   Ports 161 and 162 are standard.
   The following prompt appears:

   Enter the username to access SNMP on LEM (default: orion):

7. Type the user name to use, and then press Enter.
The following prompt appears:

Enter the password hashing algorithm (SHA1, MD5 or NO for no authentication, default: SHA1):

8. Enter an option, and then press Enter.

The following prompt appears:

Enter the authentication password (default: orion123):

9. Type the password, and then press Enter.

The following prompt appears:

Enter the communication encryption algorithm (AES128, DES56 or NO for no encryption, default: AES128):

10. Enter an option, and then press Enter.

The following prompt appears:

Enter the encryption key (default: orion123):

11. Type the encryption key, and then press Enter.

The SNMP Request Service is started.

12. To return to the main menu, type exit at the cmc::service> prompt.

13. To log out and close the CMC command-line, type exit again.

Configure LEM to store original log messages (nDepth log retention)

LEM can store raw (unnormalized) log messages for retention and search purposes. To enable this feature, configure the LEM Manager and the applicable connectors accordingly.

nDepth log retention refers to storing raw data (that is, original log messages) in a separate database. Other than the name, nDepth log retention is separate from the nDepth search engine that is available in the LEM console under Explore > nDepth.

About nDepth log retention

This section describes nDepth log retention.
Why use a separate nDepth VM?

A separate nDepth appliance provides additional capacity to store and retrieve raw log messages. If long-term storage of original log messages is a priority, then consider a separate nDepth VM. Otherwise, a separate instance is probably unnecessary. For more information contact your SolarWinds sales representative or SolarWinds Technical Support.

Rules

- Rules do not fire on raw (unnormalized) log data. Rules can only fire on normalized data.
- Raw (unnormalized) log messages do not appear in Monitor view in the Console.
- If you enable original log storage (raw database storage), and you enable connectors to send data to both databases, LEM storage requirements may double for the same retention period, and extra resource reservations of at least two additional CPUs and 8-16GB of RAM may be required.

Install a separate nDepth appliance or VM

In this configuration, each LEM Manager has its own dedicated nDepth appliance or VM that stores the original log files from each host (network device) and source (application or connector) that the LEM Manager monitors. You still access and explore this information using the LEM console's nDepth view even though it resides in a separate appliance or VM.

- To use a separate nDepth appliance or VM, you must install it before you begin using nDepth. Contact SolarWinds Technical Support for instructions on installing a separate appliance.
- If you are not using a separate appliance, this procedure is not required, because short-term log messages are stored directly on LEM.

Configure network connectors for use with nDepth

Each data-gathering connector (or sensor connector) must be configured for use with nDepth log retention. First, decide which network devices, applications, and connectors monitored by the Manager should send raw log messages to nDepth. Next, configure each of these connectors for use with nDepth. You can route connector log messages directly to LEM, directly to nDepth, or to both.

See Configure connectors to send original log data to LEM for more information.

SolarWinds recommends configuring each connector so it routes its log messages to both nDepth and LEM. This allows you to receive events on these connectors, and to search log messages stored on the separate nDepth instance.

Configure LEM Manager to store original log files in their own database

The following procedure must be completed prior to configuring any connector to send log messages to your LEM appliance.

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. At the cmc> prompt, enter manager.
3. At the `cmc::manager>` prompt, enter configurendepth, and then follow the prompts to configure your LEM Manager to use an nDepth server.
   - Enter `y` at the Enable nDepth? prompt.
   - If you are prompted with Run nDepth locally? (Recommended), enter `y`. This will configure a separate database on your LEM appliance to store original log files.
   - If your LEM implementation consists of several appliances, follow the prompts to complete the process for your dedicated database or nDepth appliance. For additional information about this process, contact Support.

4. At the `cmc::manager>` prompt, enter `exit` to return to the previous prompt.

5. At the `cmc>` prompt, enter `ndepth`.

6. At the `cmc::nDepth#` prompt, enter `start`. This command will start the Log Message search/storage service.

7. To return to the previous prompt, enter `exit`.

8. To log out of your LEM appliance, enter `exit`.

Configure connectors to send original log data to LEM

1. Open the connector for editing in the Connector Configuration window for the LEM Manager or LEM Agent, as applicable.
   - If the connector has already been configured, stop the connector by clicking ⚪️ > Stop, and then click ⚪️ > Edit.
   - If the connector has not been configured, create a new instance of the connector by clicking ⚪️ > New next to the connector you want to configure.

2. In the Connector Details pane, change the Output value to Alert, nDepth. Leave the nDepth Host and nDepth Port values alone unless otherwise instructed by Support.

   The Output values are defined as:
   - Alert: Sending data to the alert database
   - nDepth: Sending data to the RAW (original log) database

   For help, see The Connector Configuration form fields for data-gathering (sensor) connectors.

3. If you are finished configuring the connector, click Save.

4. To start the connector, click ⚪️, and then select Start.

5. To close the Connector Configuration window, click Close.

6. Repeat these steps for each connector you want to send original log data to your LEM appliance.

View and search your original log messages

See Search raw log messages using nDepth search in LEM for details.
Configure the LEM event distribution policy

Configure the event distribution policy to choose which events should go to the LEM console, and which should go to the local LEM database. This topic explains how to configure the event distribution policy on the LEM Manager.

Practical uses for event distribution policy

Many data sources generate events that are difficult to control at a granular level, or they generate events of little or no value. SolarWinds recommends removing these events from the system to reduce the volume and noise sent to the LEM console and LEM database. By configuring the event distribution policy, you can disable (or exclude) specific event types at the event level from being sent to these destinations. The data sources continue to generate these events, and you can enable them at any time, but the selected system destinations will ignore them while they are disabled.

Additionally, you may have events that you want to monitor in the console, but that do not require long-term storage or reporting. In this case, you can configure the event distribution policy to disable database storage for those events, but enable processing by the console.

See also: Collect Windows Filtering Platform (WFP) events in LEM

Open the Event Distribution Policy window

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. Next to the targeted LEM Manager in the Appliances grid, click ✉️, and then select Policy. The Event Distribution Policy for [Manager] window appears.
If you open the Event Distribution Policy window while it is in use by a user, a Policy Locked message appears. You can choose to take over the window, or view it in read-only mode. Any Full User can unlock any other user.

The following table describes the key features of the Event Distribution Policy window.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event/Field</td>
<td>Lists event categories and event types. Click ▼ to maximize an event category.</td>
</tr>
<tr>
<td>Console</td>
<td>Select a check box to indicate whether an event time or event category is sent to the console or local database.</td>
</tr>
<tr>
<td>Database</td>
<td>When selected, the event type is routed to that destination. Clear a check box to prevent the event type from being routed to that destination.</td>
</tr>
<tr>
<td>Warehouse</td>
<td></td>
</tr>
<tr>
<td>Rules</td>
<td></td>
</tr>
<tr>
<td>Export</td>
<td>Exports a Manager event policy to a spreadsheet file.</td>
</tr>
<tr>
<td>![icon]</td>
<td>Click to select the Apply State to Branch command. This command pushes (or propagates) the selected event node check box settings down to the related, lower-level event types in the node tree hierarchy.</td>
</tr>
<tr>
<td>Description</td>
<td>Provides a description of the event type or event category currently selected in the grid.</td>
</tr>
</tbody>
</table>

Configure the event distribution policy

Use the Event Distribution Policy window to configure your event distribution policy. Locate the event types you need, and then select the appropriate check boxes to determine whether these event types are routed to a particular destination.

1. Open the Event Distribution Policy window. See Open the Event Distribution Policy window for steps.
2. Locate the events that you want to disable by either browsing the alert taxonomy or by using the search box under Refine Results.

   ![tip] You can locate all of the events listed below by typing Windows Security in the search box.

3. Select or clear the check boxes in the Console, Database, Warehouse, or Rules columns as appropriate.
   - Clear the Console box to prevent LEM Manager from showing an alert in the LEM console.
   - Clear the Database box to prevent LEM Manager from storing the alert in the LEM database.
   - Clear the Warehouse box to prevent LEM Manager from sending the alert to an independent database warehouse.
   - Clear the Rules box to prevent LEM Manager from processing the alert against LEM rules.
   - Select any check box to enable processing for the alert at any of the four levels listed above.
4. To save your changes, click Apply.
5. To save your changes and exit the Alert Distribution Policy window, click Save.

This process may require 30 seconds to several minutes to complete.

Push event policy to lower-level event types

Use the Apply State to Branch command to propagate (or push) event distribution policy settings from a high-level event type to each of its lower-level "child" event types in the event hierarchy.

For example, if you select the top Security Event row and select the corresponding Console and Warehouse check boxes. Clicking Apply State to Branch assigns the same Console and Warehouse check box settings to every child item associated with Security Event. When you save your configuration, the policy causes all child event types of Security Event to send events to all user consoles and your data warehouse.

1. Open the Event Distribution Policy window for a selected Manager. See Open the Event Distribution Policy window for steps.
2. In the Event/Field grid, locate the event type that is a parent to the event types you want to configure.
3. In the parent row, define the policy by selecting or clearing the Console, Database, Warehouse, and Rules check boxes.
4. Next to the targeted row, click ✡, and then select Apply State to Branch.
   
   The Console pushes (or propagates) the parent row check box settings down to each of its lower-level event types in the node tree hierarchy.

   If you select one or more of the parent row check boxes, the console selects the same check box settings for each related lower-level event type in the node tree. When you save your configuration, the policy begins sending the “child” event types to the selected destinations.

   If you clear any of the parent row check boxes, the console disables the same check box settings from each related lower-level event type in the node tree. When you save your configuration, the policy stops sending those event types to those destinations.

5. To save your changes, click OK.

   The Console implements the new policy.

Export a Manager event policy

You can export a Manager event policy to a spreadsheet file to:

- View and manipulate the policy information in a spreadsheet application, such as Microsoft Excel.
- Provide SolarWinds with a copy of your policy information for technical support or troubleshooting purposes.

To export a Manager policy:

1. Open the Event Distribution Policy window for a selected Manager. See Open the Event Distribution Policy window for steps.
2. At the top of the window, click Export.
   
   The Save As form appears.
3. In the Save In box, select the folder you want to export to.
4. In the File Name box, enter a name and file type for the exported file.
   In the file name, include an XLS file type to save the file as a Microsoft Excel spreadsheet.

5. To save the file, click Save.
   The Console saves the file to the folder and with the file name you specified.
   You can now view the Manager policy information in a spreadsheet file, such as Excel.

Collect Windows Filtering Platform (WFP) events in LEM

Windows Filtering Platform (WFP) logs firewall and IPsec related events to the System Security Log. These alerts are background events that require additional LEM resources to process and are not recommended for an optimized LEM deployment.

About Windows WFP events and LEM performance

By default, WFP logging is disabled in the Windows Security Log connector. Tuning out Windows noise in group policies has the following advantages:

- Reduces the space that these events occupy in the Security Event log
- Reduces network activity
- Reduces demand on LEM system resources (such as CPU, memory, and disk space)


Configure LEM to collect WFP events (Optional)

If necessary, you can enable WFP event logging in LEM.

SolarWinds strongly recommends that you keep WFP logging turned off.

To collect WFP events in LEM, configure the Windows Filtering Platform Events connector. Enabling this connector will result in LEM collecting a huge volume of data. To manage this data, see the following sections.

Improve LEM performance by tuning Windows WFP events

If you collect WFP events in LEM, SolarWinds recommends tuning WFP in your Active Directory group policies to decrease the load that background events place on the LEM Manager. The following tables describe alerts located in the Event Distribution Policy in LEM Manager. You can filter out these events by clearing the appropriate check boxes in the Console, Database, Warehouse, and Rules columns. LEM will process the remaining events.

In LEM, the terms event and alert are interchangeable.

SolarWinds recommends disabling WFP alerts using Group or Local Policy.

The ProviderSID value in the following alerts match the Windows Security Auditing Event ID format where Event ID is one of the Windows Event IDs listed in the following table.
<table>
<thead>
<tr>
<th>ALERT NAME</th>
<th>WINDOWS EVENT ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCPTrafficAudit</td>
<td>5152, 5154, 5156, 5157, 5158, 5159</td>
</tr>
<tr>
<td>IPTrafficAudit</td>
<td>5152, 5154, 5156, 5157, 5158, 5159</td>
</tr>
<tr>
<td>UDPTrafficAudit</td>
<td>5152, 5154, 5156, 5157, 5158, 5159</td>
</tr>
<tr>
<td>ICMPTrafficAudit</td>
<td>5152, 5156, 5157, 5158, 5159</td>
</tr>
<tr>
<td>RoutingTrafficAudit</td>
<td>5152, 5156</td>
</tr>
<tr>
<td>PPTPTrafficAudit</td>
<td>5152</td>
</tr>
</tbody>
</table>

Table of Descriptions by Event ID

<table>
<thead>
<tr>
<th>EVENT ID</th>
<th>BRIEF DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>5152</td>
<td>Windows Filtering Platform blocked a packet</td>
</tr>
<tr>
<td>5154</td>
<td>Windows Filtering Platform permitted an application or service to listen on a port for incoming connections</td>
</tr>
<tr>
<td>5156</td>
<td>Windows Filtering Platform allowed a connection</td>
</tr>
<tr>
<td>5157</td>
<td>Windows Filtering Platform blocked a connection</td>
</tr>
<tr>
<td>5158</td>
<td>Windows Filtering Platform permitted a bind to a local port</td>
</tr>
<tr>
<td>5159</td>
<td>Windows Filtering Platform blocked a bind to a local port</td>
</tr>
</tbody>
</table>
Manage LEM system resources

This section describes how to manage the hardware and software resources that LEM requires to work properly.

Allocate CPU and memory resources to the LEM VM

By default, LEM deploys with 8GB of RAM and 2 CPUs on the VMware ESX(i) and Microsoft Hyper-V platforms. For LEM to work properly, you must allocate sufficient CPU and memory resources to the LEM VM. This topic describes how to check resource settings and make updates.

See LEM 6.6 system requirements in the LEM Installation Guide for hardware and software sizing requirements.

As of version 6.3.0, LEM can send SNMP version 3 alerts to SolarWinds Network Performance Manager (NPM). This configuration allows you to monitor CPU, memory, and other critical LEM components from the SolarWinds Orion Web Console.

Log & Event Manager collects data from a continuous stream of traffic that fluctuates based on user, server, and network activity. The type and volume of traffic varies based on the device sending the traffic and the audit and log settings on those devices.

About incoming data traffic

Log & Event Manager receives data from syslogs and traps using up to 500 connectors that receive data traffic from several supported network devices. These connectors translate (or normalize) the data into a readable and understandable format you can view in the LEM console.

The connectors display in the Monitor view, pass through the rules engine for specified actions, and then move into a database for retrieval by the LEM Reports or nDepth search function. To process the data in real time, LEM requires system resource reservations from the virtual appliance host.

When the volume of traffic exceeds 15 million events per day, be sure to reserve additional system resources to support the additional data traffic.

Use the LEM console to view resource allocations and VM details

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Manage > Appliances.

   The Appliances toolbar, navigate to Manage > Appliances.

   The Appliances grid lists the LEM VMs registered with the console and their corresponding details.

<table>
<thead>
<tr>
<th>Appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
</tr>
<tr>
<td>🟢</td>
</tr>
</tbody>
</table>
Below the Appliances grid, the Details pane lists information about the selected VM. (If the Details and Properties panes are not visible, click the Appliances tab at the bottom of the screen.)

<table>
<thead>
<tr>
<th>Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
<td><strong>Value</strong></td>
</tr>
<tr>
<td>Platform</td>
<td>VMware</td>
</tr>
<tr>
<td><strong>CPU Reservation</strong></td>
<td>0.00 GHz</td>
</tr>
<tr>
<td>Number of CPUs</td>
<td>2</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>4.00 GB</td>
</tr>
<tr>
<td>Memory Reservation</td>
<td>4.00 GB</td>
</tr>
<tr>
<td>Status</td>
<td>Connected</td>
</tr>
<tr>
<td>Name</td>
<td>swi-lemp</td>
</tr>
<tr>
<td>Type</td>
<td>Manager</td>
</tr>
<tr>
<td>Version</td>
<td>6.3.1hotfix2</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.199.129.12</td>
</tr>
<tr>
<td>Port</td>
<td>8080</td>
</tr>
</tbody>
</table>

**Details pane descriptions**

<table>
<thead>
<tr>
<th><strong>FIELD</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>The Manager platform name, which can be Trigeo SIM, VMware vSphere, or Microsoft Hyper-V.</td>
</tr>
<tr>
<td>CPU Reservation</td>
<td>The reserved CPU memory. Reserving CPU memory ensures enough system resources are available for the allocated CPUs.</td>
</tr>
<tr>
<td>Number of CPUs</td>
<td>The number of processors allocated to the virtual appliance.</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>The maximum amount of memory the Manager can use. Set this value at or above the reservation value. You can define this value in the VM configuration. Setting memory allocation to a greater value than the memory reservation has little effect on LEM performance.</td>
</tr>
<tr>
<td>Memory Reservation</td>
<td>The amount of memory reserved for this system.</td>
</tr>
<tr>
<td>Status</td>
<td>The current connection status of the selected Manager or appliance.</td>
</tr>
<tr>
<td>Name</td>
<td>The Manager or appliance name.</td>
</tr>
<tr>
<td>Type</td>
<td>The appliance type (Manager, Database Server, nDepth Server, Logging Server, or Network Sensor).</td>
</tr>
<tr>
<td>Version</td>
<td>The Manager or appliance software version.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The Manager or appliance IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used by the LEM console to communicate with the Manager or appliance.</td>
</tr>
</tbody>
</table>

You can view your reservation settings using vSphere or an SSH client (such as PuTTY). See your VMware vSphere documentation for details about configuring resources, reservations, and storage on a vSphere virtual appliance.

### View vSphere reservation settings for LEM

You can view reservation settings using the vSphere client. See your VMware vSphere documentation for details about configuring resources, reservations, and storage on a vSphere virtual machine.

1. Log into vSphere and check the Settings/Reservations.
2. Select LEM from the list (name listed may not be the host name), and view the Summary tab to find the number of CPUs (such as 2 vCPU).

   **LEM requires at least two CPUs. The highest working setting for any LEM appliance is 16 CPUs.**

3. Provisioned Storage on the right side of the screen shows the total disk space LEM can use.
   - If LEM is set for thick provisioning, the used storage is always the total disk space.
   - Thin provisioning allows the used storage to grow to the total amount of storage allocated.

4. On the Resource Allocation tab, note the CPU reservation on the left, and the memory reservations on the right.

5. At the bottom left, check the CPU reservation. 2.0Ghz is LEM's minimum setting. To support higher speeds, see your VMware documentation for configuration information.

6. See the Memory reservation at the bottom right. This reservation is normally set at 8 GB or higher. The Memory must be the same value or higher than the reservation. Memory reservations can be set as high as 64GB of RAM, which can support over 150 million events per day.

### Change vSphere reservations for LEM

1. Shut down the LEM VM. See [Start and Stop LEM components](#) for steps.
2. Right-click the LEM VM to edit settings.
   - Select the Hardware tab and change the allocated memory size.
3. Select the Resources tab, and then change the CPU and memory settings.
   - Set the limit to unlimited for both CPU and memory reservations.
4. To save the changes, click OK.
5. Use the vSphere console to start the LEM VM.
View reservations settings using the CMC command-line

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. At the cmc> prompt, type manager.
3. Type viewsysinfo, and then press Enter.
   
   The system returns memory and CPU information, as well as LEM version and license information.
4. To return to the cmc::manager> prompt, type :q.
5. To exit the manager menu, type exit.
6. To exit the CMC command line, type exit at the cmc> prompt.

View Hyper-V reservation settings for LEM

Use the following tables to verify your Hyper-V client settings. For details about setting resources, reservations, and storage on a Hyper-V virtual appliance, see your Microsoft Hyper-V documentation.

Memory settings

<table>
<thead>
<tr>
<th>SETTING</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static RAM</td>
<td>8GB, 16GB, 24GB, 32GB, 64GB, 128GB, 256GB</td>
</tr>
<tr>
<td>Memory Weight</td>
<td>High</td>
</tr>
</tbody>
</table>

CPU settings (Windows Server 2008)

<table>
<thead>
<tr>
<th>SETTING</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of processors</td>
<td>2, 4, 6, 8, 10, 12, 14, 16</td>
</tr>
<tr>
<td>VM reserve CPU cycles</td>
<td>100%</td>
</tr>
<tr>
<td>Limit CPU Cycles</td>
<td>100%</td>
</tr>
<tr>
<td>Relative weight for CPU</td>
<td>100%</td>
</tr>
</tbody>
</table>

CPU settings (Windows Server 2012)

<table>
<thead>
<tr>
<th>SETTING</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU memory details</td>
<td>Click the Advanced tab and set the view and details</td>
</tr>
<tr>
<td>CPU Priority</td>
<td>High</td>
</tr>
<tr>
<td>Reserve CPU cycle</td>
<td>100%</td>
</tr>
<tr>
<td>Limit CPU cycles</td>
<td>100%</td>
</tr>
</tbody>
</table>
Manage LEM data storage

This topic addresses LEM database management.

About the three LEM data stores

By default, the LEM database is allowed 230 GB of the 250 GB allocated to the LEM virtual appliance. This partition consists of three data stores:

- Syslog store
- Events store
- Original or raw log data store (optional)

The **syslog store** consists of all syslog or SNMP log data sent to the LEM VM. LEM reads and processes the data in real time, and then sends it to the **event store** for long-term storage. LEM stores the original data for 50 days in its original format (in case you need to review it). The data in the syslog store is compressed and rotated daily to maintain a consistent 50-days' worth of data. The amount of data stored here should level off at around the 50-day mark.

The **event store** (the second store) contains all normalized events generated by the LEM Manager and LEM Agents. Data in this store is compressed at ratios of 40:1 to 60:1, which equates to an average compression rate of 95–98 percent. Both nDepth and the LEM reports application query the event store for event data when they run.

The **original log store** (the third store) is an optional store for original or raw log messages that can be searched using Log Message queries in nDepth. The data in this store can come from LEM Agents or other devices logging to the LEM appliance. You can configure if data is sent to this store at the connector level, so not all devices have to store raw log messages in this manner.

For more information about storing original log messages, see Configure LEM to store original log messages (nDepth log retention).

Strategies for managing your LEM data storage needs

Depending on the needs of your environment, you can use one or more of the alternate storage methods listed below.

- Back up the LEM VM on a regular basis. This will provide offline storage for your LEM data stores.
- Decrease the number of days that syslog and SNMP data is stored in LEM.
- Deploy another LEM VM to be used as a syslog server.
- Deploy another LEM VM to be used as a database server.
- Increase the space allocated to your LEM VM.

To get help with any of these methods, submit a ticket to Customer Support:

https://customerportal.solarwinds.com/support/submit-a-ticket
View LEM database usage numbers

There are three locations to find metrics that indicate how the LEM database is used:

- Disk Usage summary in the CMC
- Database maintenance report
- Log storage maintenance report

View the Disk usage summary

When you use the command line to log in to LEM, LEM automatically generates a Disk Usage summary. You can also generate an ad hoc disk usage summary by running the `diskusage` command from the `cmc > appliance` prompt. The two lines to note here are `Logs/Data` and `Logs`.

- The `Logs/Data` figure represents the total space being utilized by the LEM database. This value is presented in the percent % (usedG/allocatedG) format, where `percent` is the percent of the allocated space currently being used, and `allocated` is the total amount of space currently allocated to the LEM database.
- The `Logs` figure represents the amount of space used by the syslog store. This figure is included in the used figure noted above. To figure out how much space is currently being used by the Event store, subtract the `Logs` value from the used value. If you are storing original log messages in the LEM database, the above calculation shows the combined space utilized by both your Event and original log stores.

View the Database maintenance report

Run the Database Maintenance Report in LEM reports to view a snapshot of your current database usage. The report includes the following values:

- Disk Usage Summary – provides disk usage values in terms of the percentage of space allocated to the LEM database
- Disk Usage Details – provides disk usage values in terms of physical file size
- Database Time Span (days) – shows how many days' worth of live event data is currently stored in the LEM database
- Other Files – represents the amount of space used by the syslog store

For more information, see the following KB article in the Customer Success Center: [Use the LEM Database Maintenance Report to See Retention and Volume of Traffic](#)

View the Log storage maintenance report

Run the log storage maintenance report in LEM reports to get detailed information about the original log store. If you have not enabled LEM to store original log messages, this report will be blank.

For more information, see the following KB article in the Customer Success Center: [Live Data Storage Retention in LEM](#)
Create a disk usage alert in LEM to warn you when a disk reaches a set limit

You can create a disk usage alert from the CMC command line to warn you when a disk partition reaches a preselected use limit. When the limit is reached, an InternalWarning event displays in the Monitor view.

You can define the disk use limit by the percentage of unavailable disk space (such as 75 percent), or by the amount of free disk space (such as 58G).

To create the disk usage alert:

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. To access the Appliance menu, at the cmc> prompt, enter appliance.

3. To view the disk use of each partition, at the cmc::appliance> prompt, enter diskusage. For example:

```bash
cmc::appliance > diskusage
Checking Disk Usage (this could take a moment)
.
Partition Disk Usage:
LEM: 35% (991M/3.0G)
OS: 45% (1.3G/3.0G)
Logs/Data: 1% (901M/234G)
Temp: 2% (252M/5.9G)

Database Queue(s): 4.0K (No alerts queued, 0 alerts waiting in memory)
Rules Queue: 2.1M (0 alerts queued, 0 alerts waiting in memory)
Console Queue: 2.1M (0 alerts queued, 0 alerts waiting in memory)
DataCenter Queue: 2.1M (0 alerts queued, unknown number of alerts waiting in memory)
EPIC Rules Queue: 2.1M (0 alerts queued, 0 alerts waiting in memory)
Forensic Database Queue: 2.1M (0 data queued, unknown number of data items waiting in memory)
Logs: 1.3M
```
4. **At the cmc::appliance> prompt, enter diskusageconfig.**

Each partition and corresponding disk use limit displays on your screen. For example:

```
cmpy::appliance > diskusageconfig
Current Disk Usage Configuration:
# | Partition (filesystem) | Configured limit
===============================================
1 | LEM (/usr/local) | 90%  
2 | OS (/) | 90%  
3 | Logs/Data (/var/) | 10G  
4 | Temp (/tmp) | 90%
```

You can define your disk use limit by the percentage of unavailable disk space (such as 75%) or the amount of free disk space (such as 58G). Enter the partition number you want to change (enter 'exit' and press <Enter> to quit):

5. Enter the partition number you want to change, and then press Enter.

6. Enter the disk usage limit value in percentage (such as 75 percent) or size (such as 58G), and then press Enter.

For example, to change the OS disk partition limit in step 3 from 45 percent to 4 percent, enter 40 percent. To change the OS disk partition limit from 1.3 GB to 2.0 GB, enter 2GB.

```
Disk usage limit [90%, sizeK, sizeM, sizeG, sizeT] (default 90%): 40%  
Limit '40%' for the 'OS' partition is set.  
Press <Enter> to set the next partition. Enter 'exit' and press <Enter> to quit.
```

7. Press Enter to set the next partition and repeat step 6 (if required).

See [Change the Logs/Data partition setting](#) for additional information.

8. When you are finished, type exit, and then press Enter to quit.

**Change the Logs/Data partition setting**

When you set the Logs/Data partition (3), a message prompts you to consider changing the database disk configuration using the dbdiskconfig command. SolarWinds recommends setting the Logs/Data partition and the database disk configuration to the same value.
Change the database disk configuration

1. Finish configuring your partitions.

2. At the cmc::appliance> prompt, enter dbdiskconfig.
   The following message displays:
   
   ```
   Current configuration:
   DoNotExceedPercentage = 90%
   
   The Manager will restart and apply your changes. To exit, enter 'exit' and press Enter.
   Enter a new value for DoNotExceedPercentage (default 90):
   Please enter an inter number 0-100 or 'exit'
   ```

3. At the prompt, enter a usage limit value between 0 and 100, and then press Enter.
   
   ![Note](If you enter a value less than 25, the partition will be deleted when this value is reached.)

   The database disk configuration value is saved, and the appliance restarts the Manager Service.

View a disk usage event

Log in to your LEM console as an administrator, and then open the Monitor view. The event displays in the All Events grid.

For example, if you set the OS disk partition limit as a percentage, the following event displays in the All Events grid when the limit is reached:

```
Internal/Info    Manager/monitor_info: Disk usage of Logs/Data: 4% (7.3G/234G)
Internal/Warning Manager/monitor_warning: Disk Usage: The OS filesystem is over 40% full
Internal/Info    Manager/monitor_info: Disk usage of OS: 46% (1.9G/3.9G)
```

If you set the OS disk partition limit as a file size, the following event displays in the All Events grid when the limit is reached.

```
Internal/Info    Manager/monitor_info: Disk usage of Logs/Data: 4% (7.3G/234G)
Internal/Warning Manager/monitor_warning: Disk Usage: The OS filesystem has under 2G left
Internal/Info    Manager/monitor_info: Disk usage of OS: 45% (1.9G/3.9G)
```

Select the event in the grid and review the content in the Event Details tab for additional information.

**LEM tuning and periodic maintenance tasks**

SolarWinds recommends that you complete the tasks in this topic to ensure LEM performs optimally as your network changes.

Complete the following tasks to ensure that LEM uses processor and memory resources efficiently.

Review your rule configurations

Review your rules periodically to ensure that they are not triggering too frequently. This can be caused by:
• **Low threshold settings.** Consider increasing the threshold for rules that trigger due to network traffic.

• **Broadly-defined conditions.** Define rules to apply only to specific user names, IP addresses, or systems. Consider whether a different set of rules with different conditions could serve two distinct areas of your environment.

• **Rules using event groups instead of a single event or subset of events.** Rules that detect authentication or network traffic may trigger on additional events, but may only apply to a subset of those events.

Validate your virtual appliance reservations

System requirements can change over time, so periodically review your resource allocations. See Manage LEM VMs and appliances in the LEM console for details.
Integrate LEM with other SolarWinds products

This section describes how to configure LEM to work in combination with other SolarWinds products.

Monitor LEM from NPM and the Orion Web Console using SNMP

If you use Network Performance Manager (NPM) and the SolarWinds Orion Web Console, you can use it to monitor CPU, memory, and other critical resources utilized by LEM. Complete the steps in this topic to configure LEM to communicate with NPM.

As of version 6.3.0, LEM can use SNMP version 3 to communicate with SolarWinds Network Performance Manager (NPM). Versions of LEM older than 6.3.0 can send SNMP traps to other devices when rules fire, but older LEM versions do not support sending health or status updates to other devices over SNMP.

Enable the SNMP Request Service

See Send SNMP traps from LEM to other applications by turning on the SNMP Request Service for details. After you enable and configure the SNMP Request Service, go to the next topic, Set up the Orion Web Console for SNMP monitoring.

Set up the Orion Web Console for SNMP monitoring

When you are finished enabling the SNMP Request Service, log in to the Orion Web Console and set up the LEM Manager as a monitored node on the Orion Platform.

1. Log in to your Orion Web Console as an administrator.
2. Navigate to Settings > Manage Nodes, and then click Add a Node.
   
   If the node already exists and it is not managed, click the node and select Not Managed Node > Yes to manage the node.
   
   The Define Node window displays.
3. In the Polling Hostname or IP Address field, enter the IP address of the LEM Manager.
4. Under Polling Method, select Most Devices: SNMP and ICMP.
5. Select your polling method settings.

![Polling Method Settings Diagram]

- a. Select SNMPv3 for the SNMP version.
- b. Enter the port number used to access SNMP on the LEM appliance.
- c. Under SNMPv3 Credentials, enter the user name used to access SNMP on the LEM appliance.
- d. Under SNMPv3 Authentication, enter the hashing algorithm method and password.
- e. Under SNMPv3 Privacy / Encryption, enter the communication encryption algorithm and password.
- f. Accept the default selections in the remaining options.

6. To test the connection, click TEST.
   If the connection is good, Test Successful appears.

7. Click Next.
   The Orion Platform authenticates the LEM Manager and runs a discovery to locate the resources available to monitor on the LEM appliance. The discovered resources will list all the elements that are available to monitor. The Orion Platform will automatically provide a list of selected resources based on the device type.

8. In the Choose Resources window, select the resources to monitor on the node, and then click Next.

9. In the Add Application Monitors window, click Next.

10. In the Change Properties window, click Next.

11. Click OK, Add Node.
    The LEM appliance is added to the Orion Web Console for monitoring.
Troubleshooting your Orion connection

If you cannot establish a connection between your LEM appliance and the Orion Platform:

- Ensure that the settings you entered in the Define Node window match the settings used to enable the SNMP Request Service.
- Review the Orion logs located at c:\ProgramData\SolarWinds\Discovery for errors.

See [Unable to add nodes through the Web Console](#) for additional troubleshooting information.
Secure LEM

This section describes how to secure LEM to prevent unauthorized access.

**LEM security checklists: Ensure that only authorized users can access LEM**

Complete the following tasks to help prevent unauthorized users from accessing LEM.

### General security tasks

- Read the Log & Event Manager Appliance Security and Data Protection [blog post](https://thwack.net) on THWACK.

### Secure the LEM Manager and the LEM consoles

- Run the activate command from the CMC command line.
  - Run this command to export the SSL certificate that ensures secure communications between the LEM desktop console and the LEM Manager.
  - See [Run the activate command to secure LEM and configure network settings](https://thwack.net) for steps.

- Set the minimum password requirements for local LEM user accounts.
  - See [Set the global password policy for LEM users](https://thwack.net) for steps.

- Restrict the filters that Monitor role users can access.
  - See [Specify the filters that users assigned the Monitor role can use in the LEM console](https://thwack.net) for steps.

### Secure the CMC command-line interface

- Change the default CMC password.
  - See [Change the LEM CMC password](https://thwack.net) for steps.

- Restrict SSH access to the CMC command-line interface.
  - (Optional) This procedure blacklists everyone from logging in to the CMC interface except those users who connect from an explicitly allowed IP address or host name.
  - See [Restrict SSH access to the LEM CMC interface](https://thwack.net) for steps.

### Secure the LEM reports application

- Secure the LEM reports application.
  - See [Restrict access to the LEM reports application](https://thwack.net) for steps.
Enable transport layer security (TLS) between the LEM reports application and the LEM database.

(Optional) The Transport Layer Security (TLS) option introduces an extra level of security for data transfers between a LEM database and the Reports application.

See Enable transport layer security (TLS) in the LEM reports application for steps.

Restrict SSH access to the LEM CMC interface

Users who have CMC command-line interface (CLI) access can connect to the LEM VM and perform administrative tasks. You can restrict SSH access to the CMC interface by IP address or host name. This optional procedure blacklists everyone from logging in to the CMC interface except those users who connect from an explicitly allowed IP address or host name.

To restrict SSH access to the CMC command line:

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. Type service, and then press Enter.
3. Type restrictssh, and then press Enter.
4. Complete the wizard to limit access to the LEM cmc console by IP address or host name. You can enter multiple addresses and host names separated by a space.

Test the restriction by attempting to log in from a blacklisted host or IP address. Repeat the test to confirm that you can log in from whitelisted hosts and IP addresses.

To remove access restrictions from the CMC interface

Complete the steps to allow users from any IP address or host name to access the CMC interface using SSH.

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. Type service, and then press Enter.
3. Type unrestrictssh, and then press Enter.
4. Complete the wizard to remove access restrictions.

Test the restriction by logging in from a previously blacklisted host or IP address.

Restrict access to the LEM reports application

This topic documents how to secure the LEM reports application so that only authorized users can access it.

Understand your options for securing LEM reports

Older versions of LEM (pre 6.2) allow unrestricted access to the LEM database by the reports application installed on a Windows computer. No credentials were required for the access.
Starting with LEM version 6.2.0, the LEM Reports application requires a username and password to allow the LEM Reports application to access the database.

As with all versions of LEM, there is one additional level of security for the Reports application, but the same holds true for the SSH connection or the Console connection (web-based or air-based). You only need to run the restrictreports command (or restrictconsole or restrictssh commands) to create a whitelist of computer hostnames or IP addresses that can run reports and access the database (or the console or SSH, if using that parameter).

- Access can be restricted to specific computers.
- Access can be restricted by port number. The Reports application communicates over port 9001, using TLS or no encryption. Console access only on port 8443/443 when the LEM is activated, but port 8080/80 is available during evaluation period or if togglehttp command used to re-enable the port 8080/80. SSH access is allowed on port 22 or 32022, but support can assist you with forcing only one port. LEM versions prior to 6.3.1 only had port 32022 available for SSH.
- The LEM reports application can be configured to require a user name and password.

To encrypt communication between the LEM reports application and the LEM database, see Enable transport layer security (TLS) in the LEM reports application.

Restrict access to LEM reports to specific computers

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. At the `cmc>` prompt, type `service`.
3. At the `cmc::service>` prompt, type `restrictreports`.
4. When prompted, press the Enter key.
5. Enter the IP addresses of the computers you want to allow to run the LEM reports application, separated by spaces.

   Ensure that the list you provide is complete. Your entry will override any previous entries.

6. To confirm your entry, type `y`.
7. To return to the `cmc>` prompt, type `exit`.
8. To log out of the CMC command line, type `exit`.

Remove all LEM reports access restrictions

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. At the `cmc>` prompt, type `service`.
3. At the `cmc::service>` prompt, type `unrestrictreports`.
4. When prompted, press the Enter key.

Removing LEM reports restrictions will make the LEM database accessible to any computer on your network that is running the LEM reports application.
5. To return to the `cmc>` prompt, type `exit`, and then press Enter.
6. To log out of the CMC command line, type `exit`, and then press Enter.

Enable transport layer security (TLS) in the LEM reports application

The Transport Layer Security (TLS) option introduces an extra level of security for data transfers between the LEM reports application and the LEM database.

- By default, TLS is disabled on versions of LEM that have been upgraded from LEM version 6.0.1 or earlier.
- The procedure to enable TLS differs depending on your LEM configuration (standalone or with a dedicated database appliance).
- When enabling TLS, the LEM certificate for accessing the web or AIR console needs to be rebuilt. Machines used to access LEM web or AIR console must re-import their certificates.

Enable TLS on a standalone LEM VM or appliance

Use these steps if the LEM database is located on the same VM or appliance as the LEM Manager. This is the most common arrangement.

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.

   Steps 2 - 6 below are required to upgrade older versions of LEM. If you have LEM version 6.0.1 or later, go to step 7. The default hostname is `swi-lem`.

2. At the `cmc>` prompt, type `appliance`.
3. At the `cmc::appliance>` prompt, type `hostname`.
4. Enter the name of the LEM Manager at the Please enter the new hostname prompt.

   Enter the currently-used hostname if you do not want the LEM Manager name to change.

5. At the `cmc::appliance>` prompt, type `exit`.
6. At the `cmc>` prompt, type `manager`.
7. At the `cmc::manager>` prompt, type `exportcert`.
8. Follow the prompts to export the LEM Manager CA certificate.

   An accessible network share is required. Once the export is successful, you will see the following message: Exporting CA Cert to `\server\share\SWICAer-hostname.crt` ... Success.

9. At the `cmc::manager>` prompt, enter `enabletls`.
10. At the `cmc::manager>` prompt, enter `restart`.

Set up a dedicated LEM user for accessing reports

Starting with LEM 6.0.1, a user account with the Reports role is required to access LEM from the LEM reports application.
If a suitable user with the Reports role already exists, go to Configure the Reports application to use TLS. An Active Directory user can be a Reports user if LEM is set up to authenticate to Active Directory. See Import an Active Directory user into LEM and specify the Reports role in the LEM Groups field. Otherwise, complete the following steps to create a user with the Reports role in the LEM console.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Users.
3. To create a new LEM user, click .
4. Complete the fields as required.
5. From the LEM Role drop-down list, select Reports.
6. Save the new user.

Configure the Reports application to use TLS

1. Start the LEM reports application. See Open the LEM reports application for steps.
2. From the Configure drop-down list, select Managers > Credentials and Certificates.
3. Click the green button.
4. Enter the Manager IP or hostname.
5. Fill in the credentials of the user created previously in the LEM web console.
6. Select the Use TLS connection option.
7. To add a new Manager, click the green button again.
8. Click the Certificates tab.
9. Click Import Certificate.
10. Browse and Open LEM certificate (the network share folder specified during the certificate export).
11. Use the certificate from the Database Appliance in case you have LEM configured with a dedicated database.
12. Close the Manager Configuration window.

If LEM changed its host name, importing the LEM CA certificate again is not required.
Enable TLS on a LEM Manager with a separate database appliance

Typically, the LEM database is located on the same VM or appliance as the LEM Manager. If your LEM deployment has a separate LEM database, follow these steps.

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. At the cmc> prompt, type appliance.
3. At the cmc::appliance> prompt, type hostname.
4. At the Please enter the new hostname prompt, enter a name for the LEM Manager.
   
   If you do not want your LEM Manager name to change, enter the currently-used hostname.

5. At the cmc::appliance> prompt, type exit.
6. At the cmc> prompt, type manager.
7. At the cmc::manager> prompt, type exportcert.
8. Follow the prompts to export LEM CA certificate.

   An accessible network share is required. Once the export is successful, the following message appears:

   Exporting CA Cert to \server\share\SWICAert-hostname.crt ... Success.

9. At the cmc::manager> prompt, type enabletls.

   To use the custom CA to sign a database or LEM Manager certificate, generate and sign the certificate after you change the hostname.

Import certificates into the LEM Manager and database

LEM Manager and database nodes need to trust each other's certificates. This can be done by importing certificates from both sides.

This procedure is not required if you upgraded from LEM 6.0.0 or earlier, or if version 6.0.1 or later was deployed and the CA was used to sign both LEM certificates.

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. At the cmc> prompt, type manager.
3. At the cmc::manager> prompt, type importl4ca.
4. Choose the network share location specified during certificate export of Database.
5. When prompted for a file name, specify the name of a Database certificate.
   
   Enter the full file name, including the file extension.

6. Open the cmc prompt on the LEM database machine.
7. At the cmc> prompt, type manager.
8. At the cmc::manager> prompt, enter importl4ca.
9. Choose the network share location specified during certificate export of Manager.
10. When prompted for a file name, specify the name of the LEM Manager certificate.

**Next steps:**
- Set up a dedicated LEM user for accessing reports
- Configure the Reports application to use TLS

**Import a self-signed certificate into the LEM Manager**

Use the `importcert` command in the CMC to import a signed certificate by any CA into the manager.

1. Open the CMC command line. See [Log in to the LEM CMC command line interface](#) for steps.
2. At the prompt, enter `manager`.
3. At the `cmc::manager>` prompt, type `importcert`.
4. Choose the network share path.
5. When prompted, confirm the share name.
6. When prompted for a file name, enter the full name of the certificate, including the CER extension.
7. When completed, the following message appears:
   - Certificate successfully imported.
# Manage users in LEM

This section contains topics related to managing LEM user accounts, including managing user access to LEM data.

## Add LEM users

Access to LEM data requires a user account. Even basic access, such as receiving notifications sent by LEM through email or SMS text message, requires a user account.

## About LEM roles

To restrict user access to sensitive data, user accounts need to be assigned to a LEM role. There are six LEM role types: Administrator, Auditor, Monitor, Contact, Guest, and Reports. Role types are described in the following table.

<table>
<thead>
<tr>
<th>ROLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>The default user. This role cannot be deleted and has full access to the LEM console.</td>
</tr>
<tr>
<td></td>
<td>![i] SolarWinds does not recommend multiple users sharing the Admin account for auditing purposes.</td>
</tr>
<tr>
<td>Auditor</td>
<td>User has extensive view rights to the system, but cannot modify anything other than their own filters.</td>
</tr>
<tr>
<td>Monitor</td>
<td>User has read-only access to the LEM console. See <a href="#">Specify the filters that users assigned the Monitor role can use in the LEM console</a> to configure the filters assigned to this role. Users assigned to this role cannot edit filters.</td>
</tr>
<tr>
<td>Contact</td>
<td>User cannot log in to the LEM console, but can receive external notifications such as email sent to either the user's email address, imported distribution lists, or cellular email-to-SMS addressees for texts. Use this role if you have an external incident resolution or trouble ticket system, or if you have a user who does not need to access the console.</td>
</tr>
<tr>
<td>Guest</td>
<td>User has extensive view rights to the system, but cannot modify anything other than their own filters.</td>
</tr>
<tr>
<td>Reports</td>
<td>User cannot log in to the LEM console, but can access the LEM reports application. This role can access the LEM database over a secure channel if TLS encryption is enabled. See <a href="#">Enable transport layer security (TLS) in the LEM reports application</a> for details.</td>
</tr>
</tbody>
</table>

[i] Do not confuse roles and groups:
Roles restrict the actions a user can perform in LEM.
Groups organize related elements into logical units so that they can be used in LEM rules and filters.

About LEM user accounts

There are two ways to add a user account in LEM:

- Add an Active Directory user account
- Create a local user account

SolarWinds recommends using Active Directory accounts if Microsoft Active Directory is in use at your organization.

Each user should have a valid email address so that the user can receive notifications sent by LEM. SolarWinds recommends that you create distinct users for everyone who needs to receive email notifications from LEM Manager. If you want to send identical notifications to your IT department personnel, associate a distribution list email address to all relevant users.

To establish minimum password requirements for local user accounts in LEM, see Set the global password policy for LEM users.

How Active Directory accounts work in LEM

You can configure LEM to allow users to log in with their Active Directory credentials. Using Active Directory for user authentication means you do not have to maintain duplicate user accounts in LEM, and users do not have to remember an additional user name and password just for LEM.

See Set up Active Directory authentication in LEM to configure LEM to allow users to log in with their Active Directory credentials.

LEM roles are mapped to DS groups in Active Directory if AD authentication is enabled.

See Configure or view Active Directory authentication settings in LEM to look up which Active Directory groups are mapped to LEM roles.

LEM supports Active Directory single sign-on (SSO). If SSO is enabled, users can bypass the LEM login screen and go straight to the application if they are already logged in to another application that accepts the user's AD credentials.

See Set up single sign-on in LEM to configure LEM to allow users to bypass the LEM login screen if they are already logged in to an application that accepts the user's AD credentials.

LEM can use Active Directory groups of Windows users and computer accounts in LEM rules and filters. Any changes made to users or groups in Active Directory propagate to rules and filters in LEM.

See Configure directory service groups in LEM for details.
Import an Active Directory user into LEM

Before you create an Active Directory user account:

- Complete the steps in this topic: [Set up Active Directory authentication in LEM](#)
- Be sure to either map your Active Directory groups to LEM security groups, or create at least one custom security group in Active Directory for LEM to use. If you created custom LEM security groups in Active Directory, populate the groups with AD users before continuing. See [Create custom security groups in Active Directory for LEM to use](#) for details.
- Verify that the user account includes a valid email address.
  
  LEM requires an email address to create a user account. LEM uses the email address to send the user a notification when an assigned alert event occurs.

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Build > Users.
3. Click 📋, and then select Import LEM User. The Import Users form opens.
4. Complete the Import Users form, and then click Import.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEM Groups</td>
<td>Select the LEM security group that the Active Directory user belongs to.</td>
</tr>
<tr>
<td>Search User</td>
<td>Type at least the first three characters of the user name.</td>
</tr>
<tr>
<td>Search</td>
<td>Click to find matching users.</td>
</tr>
<tr>
<td>Available Users</td>
<td>Select one or more users to import and click the green and white arrow button.</td>
</tr>
<tr>
<td>Selected Users</td>
<td>Lists the AD user (or users) to import.</td>
</tr>
</tbody>
</table>

The Active Directory user is imported.

Create a local LEM user account

Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.

1. On the LEM toolbar, navigate to Build > Users.
2. If you have multiple LEM Manager instances, click the drop-down list next to the +, and then choose the LEM Manager instance that will be associated with the user account.
3. Click 📋, and then select LEM User.
4. Complete the form in the User Information for: <New User> section, and then click Save. See the following table for help with form fields.

   The local user account is added to the Users grid.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter a user account name. You cannot use admin_role, audit_role, or reports_role for the user name.</td>
</tr>
<tr>
<td>First Name</td>
<td>Enter the user's first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter the user's last name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a user password to access the Manager. This can be an initial system password or a temporary password that is assigned to replace a forgotten password.</td>
</tr>
<tr>
<td></td>
<td>If you are creating a Contact user, a password is not required. If the Must Meet Complexity Requirements check box is selected in the Manage &gt; Appliance &gt; Properties &gt; Settings tab, the console enforces the following policy:</td>
</tr>
<tr>
<td></td>
<td>• Passwords must have a minimum of six characters. Spaces are not allowed.</td>
</tr>
<tr>
<td></td>
<td>• Passwords must have two of the following three attributes: at least one special character, at least one number, and a mix of lowercase and uppercase letters.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the password again.</td>
</tr>
<tr>
<td>LEM Role</td>
<td>Select a LEM role for this user.</td>
</tr>
<tr>
<td></td>
<td>• Administrator - Has full access to the system, and can view and modify everything.</td>
</tr>
<tr>
<td></td>
<td>• Auditor has extensive view rights to the system, but cannot modify anything other than their own filters.</td>
</tr>
<tr>
<td></td>
<td>• Monitor - Can access the console, cannot view or modify anything, and must be provided a set of filters. See &quot;Specify the filters that users assigned the Monitor role can use in the LEM console&quot; on page 129 for steps.</td>
</tr>
<tr>
<td></td>
<td>• Contact - Cannot access the console, but can receive external notification.</td>
</tr>
<tr>
<td></td>
<td>• Guest - Has extensive view rights to the system, but cannot modify anything other than their own filters.</td>
</tr>
<tr>
<td></td>
<td>• Reports - Cannot log in to the LEM console, but can log in to the LEM reports application. This role can access the LEM database over a secure channel if TLS encryption is enabled. See Enable transport layer security (TLS) in the LEM reports application on page 78 for details</td>
</tr>
<tr>
<td>View Role</td>
<td>Click to open the role privileges assigned to the new user. Role privileges cannot be changed.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a brief description (up to 50 characters). For example, provide the user title, position, or area of responsibility.</td>
</tr>
</tbody>
</table>
**FIELD** | **DESCRIPTION**
--- | ---
Contact Information | Enter an email address. LEM Manager notifies users by email about network security events. You can add as many email addresses as required.

1. Type an email address and click ✪ to add the address to the Contact Information box. Use the following format: username@example.com
2. Click Save, and then click ✉ to send a test email to the email address.
3. Verify that the user received the email test message.
4. Repeat these steps to add additional email addresses.

---

**View user accounts in the LEM console**

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Build > Users.
3. To sort the table, click a column heading. For example, click LEM Role to sort users by role. To reverse sort, click again.

**View the system privileges associated with a role**

After you select a user role, you can click View Role to view the system privileges associated with the user role.

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Build > Users.
3. In the Users grid, select a user.
   Details about the user display in the User Information pane.
4. In the User Information pane, click View Role.
   The Privileges window appears.

ℹ️ The information in the Privileges window is read-only and cannot be changed.
5. To return to the console, click Close.

Edit user account settings

You can update all user settings in the Build > Users view. Only the description and role can be edited for Active Directory users.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Users.
3. In the Users grid, click next to a user, and then select Edit.
4. Update the user information in the User Information pane.
   - To delete an email address, click next to each email address you want to delete.
5. Click Save.
   - The user information is updated.

To establish minimum password requirements for local user accounts in LEM, see Set the global password policy for LEM users.

Delete a user account from a LEM Manager instance

You cannot delete the admin user from the system.
1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Build > Users.

3. In the Users grid, locate the user you want to delete.

4. In the Users grid, click next to the targeted user, and then select Delete.

5. When prompted, click Yes to confirm.
   The user is removed from the Users list and is no longer authorized to use the Manager.

**Set the global password policy for LEM users**

This topic describes how to set minimum password requirements for local LEM user accounts.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Manage > Appliances.

3. In the Properties pane, click the Settings tab.

4. Adjust the Minimum Password Length setting according to your preference.

5. To require complex passwords for LEM users, select the Must Meet Complexity Requirements check box.
   Complex passwords must include any three of the following four character types:
   - Capital letters
   - Lower-case letters
   - Numerals (0–9)
   - Symbols (!, @, #, etc.)

6. Click Save.

**Set up Active Directory authentication in LEM**

Set up Active Directory authentication to allow users to log in to LEM with their Active Directory (AD) credentials.

- These steps apply to LEM version 6.3.1 and newer. To configure older versions of LEM for LDAP authentication, see Set up Active Directory authentication in LEM 6.3.0 and older.
- This task configures LEM for Active Directory authentication. See Set up LEM to monitor Active Directory Accounts to configure LEM to monitor Active Directory accounts for security violations.

**Gather required information**
Before you begin, gather the following:

- Either the IP address or fully-qualified domain name (FQDN) of the Active Directory server.
- The domain credentials for an account that LEM can use to log in to Active Directory. SolarWinds recommends using a service account with a non-expiring password. This account does not need elevated privileges.

To get directory server details, open a Windows command prompt on a computer on the correct network and type `nslookup`.

Create a user in Active Directory that LEM can use to log in

1. Log in to the domain controller and open Active Directory Users and Computers.
2. Create a user account that LEM can use to log in to Active Directory. SolarWinds recommends using a service account with a non-expiring password. This account does not need elevated privileges (such as Domain Admin privileges).

Create custom security groups in Active Directory for LEM to use

User access in LEM is based on Active Directory group membership.

- If you have at least LEM version 6.3.1 Hotfix 2, you can use your existing Active Directory groups for alerts, reports, and so on. Skip this section and go to the next section: Configure or Active Directory authentication settings in LEM.
- If you have either LEM version 6.3.1, or LEM version 6.3.1 Hotfix 1, complete the steps in this section to create the required custom security groups in Active Directory.

1. Log in to the domain controller and open Active Directory Users and Computers.
2. Create at least one security group called `ROLE_LEM_ADMINISTRATORS`. Group names must be identical to the names given below, otherwise users cannot log in to the LEM console. SolarWinds recommends creating LEM group names using capital letters to help you quickly identify LEM groups in Active Directory.

You can add up to six of the following LEM custom groups:

- `ROLE_LEM_ADMINISTRATORS` (Required if you are using LEM 6.3.1 Hotfix 1 or older.)
- `ROLE_LEM_ALERTS_ONLY`
- `ROLE_LEM_AUDITOR`
- `ROLE_LEM_GUESTS`
- `ROLE_LEM_CONTACTS`
- `ROLE_LEM_REPORTS`

The `ROLE_LEM_CONTACTS` group is only used for email notification in rules. Users added to this group do not have login rights.
Configure or view Active Directory authentication settings in LEM

To test the settings, log in with a user name and the fully-qualified domain name (FQDN). The user name and fully-qualified domain should be formatted as follows: user@example.com or example.com\user.

1. **Log in to the LEM admin user interface.**

   If you are not redirected to the Settings page, use the following URL:
   ```
   https://<lem_manager_IP_address>:8080/mvc/configuration
   ```

2. In the Authentication settings, click LDAP Configuration.

   ![Authentication Settings](image)

   The LDAP Configuration Management screen appears.

3. Choose from the following:
   - To configure a new Active Directory LDAP integration profile, click Add New Configuration. The Create LDAP Configuration page opens.
   - To view or edit settings for an existing Active Directory integration profile, click Edit. The LDAP Configuration page opens.
   - To disable an Active Directory integration profile, click the green check mark to make the gray x visible.
   - To enable a disabled Active Directory integration profile, click the gray x to make the green check mark visible.
   - To delete an Active Directory integration profile, click Delete.

4. To create or edit the LDAP configuration, complete the form, and then click Save. Or click Cancel after you review your previously saved LDAP connection settings.

   Starting with LEM 6.3.1 Hotfix 2 you can configure LEM to use existing groups for alerts, audit, reports, and so on. Expand the "Advanced Settings" section to specify custom group names when creating or editing the LDAP configuration settings.
## LDAP Configuration

**Field** | **Description**
---|---
LDAP Configuration Name | Enter a friendly name of your choosing for the LDAP configuration.
IP Address or Hostname | Enter the IP address or host name of your LDAP server.
Domain | (LEM 6.3.1 Hotfix 2 and newer only) Enter the fully-qualified domain name for the account store.
Directory Service Server User Name | Use the format account_name@example.com. SolarWinds recommends using a Directory Service account to prevent integration issues if the software license expires. The user name does not require special privileges (such as Domain Admin) to be a Directory Service user.
Directory Service Server Password | Enter the password for the user account.
<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use SSL Encryption</td>
<td>(Optional) Select to use the transport layer security protocol (LDAPS) for a secure connection. This option directs traffic from the LEM VM to a designated server (usually a domain controller) for use with the Directory Service tool.</td>
</tr>
<tr>
<td>LDAP Port</td>
<td>If this field is left empty, LEM uses the default LDAP port (port 389). Otherwise, enter the port number used by your domain controller. The default LDAP port with SSL encryption (LDAPS) is 636.</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td>(LEM 6.3.1 Hotfix 2 and newer only)</td>
</tr>
<tr>
<td>• Domain Aliases</td>
<td>Specify any Domain Alias names that should be authenticated using this LDAP configuration. (The role/group names configured on this page will also apply.)</td>
</tr>
<tr>
<td>• NetBIOS Names</td>
<td>Specify any NetBIOS names that should be authenticated using this LDAP configuration. (The role/group names configured on this page will also apply.)</td>
</tr>
<tr>
<td>• Admin Group</td>
<td>Specify the DS group in Active Directory to use for the LEM administrator role. If you do not specify a name, the default ROLE_LEM_ADMINISTRATORS group is used.</td>
</tr>
<tr>
<td>• Alerts Only Group</td>
<td>Specify the DS group in Active Directory to use for the LEM alerts role. If you do not specify a name, the default ROLE_LEM_ALERTS_ONLY group is used.</td>
</tr>
<tr>
<td>• Audit Group</td>
<td>Specify the DS group in Active Directory to use for the LEM auditor role. If you do not specify a name, the default ROLE_LEM_AUDITOR group is used.</td>
</tr>
<tr>
<td>• Guest Group</td>
<td>Specify the DS group in Active Directory to use for the LEM guest role. If you do not specify a name, the default ROLE_LEM_GUESTS group is used.</td>
</tr>
<tr>
<td>• Notify Only Group</td>
<td>Specify the DS group in Active Directory to use for the LEM notifications role. If you do not specify a name, the default ROLE_LEM_CONTACTS group is used.</td>
</tr>
<tr>
<td>• Reports Group</td>
<td>Specify the DS group in Active Directory to use for the LEM reports role. If you do not specify a name, the default ROLE_LEM_REPORTS group is used.</td>
</tr>
</tbody>
</table>

Your LDAP configuration settings are now complete.
To test the settings, log in with a user name and the fully-qualified domain name (FQDN). The user name and fully-qualified domain should be formatted as follows: user@example.com or example.com\user.

Add an Active Directory user to LEM

To grant a user access to LEM, add the user to the appropriate role (security group) in Active Directory.

LEM does not support nested Active Directory groups.

1. Open Active Directory Users and Computers.
2. Add the user to the appropriate role (security group) in Active Directory. Users added to the ROLE_LEM_CONTACTS group do not have sufficient privileges to log in to LEM.
   - For LEM 6.3.1 Hotfix 2 and higher, add the user to an Active Directory security group that is configured for use with LEM. To see which groups are configured for LEM, open the LDAP Configuration Management page and expand the list under Advanced Settings. See Configure or view Active Directory authentication settings in LEM for details.
   - For LEM version 6.3.1, or LEM version 6.3.1 Hotfix 1, add the user to one of the Active Directory security groups listed under Create custom security groups in Active Directory for LEM to use. At least one user should be assigned to the ROLE_LEM_ADMINISTRATORS security group.

When configuring user accounts, make sure the user's Primary group is not assigned to a custom group, otherwise the user cannot log in to LEM. The user will see an Invalid username and password message instead, and a message like the following will be logged:

[LemSpringSecurityAuthManager] {http-nio-8080-exec-1:349} Authentication failed: User is not member of any required role group!

Set up Active Directory authentication in LEM 6.3.0 and older

These steps apply to LEM version 6.3.0 and older. To configure newer versions of LEM (version 6.3.1 and above), see Set up Active Directory authentication in LEM

Complete the steps in this topic to allow users to log in to LEM with their Active Directory credentials.

Configure the Directory Service Query connector

Before you begin, gather the following:

- Either the IP address or fully-qualified domain name (FQDN) of the Active Directory server.
- The domain credentials for an account that the Directory Service Query connector can use.
To get directory server details, open a Windows command prompt on a computer on the correct network and type nslookup.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. Select the LEM Manager.

3. On the LEM toolbar, navigate to Manage > Appliances.

4. Click the gear icon next to your LEM Manager, and then select Connectors.

5. Enter Directory Service Query in the search box on the Refine Results pane.

6. Click the gear icon next to the master connector on the right, and select New.

7. Complete the Directory Service Query connector form:
   a. In the Domain Name field, enter the fully-qualified domain name for your directory service server using lowercase characters.
      For example, example.com.
   b. In the Directory Service Server field, enter the IP address or hostname of your directory service server.
   c. SolarWinds recommends using the IP address to avoid possible DNS issues. The LEM network configurations (netconfig) allow for setting or changing the DNS server to resolve the host.
   d. Enter the domain credentials for a user account that the connector can use.
      SolarWinds recommends using a service account with a non-expiring password, otherwise you will have to manually update the connector every time the password expires. This account does not need elevated privileges. When entering domain credentials, provide only the user name.
   e. If the Active Directory server supports encryption, select TLS or SSL from the Encryption drop-down list. Otherwise, select No SSL.
   f. If using a non-standard port, enter it in the Custom Port field.

8. When finished, click Save.

9. Locate the new instance of the connector. The gray icon in the Status column indicates that the connector is not running.

10. Click the gear icon next to the new connector, and then select Start. A green icon in the Status column indicates that the connector is running.

A green icon in the Status column indicates that the connector is running.
Test the Directory Service Query connector settings

1. Click the Test Domain Connection button at the bottom of the connector settings pane.
2. Create an nDepth query. See Create an nDepth query for steps.
   - Expand the Event Groups menu, select Any Alert, and drag EventInfo into the nDepth search bar.
   - Enter *Connection to* in the search field.
3. Run the search.
4. To view the results, click Results Details on the nDepth explorer toolbar.
5. Check the EventInfo field to verify that it does not say Connection to Directory Service failed.

Import your Active Directory organizational groups into LEM

Complete these steps to import your directory service groups into LEM Manager and start the group synchronization process. The synchronization process runs every five minutes if the connector is running.

Before you begin, the Directory Service Query connector must be configured on LEM Manager.

1. Log in to the LEM console.
2. On the LEM toolbar, navigate to Build > Groups.
3. Click the plus button in the upper right corner, and then select Directory Service Group.
4. In the details pane at the bottom of the LEM console window, select a group category from the folder tree on the left to populate the Available Groups pane on the right.
5. Check the boxes next to the groups you want to import into LEM Manager.
6. Repeat Steps 4 and 5 until you have selected all the groups you want to import.
7. Click Save.

Import an Active Directory user and assign the user LEM login rights

1. Log in to the LEM console.
2. On the LEM toolbar, navigate to Build > Users.
3. Click ✍, and then select Import LEM User.
   - The Import Users dialog opens.
4. Complete the form to select the user to be given LEM console login rights.
   - LEM Groups – Choose All to search for a user across all security groups, or choose a specific security group to limit your search to just that group.
   - Search User – Type a portion of the user name to search for. You must type at least three letters.
   - Search – Click search to get a list of users that meet the search criteria. Search will not return more than 10 users.
• Available Users – Select one or more users to import from the search results.
• Selected Users – Click the green arrow to move users from the Available Users list to the Selected Users list.

5. Click Import.
   The system adds the user to the Users view list.

6. In the Users list, select the user and verify that the user's email address appears in the Contact Information box.
   If the email address is missing, Active Directory is not configured to supply this information and you will not be able to send email notifications to this user. You can create the email address or add it to a local user when rules fire.

Set up single sign-on in LEM

LEM supports Active Directory (AD) single sign-on (SSO). When enabled, LEM does not request a user name and password if the user is already logged in to AD. Instead, AD authenticates the user in the background, and automatically logs the user in to LEM with the appropriate user access rights. User access in the LEM consoles (desktop, web, and the LEM reports application), is based on AD group membership.

Set up Active Directory authentication in LEM

First configure Active Directory (AD) authentication and verify that users can log in to LEM with their AD credentials. For details, see Set up Active Directory authentication in LEM. After verifying that users can log in to LEM with their AD credentials, complete the next step.

Generate a keytab file using Ktpass

To configure LEM for Active Directory (AD) SSO, a Kerberos keytab file is required. LEM uses this file to authenticate users with AD and to enforce user account security. The keytab file is exported from AD and imported into LEM, and contains a table of AD user accounts, along with the encrypted hash of each user's password. Ktpass is the Windows Server command-line tool that generates the .keytab file, as well as the shared secret key that LEM uses to securely authenticate users with AD.

Before you run the ktpass command, gather the following information:

• Fully-qualified domain name (FQDN) of the LEM VM – The FQDN is the complete domain name of the LEM virtual machine on the Internet. It includes the host name (the label assigned to a device on the network), and the name of the domain that hosts the device. For example, if the device name is swi-lem and the company domain is yourcompany.local, the FQDN is swi-lem.yourcompany.local.

• Realm – This is the Active Directory Domain Services (AD DS) domain name. The realm name is used to route authentication requests to the AD server that holds user credentials. The realm name is case sensitive and normally appears in upper-case letters. To simplify your Kerberos client configuration, make the realm name identical to your DNS domain name by only using upper-case letters. For example, if YourCompany belongs to the DNS domain name yourcompany.com, the
Kerberos realm should be YOURCOMPANY.COM.

- Service principal name (SPN) – The SPN provides an alias (or pointer) to your domain account. The SPN consists of the FQDN, followed by the @ symbol, followed by the realm.

For example, the SPN for a device named swi-lem located at http://www.yourcompany.com would be http/swi-lem.yourcompany.local@YOURCOMPANY.COM where swi-lem.yourcompany.local is the FQDN, and YOURCOMPANY.COM is the realm.

1. Do the following to obtain the LEM host name and IP address:
   a. Open the LEM CMC command line. See Log in to the LEM CMC command line interface for steps.
   b. At the prompt, enter appliance to access the Appliance menu.
   c. At the prompt, enter viewnetconfig.
   d. When prompted, enter b to select the brief network configuration.
   e. Record the domain name, host name, and the host name's resolved IP address.
   f. Exit the management console.

2. Create a new user (host) in DNS:
   a. Open DNS manager on your domain controller.
   b. Create an A record entry for LEM on the DNS server using the host name and IP address. Verify that DNS Manager populated the domain field with the correct domain membership.

3. Open Active Directory Users and Computers.
4. Create an organizational unit (OU) and name it Keytab.
5. Select the Keytab OU and create a new user account (or Service Principle Name [SPN]).

   Write down the SPN. You will need it in a later step.

6. Use the Kerberos keytab file using the ktpass command:
   a. Log in to the Active Directory server as an administrator.
   b. Open a command prompt as an administrator.
   c. Run the following ktpass command:
ktpass -princ HTTP/<fqdn>@<REALM> -pass <SPN_account_password> -mapuser <domain_name>\<user_name> -pType KRB5_NT_PRINCIPAL -crypto ALL -out c:\lem.keytab

If you receive an error when you run the command, replace the -mapuser argument with -mapuser <user_name>.

The ktpass command takes the following arguments:
- `-princ` specifies the server principal name (SPN) in the form HTTP/<fqdn>@<REALM>. You will use this path in your LEM configuration.
- `-pass` is the SPN account password.
- `-mapuser` maps the Kerberos principle name (specified in the `-princ` argument) to the specified domain account.
- `-pType` specifies the principal type as Kerberos 5 for Microsoft Windows.
- `-crypto` specifies the encryption type. Entering `ALL` indicates all supported types. This can include Data Encryption Standard (DES), Rivest Cipher 4 (RC4), and Advanced Encryption Standard (AES) encryption types. See "ktpass" on the Microsoft TechNet website for more information about supported crypto types.
- `-out` specifies the name and location for the generated Kerberos 5 keytab file.

7. Navigate to the keytab file location (for example, `c:\lem.keytab` specified in the `-out` argument).

8. To allow LEM access to Active Directory, import the keytab file into LEM.

Configure SSO settings in LEM using the Admin web console

You can use the command line to configure SSO settings in LEM. For details, see Configure SSO settings in LEM using the command-line.

1. Open a web browser and connect to the LEM Admin user interface using the following URL:
   
   https://<lem_manager_IP_address>:8443/mvc/login
   
   If you have not yet activated LEM, or if you reopened port 8080, use the following URL:
   
   http://<lem_manager_IP_address>:8080/mvc/login
   
   You can also access the Admin user interface by entering `admin` at the cmc> prompt.

2. Enter your name and password in the log in screen.
   
   The Settings/Authentication page opens.
3. Click SSO Configuration.

![SSO Configuration](image)

4. Complete the form:

![ADD SSO CONFIGURATION](image)

**WARNING!**
For security reasons, when SSO is enabled, local user authentication will be disabled. If you are logged in as a LEM local user, when you click the “Save” button below, you will be logged out of the LEM. Log back in using your SSO/LDAP credentials.

a. Enter the SPN in the Service Principle Name (SPN) field. See Generate a keytab file using Ktpass for details.

For example: `http/swi-lem.yourcompany.local@YOURCOMPANY.COM`

b. Click Browse, and then select the keytab file.

5. Click Save.

Your keytab file is uploaded to LEM. If you are logged in as a local user, LEM logs you out of the Admin user interface.

SSO is now configured on LEM.

**Configure web browser settings for SSO**

Follow the appropriate procedure to enable Kerberos authentication for SSO in your web browser.

**Internet Explorer**

By default, Internet Explorer does not restrict the transmission of login credentials for intranet sites. However, your company may have policies that have this restriction on intranet sites.
To add the LEM Manager URL to the list of trusted intranet sites:

1. Open Internet Options.
2. Under Security, set your local intranet sites to automatically detect an intranet network with no other options.
3. In your Local intranet Advanced settings, add your FQDN or URL as a website in the Local Intranet zone.
   For example:
   swi-lem or https://swi-lem
4. Save your settings and close Internet Options.

**Mozilla Firefox**

1. Open Firefox, and then enter about:config in the address bar.
2. In the Filter field, enter network.negotiate-auth.trusted-uris.
3. In the list, double-click network.negotiate-auth.trusted-uris.
4. Enter the fully-qualified domain name (FQDN) or URL that you use for LEM.
   For example: mylemappliance.example.com
   The web browser is now configured for SSO.

**Google Chrome and Opera**

Add the LEM Manager URL to the list of trusted intranet sites in Internet Explorer, and then install Chrome or Opera on your workstation. Chrome and Opera inherit their settings from Internet Explorer if they were installed after you entered the trusted intranet sites into Internet Explorer.
Configure LEM for either SSO-only authentication, or SSO and local authentication

Complete these steps to configure which credentials users can use to log in to LEM. You can allow users to log in with either local LEM credentials or SSO (LDAP) credentials, or you can restrict users to only SSO (LDAP) credentials.

1. Log in to the LEM admin user interface. See Log in to the LEM admin user interface for steps.
2. Click SSO Configuration.
   
   The SSO Configuration Management screen opens.

3. To enable the service, click the toggle switch.

4. Click the Enabled authentications list and choose from the following:
   - Credentials and SSO – Allows users to log in with either local LEM credentials or SSO (LDAP) credentials.
   - SSO only – Restricts users to log in with only SSO (LDAP) credentials.

5. Click Save.

Updates take place immediately. Log in using the appropriate credentials to verify that the settings are correct.
Configure SSO settings in LEM using the command-line

Use these alternate steps if you do not want to use the LEM admin user interface to upload the keytab file. (You do not have to repeat this process if you already uploaded the keytab file to LEM.)

1. Log in to the CMC command-line interface. See Log in to the LEM CMC command line interface for steps.

2. At the cmc> prompt, enter import.

3. Follow the prompts on your screen to complete the import.
   The file is uploaded in the appliance file system.

4. Return to the management console menu.

5. At the cmc> prompt, enter admin to access the admin command-line interface.

6. Enter your user name and password.

7. Arrow down to LOGIN, and then press Enter.

8. Arrow down to SSO configuration, and then press Enter.
9. Arrow down to Add New Configuration, and then press Enter.

   i The content on this screen may vary with your LEM implementation.

10. Enter your SSO configuration settings.

    a. Enter the Service Principle Name (SPN). See Generate a keytab file using Ktpass for details.
       For example: http/swi-lem.yourcompany.local@YOURCOMPANY.COM

    b. Enter the path to your keytab file using the following syntax:
       /var/transfer/storage/<your_keytab_file_name>.keytab

11. Arrow down to Save, and then press Enter.
    The upload is completed.
12. Exit the management console.

SSO is now configured on your appliance.

Updates take place immediately. Log in using the appropriate credentials to verify that the settings are correct.

**Change the LEM CMC password**

The CMC command-line interface (CLI) is used to connect to the LEM VM and perform administrative tasks. SolarWinds recommends that you periodically change the password used to access the CMC command-line.

These steps require the current CMC password. The default password is `password`.

1. Log in to the CMC command-line interface. See [Log in to the LEM CMC command line interface](#) for steps.
2. Type `appliance`, and then press Enter.
3. Type `password`, and then press Enter.
4. Complete the wizard to change the password. See [Special characters allowed in CMC commands and passwords](#) for help choosing a CMC password.
5. To return to the root CMC command line, type `exit`, and then press Enter.
6. To log out and close the CMC interface, type `exit`, and then press Enter again.

Test the new CMC password by logging back in to the CMC interface.

**Recover a lost CMC password**

Contact SolarWinds Support for help if you no longer have the CMC password needed to log in to the CMC interface. You can still access the CMC interface without the CMC password by logging into the VM console through the hypervisor and clicking on Advanced Configuration.

**Specify the filters that users assigned the Monitor role can use in the LEM console**

LEM users assigned to the Monitor role can use the filters they have access to, but they cannot create, edit, delete, or import/export filters.

See [About LEM roles](#) to learn more.

By default, this role has access to the same set of filters as other users. To remove and/or modify the filters that Monitor-role users can access in the console, complete the following steps. You will need to complete some of these steps on the end-user's computer. When the user logs in to LEM using the same computer and Windows profile, they will only have access to the filters specified.
1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. Temporarily assign the user to the Administrator role.

3. Instruct the user to log in to the LEM console using their Windows profile.

4. Change the filters as needed, deleting any unnecessary filters.

   If you created and exported the filters in a previous procedure, you can add new filters to the user Filters list by creating or importing the filter as appropriate. To remove a filter from the user Filter list, point to the filter and click x that appears to the right.

5. Log out the user and close the console window.

6. Using your administrator login, change the user back to the Monitor role.

7. From the user computer, have the user log in with their credentials, and then click Monitor.

   The user should only see the specified filters.
Send event data to LEM via Agents, syslog, and SNMP

This chapter describes how to configure LEM to receive events from systems, devices, and applications in your IT environment. LEM can receive events sent by LEM Agents, syslog, and SNMP.

LEM can correlate SNMP traps from devices and applications that have a corresponding connector. To configure LEM to receive SNMP traps, turn on the SNMP Trap Logging Service. See Enable LEM to receive SNMP traps by turning on the SNMP Trap Logging Service for details.

Get started adding systems and devices to LEM

This section describes how to add Agent devices (servers, domain controllers, and workstations), and non-Agent devices (firewalls, routers, and switches) to LEM.

There are two ways to configure computers and devices on your network to send log events to LEM:

- To add servers, domain controllers, and workstations, install a LEM Agent.
- To add firewalls, routers, or switches, configure your devices to send log events directly to the LEM VM using syslog or SNMP traps. After configuring your device to log to LEM, configure the appropriate connectors directly on the LEM Manager.

Click the video icon to view a tutorial about adding devices to LEM.

About the LEM Agent

Install the LEM Agent on servers, domain controllers, and workstations to monitor local events on the systems in your network. The LEM Agent is a stand-alone service that collects and normalizes log data on the remote system before it is sent to the LEM Manager for processing.

See Install LEM Agents to protect servers, domain controllers, and workstations in the LEM Installation Guide for installation steps.

LEM Agents can:

- Capture events in real time.
- Encrypt and compress the data for efficient and secure transmission to the LEM Manager.
- Buffer the events locally if the Agent loses network connectivity to the LEM Manager.

In addition to monitoring local events, the Agent provides event alerting on workstations and servers. It is also required for some active responses, including logging off a user, shutting down a computer, and detaching a USB device. You can trigger actions manually from the LEM console using the Respond menu, or you can create rules to take specific actions automatically.
Install the LEM Agent on computers that allow third-party software, including servers, domain controllers, and workstations. On Windows, the LEM Agent captures log information from sources such as Windows Event Logs, a variety of database logs, and local anti-virus logs.

SolarWinds recommends installing the LEM Agent if you have the option. If installing the LEM Agent is not feasible, send log events directly to LEM.

About sending log events directly to LEM

Configure non-Agent devices, such as firewalls, routers, or switches, to send log events directly to the LEM Manager using syslog or SNMP traps. Then, configure the appropriate device connector on the LEM Manager using the LEM console. For a complete list of supported devices, see the LEM Connector List on THWACK.

Configure LEM Agents after they are installed

This section documents LEM Agent configuration tasks.

After installation, the LEM Agent captures log information from sources such as Windows Event Logs, database logs, and local antivirus logs. Additionally, the LEM Agent allows LEM to take specific actions that you can define as rules. You can trigger actions manually from the LEM console using the Respond menu.

View the LEM Agents monitored by each LEM Manager

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Manage > Nodes.
   
   The Nodes view displays the LEM Agents monitored by each of your LEM Managers.

About the LEM Agent for Windows connectors

The LEM Agent for Windows includes several preconfigured connectors that collect and display data from these systems immediately after you install the LEM Agent. By default, the LEM Agent for Windows includes the following preconfigured connectors:

- Windows Security Log (for the host OS version)
- Windows Active Response
- Windows Application Log
- Windows System Log

- For broader coverage on your Windows computers, configure specific connectors to obtain your targeted data. See Enable additional connectors to add extra log sources to LEM for steps.
Enable additional connectors to add extra log sources to LEM

Use the following procedure to add additional log sources to your monitored Agent nodes (if desired).

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes, and then select the node you want to configure.
3. Click ➤, and then select Connectors.
4. In the Connectors grid, select a supported device or application to log.

   ![Enter a keyword in the Search field or click the Category drop-down menu to filter connectors by category.](image)

5. Next to your selected connector, click ➤, and then select Enable.
6. Click Close.
7. Repeat step 1 through 5 to add additional log sources to your nodes.

Create connector profiles to manage and monitor LEM Agents

This section explains the purpose for connector profiles and provides instructions for creating them.

See also:
- Configure LEM Agents after they are installed
- Edit LEM Agent connector-profile settings

About connector profiles

Use a connector profile to group Agents that share the same connector configuration. You can use the profile to configure a set of standardized connector settings, and then apply those settings to all Agents assigned to that profile. Once applied, every Agent in the profile will have the same connector settings.

Connector profiles maintain all Agents in a profile by updating only the profile connector configuration. The system then propagates your changes to all the Agents in the profile.

Most Agents in a network have only a few different connector configurations. Using connector profiles, you can streamline the process of connecting your network security products to LEM. If you decide not to use connector profiles, you must create at least one connector instance for every product that you intend to integrate with LEM, and then repeat this process for each Agent.

A well-planned set of connector profiles provides you with a versatile and efficient method for configuring and maintaining your Agent connector configurations. You can create as many connector profiles as you need to reflect each of your common connector configurations. For example, you can set up a standard user workstation profile, a web server profile, and so on. SolarWinds provides several default connector profiles that address common configurations.
About the connector-profile group type

LEM lets you use connector profiles in filters, rules, and searches. After you define a connector profile, you can use it in rules and filters to include or exclude the Agents associated with that profile. For example, you can create a filter using the Domain Controller connector-profile group to show web traffic from the computers in that group.

Groups organize related elements for use with LEM rules and filters. See About LEM groups for information about the various LEM group types.

Connector profile guidelines

A well-planned set of connector profiles provides you with a versatile and efficient method of updating and maintaining your Agents’ connector configurations.

When you configure your connector profiles, use the following guidelines:

- An Agent can only be a member of one connector profile. You cannot add an Agent to multiple connector profiles.
- You can only add a connector profile to one LEM Manager at a time. Each connector profile you create only applies to the LEM Manager you selected when you created the profile. To copy a connector profile for use with another LEM Manager, export the profile and then import it into the other Manager’s Groups grid. See Export a group for steps.

Create a connector profile: process overview

This section provides an overview of the steps required to create a connector profile. Creating a connector profile is a three-step process:

1. Install the LEM Agent software on all the systems that you want to include in your new connector profile, then configure a single LEM Agent to serve as the template for your connector profile.
2. Add the Agents to the connector profile. When completed, the system applies the template to all Agents in the profile.
3. Verify the connector status.

When you select an Agent for a template, ensure the Agent has a configuration that mirrors your concept of the final connector configuration.

You can prepare a template Agent in advance by configuring an Agent you know will be a member of the new profile. When completed, use the Agent as the template for the new profile. This process minimizes your need to edit the profile connector configuration in the future.

To clone and/or edit a connector-profile, see Edit LEM Agent connector-profile settings.
Create a connector profile: detailed steps

This section provides detailed instructions for creating a connector profile.

Task 1: Configure the Agent that will serve as a template for your connector profile

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. On the Groups grid connector bar, click , and then select Connector Profile.
4. Complete the connector profile selections.

The following table describes how to configure the Connector Profile form fields.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the connector profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Briefly describe the connector profile.</td>
</tr>
<tr>
<td>Template</td>
<td>Click the Template drop-down menu and select the Agent with the connector configuration that will provide the template for this profile. If you decide not to use a template, select None.</td>
</tr>
<tr>
<td></td>
<td>For best results, select a template when you create a new connector profile. Otherwise, the profile will delete the connectors on every Agent in the profile.</td>
</tr>
<tr>
<td></td>
<td>If you decide not to use a template, click Edit Connectors and add connectors to the profile before you add Agents and save the profile. Otherwise, there will be no connectors in the profile. When you save the profile, any Agents in the profile will lose their connectors.</td>
</tr>
</tbody>
</table>
**FIELD** | **DESCRIPTION**
---|---
LEM Manager | Click the Manager drop-down list and select the Manager that will host the group. If you are editing an existing group, this field displays the Manager currently hosting the profile. If your targeted Manager is not included in the list, click Manage > Appliances and log on to the Manager. You must be logged on to a Manager to create groups.

Save | Click Save to save your changes.

5. Click Save.

The new connector profile appears in the Groups grid.

**Task 2: Select the Agents that are members of the profile**

Before you begin, be sure that the connector profile you created in task 1 is selected in the Groups grid.

The Connector Profile form contains two columns:

- Available Agents list each Agent that is not in the connector profile for the associated Manager.
- Contained Agents list the Agents included in the connector profile.

To add Agents to a Connector Profile:

1. In the Groups grid, locate and double-click the new connector profile.

   The profile appears in the Connector Profile form. The Agent you selected as a template appears in the Contained Agents list by default.

2. Add or remove Agents from your connector profile.

   Click ![arrow] or ![arrow] to move one or all selected Agents from the Available Agents column to the Contained Agents column. These Agents are added to the connector from the connector profile.

   Click ![arrow] or ![arrow] to move one or all selected Agents from the Contained Agents column to the Available Agents column. These Agents are removed from the connector profile.

3. Click Save.

   The system applies the configuration to every Agent you added to the profile.

   If you remove an Agent from a connector profile that was previously saved with that profile, the Agent retains the connector configuration from the profile, but will no longer have membership in the profile.

**Task 3: Verify the connector status**

Some Agents in a connector profile will not use the same logging path for a connector. Be sure to check the configured connector status of each Agent. If the connector status is a ![icon] icon, the connector is not running and may have a different logging path. To resolve this issue, add another connector instance to the profile connector catalog that points to an alternate logging path or create a new profile with an alternate logging path.
Edit LEM Agent connector-profile settings

This topic describes how to clone or edit a connector profile, and how to add, edit, or delete the connector instances associated with a connector profile.

See also:
- Create connector profiles to manage and monitor LEM Agents

Open the connector profile settings for editing

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. In the Groups grid, locate the connector profile you want to edit.
4. Click Edit, and then select Edit.
   
   The Connector Profile pane opens at the bottom of the page, displaying the Agents in the profile.

Clone a connector-profile instance

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. In the Groups grid, locate the connector profile you want to clone.
4. Click Edit, and then select Clone.
   
   The Groups grid displays a new instance of the connector profile.
5. See Edit the connector-profile settings to change the settings of the cloned connector profile.

Editing a connector profile instance

Use the Edit Connectors command in the connector profile form to add, edit, or delete the connector instances associated with the profile.

Changing a connector profile changes the connector configuration of every Agent associated with the profile.

When you edit an Agent, you must stop and start each connector instance to edit the running Agent's configuration. When you edit a connector profile configuration, stopping or starting each connector instance is not required, but you must activate your changes.
When you edit the connector configuration in a connector profile, you are modifying the profile configuration data, not the actual Agent. When you edit a connector profile, you do not change the Agents that are members of the profile until you click Activate. After you activate the profile, the system automatically updates all Agents that are members of the profile, stops each connector instance, makes the necessary changes, and then restarts each connector instance.

Edit the connector-profile settings

Before you begin, see Editing a connector profile instance.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. In the Groups grid, locate the connector profile you want to edit.
4. Click , and then select Edit.
5. In the Properties form, update the connector settings, as needed.

<table>
<thead>
<tr>
<th><strong>FIELD</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the connector profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Briefly describe the connector profile.</td>
</tr>
<tr>
<td>LEM Manager</td>
<td>This field is read only. To copy a connector profile for use with another LEM Manager, export the profile and then import it into the other Manager's Groups grid. See Export a group for steps.</td>
</tr>
<tr>
<td>Available Agents/Contained Agents</td>
<td>Add or remove Agents from your connector profile. An Agent can only be a member of one connector profile. You cannot add an Agent to multiple connector profiles.</td>
</tr>
</tbody>
</table>

Click or to move one or all selected Agents from the Available Agents column to the Contained Agents column. These Agents are added to the connector profile.

Click or to move one or all selected Agents from the Contained Agents column to the Available Agents column. These Agents are removed from the connector profile.
Field Connectors

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Connectors</td>
<td>Click Edit Connectors (in the bottom left corner of the Connector Profile pane) to edit the connectors in the connector profile.</td>
</tr>
<tr>
<td></td>
<td>a. Find the connector to configure:</td>
</tr>
<tr>
<td></td>
<td>• Type part of the connector name in the search box, or use the filter menus in the Refine Results pane.</td>
</tr>
<tr>
<td></td>
<td>• To restrict the list to only configured connectors, select Configured.</td>
</tr>
<tr>
<td></td>
<td>b. Next to the connector instance, click 🎨, and then select New.</td>
</tr>
<tr>
<td></td>
<td>c. Complete the connector configuration form. The following fields are common across most connectors:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alias</strong>: Enter a user-friendly label for your connectors.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Log File</strong>: Enter the location of the log file that the connector will normalize. This is a location on either the local computer (Agents), or the LEM appliance (non-Agent devices).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Output</strong>, <strong>nDepth Host</strong>, and <strong>nDepth Port</strong>: You only need to configure these values if LEM is configured to save raw (unnormalized) log messages.</td>
</tr>
<tr>
<td></td>
<td>d. Click Save, and then choose from the following:</td>
</tr>
<tr>
<td></td>
<td>• Click Activate to apply your changes to all Agents associated with the connector profile.</td>
</tr>
<tr>
<td></td>
<td>• Click Discard to discard your changes and reload the previous connectors configuration.</td>
</tr>
<tr>
<td></td>
<td>e. To close the Connector Configuration form and return to the Groups grid, click Close.</td>
</tr>
</tbody>
</table>

Save

To save your changes, click Save.

6. To save the connector profile, click Save.

7. To apply your changes to all Agents associated with the connector profile, click Activate. To discard your changes and reload the previous connectors configuration, click Discard.

At times, not all the Agents in a profile will use the same logging path for a particular connector. You can verify this by checking the Agent's configured connector status. If a connector has a not running status, the connector may have a different logging path.

To correct this problem, you may want to add another instance to the connector profile's connector catalog that points to the alternative logging path. You can also create a new profile that has the alternative logging path.

8. Repeat this procedure for each connector instance you want to reconfigure.

9. To return to the Groups grid, click Close.
Add additional connectors to a connector profile

See [Edit the connector-profile settings](#) and click Edit Connectors when you update the connector settings.

**Add syslog and Agent nodes to LEM**

This section describes several different ways you can add syslog and Agent nodes to LEM so that LEM can monitor their events.

**Add a syslog node to LEM using the Add Node wizard**

Complete these steps to add a syslog node to monitor a network device. The wizard locates the new node for you and recommends the appropriate connector.

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Click Add Node.
4. Select Syslog node.
5. Enter the IP Address of the node.
6. From the drop-down list, select a node vendor.
7. Configure the node so LEM can receive syslog messages.
8. Select the I have configured this node so that LEM can receive its Syslog messages check box.
9. Click Next.

   LEM scans for new devices.

**Use Scan for New Nodes to find new syslog sources and add connectors**

Use the Scan for New Nodes feature to configure and enable multiple connectors simultaneously.

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, click Ops Center, and then locate the Node Health widget.
3. Click Scan for New Nodes in the widget toolbar.
LEM begins scanning for new nodes in your network. If new nodes are found, the New Connector(s) found banner displays in the console. Otherwise, the No nodes found banner displays.

This process may require several minutes to complete. During the scan, a message appears indicating the scan is continuing in the background. A progress bar also displays at the bottom of the console.

4. Click View Now.

5. Select the recommended connectors you want to install, and then Click Next.

Move your pointer over the connector name for details.

6. Review the Summary information, and then click Finish.

The Nodes grid displays with the new nodes.

Click Monitor to view the events collected from the new nodes.

7. On the LEM toolbar, navigate to Manage > Appliances.

8. Click , and then select Connectors.
9. In the Refine Results pane, enter a keyword for your new connector.

![Refine Results pane with keyword search]

10. Locate your connector in the list.

<table>
<thead>
<tr>
<th>Status</th>
<th>Category</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Application Switch</td>
<td>Cisco Content Services Switch</td>
</tr>
<tr>
<td></td>
<td>Firewalls</td>
<td>Cisco IOS Active Response</td>
</tr>
<tr>
<td></td>
<td>Firewalls</td>
<td>Cisco PIX and IOS</td>
</tr>
<tr>
<td></td>
<td>Firewalls</td>
<td>Cisco PIX and IOS Connector Discovery</td>
</tr>
<tr>
<td></td>
<td>Firewalls</td>
<td>Cisco PIX/ASA/FWSM Active Response</td>
</tr>
<tr>
<td></td>
<td>Firewalls</td>
<td>Cisco SA500 Series Security Appliances</td>
</tr>
</tbody>
</table>

11. Next to the connector, click 👁️, and then select Edit.
12. Edit your connector settings as required, and then click Save.

The node connector is enabled.

Manually add a new Agent or syslog node connector

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. In the Nodes grid, locate the nodes that are monitored by LEM.
4. Next to your targeted node, click 👁️, and then select Connectors.
5. Search Agent nodes by category or use the search box to locate a node by keyword.
6. Next to a search result, click 👁️, and then select new.
7. Configure the new node.
8. To start the node, click Start.

Other ways to add nodes to LEM

You can add nodes from the Getting Started wizard by clicking Add Nodes to Monitor.

![Add network devices, desktops and servers to monitor]

A dialog box prompts you to choose the type of node you want to add.

Click the drop-down list, select an Agent or non-Agent node to monitor, and then follow the instructions to add the monitored node.
You can also click Add Node in the Node Health widget to perform the same function.

Add Node(s)

Select node type above to quickly add:
For more information on adding node(s), see Adding Nodes, Devices and Systems.

Select node type
- Syslog
- Windows
- Linux
- HP
- AIX

Update LEM Agents

This section describes how to update LEM Agents on remote or local Windows computers.

Manually update LEM Agents on Windows installations using the LEM Local Agent Installer

Check the LEM release notes or ReadMe file first to be sure that the LEM Agent version you are planning to install is compatible with your installed LEM Manager version.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Manage > Nodes, and then select Agent from the Node drop-down list.

3. In the Nodes pane, select the LEM Agent(s) to upgrade. Press <Ctrl> when you click to select more than one Agent.

4. Select Add Node, and then select Agent node.

5. Select one of the following:
   - Remote Installation if you need to push SolarWinds Log & Event Manager Agents to Microsoft Windows hosts across your network.
   - Local Installation if you will log in to the device that you want to install the Agent(s) on.

6. If installing locally:
   a. Copy the setup.exe file to the computer's local hard drive.

      Security settings in newer versions of Windows may require you to copy the setup.exe files to the local hard drive on the computer.

   b. Log into the computer, right-click the installer, select Run as administrator, and complete the installation wizard.
Manually upgrade LEM Agents on Unix, Linux, Mac, and Windows hosts using LEM Remote Agent Installers

If you are installing LEM Agents on the far end of a WAN link, copy the Remote Agent Installer executable to the end of the WAN link and run it there. This will avoid using your WAN bandwidth to copy LEM Agents multiple times.

Check the LEM release notes or readme file first to be sure that the LEM Agent version you are planning to install is compatible with your installed LEM Manager version.

Download the LEM Remote Agent Installer

The following LEM Agent installers are available from the SolarWinds customer portal:

- Windows Agent Installer
- Windows Remote Agent Installer
- Linux Agent Installer (32-bit)
- Linux Agent Installer (64-bit)
- AIX Agent Installer
- HPUX Itanium Agent Installer
- Solaris Intel Agent Installer
- Solaris Agent Installer
- Mac OS X Agent Installer

Run the LEM Remote Agent installer

1. Extract the contents of the installer zip file to a local or network location.
2. Run inremagent.exe.
3. To start the installation wizard, click Next.
4. Accept the End User License Agreement if you agree, and then click Next.
5. Specify a temporary folder on your computer to use for the installation process and click Next. The default is C:\SolarWindsLEMMultiInstall.
6. Enter the hostname of your LEM Manager in the Manager Name field and click Next. Do not change the default port values.

Use the fully qualified domain name for your LEM Manager when you deploy LEM Agents on a different domain. For example, enter LEMhostname.SolarWinds.com.
7. Select Get hosts automatically or Get hosts from file (One host per line) and click OK.
   - Get hosts automatically uses a NetBIOS broadcast to identify hosts on the same subnet and domain as the computer running the installer.
   - Get hosts from file (One host per line) prompts you to browse for a text file that includes the hosts on which you want to install LEM Agents. Use this option for any of the following reasons:
     - You are deploying LEM Agents to computers on a different subnet than that on which the computer running the installer resides. Your computer may be able to access these subnets, but their hosts will not be recognized by the NetBIOS broadcast used to get hosts automatically.
     - You are deploying LEM Agents to a small segment of a large network, which could make choosing them from a list time prohibitive.
     - You are deploying LEM Agents in a network with a complex naming scheme, which could make choosing hosts from a list time prohibitive.

```
Get hosts automatically uses a NetBIOS broadcast to identify hosts on the same subnet and domain as the computer running the installer.

Get hosts from file (One host per line) prompts you to browse for a text file that includes the hosts on which you want to install LEM Agents. Use this option for any of the following reasons:
- You are deploying LEM Agents to computers on a different subnet than that on which the computer running the installer resides. Your computer may be able to access these subnets, but their hosts will not be recognized by the NetBIOS broadcast used to get hosts automatically.
- You are deploying LEM Agents to a small segment of a large network, which could make choosing them from a list time prohibitive.
- You are deploying LEM Agents in a network with a complex naming scheme, which could make choosing hosts from a list time prohibitive.
```

8. Select the check boxes next to the computers on which you want to install a LEM Agent.
9. Click Next.
10. Confirm the list provided is correct, and then click Next again.
11. Specify the Windows destination for the remote installation.
    - The default paths are provided for all supported Windows systems. We strongly recommend using the default paths, as the LEM Agent may not recognized as a service by Windows if it is not installed in a system folder.
    - The installer is set to automatically detect host operating systems by default, but you can also specify an operating system if all the target hosts are running the same one.
12. Click Next.
13. Specify whether you want to install USB-Defender with the LEM Agent, and then click Next. The installer will include USB-Defender by default. To omit this from the installation, clear the Install USB-Defender checkbox.

```
Specify the Windows destination for the remote installation.
- The default paths are provided for all supported Windows systems. We strongly recommend using the default paths, as the LEM Agent may not recognized as a service by Windows if it is not installed in a system folder.
- The installer is set to automatically detect host operating systems by default, but you can also specify an operating system if all the target hosts are running the same one.
```

14. Confirm the settings on the Pre-Installation Summary, and then click Install.
15. After the installer extracts the installation files to the temporary directory, click Next.
    The installer copies the extracted files to the installation directory.

After installation, the Agent automatically starts on each host. The installer removes the temporary installation directory from your computer. Find troubleshooting information [here](#).
Set up a separate syslog server for use with LEM

This topic describes how to add a separate syslog server to LEM. The LEM VM includes a syslog server, but you can add a separate syslog server.

This procedure uses the Node Health widget in the Ops Center to set up your syslog server. You can also click Add Nodes to Monitor in the Getting Started widget to set up your syslog server.

You can monitor your switches, routers, and firewalls using a syslog server. This server collects and sends syslog messages from non-Agent devices to the LEM Manager over TCP or UDP. LEM uses this information to monitor syslog events and displays all events in the Monitor view.

Each device is paired with a connector, enabling LEM to parse messages from the syslog server and normalize the log message content to a LEM event.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, click Ops Center, and then locate the Node Health widget.

3. In the widget toolbar, click Add Node.

4. On the Specify Nodes to Add tab, select Syslog node.

5. Enter your syslog server IP address. This device will send syslog event logs to the LEM Manager.
6. From the drop-down list, select the node vendor.

7. Follow the instructions in the window to configure your node and send syslog messages to the LEM appliance.

8. After you configure the node, select the check box in the window, and then click Next.

The wizard locates the new node and recommends the appropriate connector.
Connectors enable Log & Event Manager to parse messages from syslog devices and normalize the original log message content to a LEM event.

If the LEM virtual appliance receives logs from the new device, it automatically detects and presents the device name or IP address.

9. To confirm the device is identified correctly, click Finish.

The syslog node displays in the Node Health widget.

10. (Optional) Based on your LEM deployment architecture, repeat this procedure to add a second syslog server in a multiple location deployment with two or more syslog servers.
LEM connectors: Normalize events sent from specific products on your network

Configure connectors to intercept events sent from a specific product on your network and convert those events into normalized messages that LEM can understand.

Configure LEM connectors for Agent and non-Agent devices

This section describes how to configure LEM connectors.

Configure connectors for the devices that you want to monitor with LEM

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. Choose from the following:
   - To configure Agent connectors, navigate to Manage > Nodes.
   - To configure non-Agent connectors, navigate to Manage > Appliances.

3. Next to the LEM Agent or LEM Manager instance that you want to configure, click , and then select Connectors.

4. Find the connector to configure:
   - Type part of the connector name in the search box, or use the filter menus in the Refine Results pane.
   - To restrict the list to only configured connectors, select Configured.

5. Next to the connector instance, click , and then select New.

6. Complete the connector configuration form. The following fields are common across most connectors:
   - Alias: Enter a user-friendly label for your connectors.
   - Log File: Enter the location of the log file that the connector will normalize. This is a location on either the local computer (Agents), or the LEM appliance (non-Agent devices).
   - Output, nDepth Host, and nDepth Port: You only need to configure these values if LEM is configured to save raw (unnormalized) log messages.

7. Click Save.

8. In the Tools list, click the gear icon next to the new connector (denoted by an icon in the Status column), and then select Start.
9. Verify that the connector is working:
   a. On the LEM toolbar, click Monitor.
   b. Check the SolarWinds Events filter to verify the connector started.
   c. Create a filter to test the new connector. For example, check the default Firewall filter after configuring your firewall connector.

Configure LEM Manager connectors

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. To open the Connector Configuration for [Manager] form, click 🔄, and then select connectors.
4. Add a connector instance for each product event log source.
5. When you are finished, start the connector instance.
6. Repeat Steps 6 and 7 for each product or device logging to the Manager computer.
7. Repeat Steps 4–8 for each Manager until you configured connectors for each point on your network.

Configure the sensor and actor connectors for each LEM Agent

Use the connector configuration form to connect the Agent connector to the target product that is either installed on, or remotely logging to the Agent computer. After configuring the Agent connectors, the Manager can monitor and interact with the products and devices on that computer.

Agent connectors run locally to monitor log files, as well as data logged to the Agent computer from remote devices that cannot run an Agent. The active response connectors (actors) allow the Agent to receive instructions from the Manager and perform active responses locally on the Agent computer, such as sending pop-up messages or detaching USB devices.

Connectors grid icons

The following table describes the icons used in the Connectors grid.

<table>
<thead>
<tr>
<th>ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>📄</td>
<td>A product sensor. The sensor displays the name of the product it is designed to monitor.</td>
</tr>
<tr>
<td>🎨</td>
<td>A product actor that performs an active response. The actor displays the name of the product it is designed to interact with.</td>
</tr>
<tr>
<td>🛠️</td>
<td>A configured instance of a sensor connector. The Status column displays Stopped 🛠️ or Running 🛠️ for each instance.</td>
</tr>
<tr>
<td>⚡️</td>
<td>A configured instance of an actor connector. The Status column displays Stopped 🛠️ or Running 🛠️ for each instance.</td>
</tr>
</tbody>
</table>
Configure Agent connectors

Follow this procedure to configure the connectors (sensors and actors) used by the Agent to monitor and interact with each network security product and device running on the Agent computer.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Search for the IP address or host in the Nodes grid.
4. Beside the hostname or IP address, click , and then select Connectors.
5. In the Refine Results pane, enter a search term that describe the connector you need.
6. Next to your targeted connector, click , and then select New.
7. Complete the connector information form, and then click Save.

Some connectors require the exact path of the Windows log and some just read the Windows Event Viewer logs.

8. When you are finished, start the connector instance.
9. Repeat steps 3 through 7 for each product or device that the Agent is monitoring on the Agent computer.

If you are not using connector profiles, repeat steps 2 through 7 for each Agent until you have configured the connectors for each point on your network. If you are using connector profiles, you can use a configured Agent as a template for a connector profile.

Use connector profiles to configure multiple Agents

Most Agents in a network include a few different connector configurations. You can streamline your connector configuration process by creating connector profiles. A connector profile groups Agents that share the same connector configuration.

For more information, see Create connector profiles to manage and monitor LEM Agents.

Manage LEM connectors

Use the Connector configuration form to:

- Configure and manage the LEM Manager sensor, actor, and notification connectors.
- Configure and manage the Agent sensor and actor connectors.
- Change the connectors configured in the Agent Connectors Profile.

To change a Connector Profile's membership and properties, edit the Connector Profile in the Build > Groups view.

You must be logged in to a Manager before you can configure its connectors or its Agents’ connectors.
Open a connector configuration form

Use this form to add connector instances for each network security product or device the Manager or Agent monitors or interacts with on the Manager computer.

Open a Manager connector configuration form

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. In the Appliances grid, locate your targeted Manager.
4. Click , and then log in to the Manager (if required).
5. Click , and then select Connectors.

Use this form to open an existing connector or add a new connector instance. See Find a connector or Add a new connector instance below for steps.

Open an Agent’s connector configuration form

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. In the Nodes grid, locate an Agent.
4. Click , and then select Connectors.

If the Agent is not in a connector profile, the Connector Configuration for [Agent] form appears.

If the Agent is in a connector profile, the Agent Connector Configuration prompt appears. A prompt warns you that the Agent belongs to a connector profile.

Find a connector

1. Open the connector configuration form. See [Open a connector configuration form](#) for help.
2. Search for a connector as follows:
   - To view all configured connectors: Leave the search box empty, choose All from the Category and Status menus, and select the Configured option.
   - To search for a connector by name: Enter part of the name in the search box on the Refine Results pane.
   - To view all connectors in a category: Leave the search box empty and choose from the Category menu.
   - To view all connectors that are either stopped or running: Leave the search box empty, choose All from the Category menu, and choose Running or Stopped from the Status menu.

The Connectors grid updates to show the matching connectors.
Add a new connector instance

Use the Connector Configuration form to configure the connection settings for:

- Each sensor that collects data from network security product event logs.
- Each actor that initiates an active response from a network security product or device.

Each sensor or actor connector configuration is a connector instance. Most products write to one log source and require a single connector instance. However, some products write to more than one log file. For these products, create separate connector instances for each log source. When a product requires more than one instance, you can differentiate between them by assigning each instance to a unique name called an alias.

1. Open the connector configuration form for a Manager or Agent. See Open a connector configuration form for help.
2. Use the Refine Results pane to select a connector Category.
3. In the Connectors grid, select a connector to configure.
   - The 🔄 icon indicates a sensor connector.
   - The 🔄 icon indicates an actor connector.
4. Click ⚒, and then select New.
   
   A form appears under the Connectors grid.
   
   The fields on the form vary for each connector. For new instances, the form displays the default connector settings required to configure the product or device. In most cases, you can save the connector with its default settings. However, you can change the settings as required.
5. Complete the Properties form as required.

   Hover over each selection to view the tooltip.

6. To save the connector configuration as a new connector instance, click Save.
   - If you configured a sensor, a sensor connector instance 🔄 icon appears below the connector.
   - If you configured an actor, an actor connector instance ✗ icon appears below the connector.
   - The 🔄 icon in the Status column indicates the connector instance is stopped. All new connector instances automatically have a Stopped status.
7. To start the connector instance, click ⚒, and then select Start.
   
   The system starts the connector instance, and the connector Status icon changes to a Started ✗ icon.
8. Repeat steps three through seven for each additional connector instance required to integrate this product or device with the LEM.
Start a connector instance

When you finish adding or reconfiguring a connector instance, start the connector instance to enable the connector configuration.

When you start a sensor connector instance, the sensor starts monitoring the product event log. When you start an actor connector instance, the actor starts initiating active responses on the product when requested by policy.

1. Open the connector configuration form for your targeted Manager or Agent.
2. In the Connectors grid, select the connector instance you want to start.
3. Click \( \textbullet \text{Start} \), and then select Start.

   The system starts the connector instance, and the Status icon changes to a Started \( \textbullet \text{Started} \) icon.

If the connector fails to start, the console displays a warning or failure event that describes the problem. Normally, connectors fail to start because:

- The network security device log file does not exist.
- The Agent does not have permission to access the file.

Stop a connector instance

Stop a connector instance before you edit or delete a connector instance. This process prevents the connector from gathering data for the console and initiating active responses on a network security product or notification system. After a connector instance is stopped, you can edit, delete, or restart the instance as required. The connector instance remains stopped until you restart the instance.

1. Open the Connector Configuration form for your targeted Manager or Agent.
2. In the Connectors grid, select the connector instance you want to stop.
3. Click \( \textbullet \text{Stop} \), and then select Stop.

   The system stops the connector instance, and the Status icon changes to a Stopped \( \textbullet \text{Stopped} \) icon.

Edit a connector instance

You can edit an existing connector instance configuration setting, but you cannot edit its name (alias). If you need to rename a connector instance alias, delete the current connector instance and create a new instance with the new name. You cannot edit the log file value for some Windows event log sensors.

1. Open the Connector Configuration form for the targeted Manager or Agent.
2. In the Connectors grid, select your targeted connector instance.
3. Click \( \textbullet \text{Stop} \), and then select Stop.

   She system stops the connector instance, and the status icon changed to a Stopped \( \textbullet \text{Stopped} \) icon.
4. Click \( \textbullet \text{Edit} \), and then select Edit.
5. Update the connector settings in the Properties form as required.
6. Click Save.
7. Click ☑️ and then select Start.

   The system starts the connector instance, and the Status icon changes to a Started 🟢 icon.

Delete a connector instance

You can delete an obsolete or incorrect connector instance when required.

1. Open the Connector Configuration form for the targeted Manager or Agent.
2. In the Connectors grid, select the connector instance you want to delete.
3. Click ☑️, and then select Stop.

   The system stops the connector instance, and the Status icon changes to a Stopped ⬅️ icon.
4. Click ☑️, and then select Delete.
5. When prompted, click Yes to confirm the delete.

   The connector instance disappears from the Connectors grid.

   ¡ Do not recreate the connector until it is completely removed. This process may require up to two minutes to complete.

Apply a LEM connector update package

This section describes different options for updating LEM connectors.

Enable global automatic connector updates

When enabled, this feature automatically updates Agents as they connect.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. In the Properties pane, click the Settings tab.

Update connectors on-demand

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. In the Appliances toolbar, click the Connector Updates drop-down list and select Update now.

![Connector Updates dropdown list](image)

### Update LEM connectors manually using the CMC interface

Customer Support occasionally provides stand-alone connector updates to address unmatched data alerts in your environment.

1. Go to the SolarWinds Customer Portal and download the Connector Update package from the Additional Components page.
2. Prepare the update package:
   a. Extract the update package from the .zip file, and then open the SolarWinds-LEM-Connectors folder.
   b. Copy the LEM folder to the root of a network share. For example: `C:\share\LEM`.
3. Open the CMC command line. See [Log in to the LEM CMC command line interface](#) for steps.
4. At the `cmc>` prompt, enter `manager`.
5. At the `cmc::manager>` prompt, enter `sensortoolupgrade`.
6. To start the upgrade process, press Enter.
7. To indicate that the update is located on the network, enter `n`.
8. To continue, press Enter.
9. Enter the path to the network share where the update package is located. Specify the path using the following UNC format: `\server\volume`
10. To confirm your entry, enter `y`.
11. Enter the domain and user name for a user that can access the share. Use the following format: `domain\user`.
12. To confirm your entry, enter `y`.
13. Enter the password for the user. Re-enter the password to confirm your entry.
14. To start the update, enter `1`.
   The update will take several minutes.
   Verify that the configured connectors restart after they are updated by watching for `InternalToolOnline` alerts in the default SolarWinds Alerts filter in the LEM console.
15. After the update is finished, type `exit` twice to exit the CMC interface.
Troubleshooting LEM connector upgrades

During the update process, the update script restarts all configured LEM connectors. In most cases, restarted connectors trigger one offline and one online alert in your LEM console.

An **InternalWarning** alert may appear, indicating that a connector started at the beginning of the corresponding log file. This alert may be caused by:

- An unnecessary connector. For example, you could have an NT DNS connector configured on a server that is not running the DNS service.
- A misconfigured connector. For example, you could have a connector pointing to the wrong location for the requisite log file.
- The device associated with the connector rotated its logs while the connector was offline.

Below is the event information for the **InternalWarning** alert.

```
EventInfo: -1:Start location was -1. Init set to 'newest' record, record info: 1 - 193 (101 - 293) @ -1. InsertionIP: lab-vm-exc10.lab.exc Manager: lem DetectionIP: 10.0.0.1 InsertionTime: 11:51:04 Thu Jun 16 2016
DetectionTime: 11:51:04 Thu Jun 16 2016 Severity: 2 ToolAlias: NT DNS InferenceRule: ProviderSID: FASTCenter normal error ExtraneousInfo: Component: FASTCenter:NT DNS Description: -1:Start location was -1. Init set to 'newest' record, record info: 1 - 193 (101 - 293) @ -1. Detail: StackTrace:
```

**LEM connector categories**

The table in this section describes the various categories of network security products that can be connected to LEM. The Description column describes how the connectors (sensors and actors) typically work with each type of product or device. The Use with columns indicate if each product type requires Manager connectors, Agent connectors, or both.
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Use with Managers</th>
<th>Use with Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Virus</td>
<td>This category lets you configure sensors for use with common anti-virus products. These products protect against, isolate, and remove viruses, worms, and Trojan programs from computer systems. To configure an anti-virus connector, the anti-virus software must be currently installed on the Agent computer. Some anti-virus connectors can also be run on the Manager by remotely logging from an Anti-Virus server. Due to software conflicts, SolarWinds recommends running only one brand of anti-virus software per computer.</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Application Switch</td>
<td>This category lets you configure sensors for use with application switches. Application-Layer switches transmit and monitor data at the application layer.</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>This category lets you configure sensors for use with database auditing products. These products monitor databases for potential database intrusions, changes, and database system events.</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>File Transfer and Sharing</td>
<td>This category lets you configure sensors for use with file transfer and file sharing products. These products are used to share files over the local network and the Internet. Monitoring these products provides information about what files are transferred, by whom, and system events.</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>CATEGORY</td>
<td>DESCRIPTION</td>
<td>USE WITH MANAGERS</td>
<td>AGENTS</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Firewalls</td>
<td>This category lets you configure sensors and actors for use with applications and devices used to protect and isolate networks from other networks and the Internet.</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Firewall sensors connect to, read, and retrieve firewall logs. Most firewalls also have an active response connector. These connectors configure actors that interface with routers and firewalls to perform block commands. Actors can perform active responses either via telnet or a serial or console cable. Normally, you will configure these connectors on the Manager.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To configure a firewall connector, the firewall product must already be installed on the Agent computer, or it must be remotely logging to an Agent or Manager. Normally, you will configure these connectors on the Manager.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You must also configure each firewall's data gathering and active response capabilities separately. For example, configuring a firewall's data gathering capabilities <em>does not</em> configure the firewall's active response settings.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>This category lets you configure sensors for use with identity access, identity management, and other single-sign on connectors. These products provide authentication and single-sign on capabilities, account management, and other user access features. Monitoring these products provides information about authentication and management of accounts.</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>CATEGORY</td>
<td>DESCRIPTION</td>
<td>USE WITH MANAGERS</td>
<td>USE WITH AGENTS</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>IDS and IPS</td>
<td>This category lets you configure sensors and actors for use with network-based and host-based intrusion detection systems. These products provide information about potential threats on the network or host, and can be used to raise alarms about possible intrusions, misconfigurations, or network issues. Generally, network-based IDS and IPS connectors are configured to log remotely, while host-based IDS and IPS systems log locally on an Agent system. Some network-based IPS systems provide the capability to perform an active response via their actor connector, allowing you to block an IP address at the IPS device.</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Manager</td>
<td>This category lets you configure sensors for use with the Manager and other Appliances. These connectors monitor for conditions on the Manager that may be informational or display potential problems with the appliances.</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Network Management</td>
<td>This category lets you configure sensors for use with network management connectors. These connectors monitor for different types of network activity from users on the network, such as workstation-level process and application monitoring. Generally, these systems are configured to log remotely from a central monitoring server.</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Network Services</td>
<td>This category lets you configure sensors for use with different network services. These connectors monitor service-level activity for different network services, including DNS and DHCP. Most network services are configured to log locally on an Agent's system. However, some are configured to log remotely.</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
<td>Use with Managers</td>
<td>Agents</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>This category lets you configure sensors for use with utilities in the Microsoft Windows operating system that monitor system events. This category includes a Windows Active Response connector. This connector configures an actor that enables Windows active response capabilities on Agents using Windows operating systems. This allows LEM to perform operating system-level responses, such as rebooting computers, shutting down computers, disabling networking, and disabling accounts. To configure an operating system connector, the operating system software must already be installed on the Agent computer. If you perform the remote Agent installation, the Windows NT/2000/XP Event Application Logs and System Logs connectors are configured by default.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy Servers and Content Filters</td>
<td>This category lets you configure sensors for use with different content monitoring connectors. These connectors monitor user network activity for such activities as web surfing, IM/chat, and file downloads, and events related to administering the monitoring systems themselves. Generally, these connectors are configured to log remotely from the monitoring system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routers/Swi</td>
<td>This category lets you configure sensors, and in some cases actors, for use with different routers and switches. These connectors monitor activity from routers and switches such as connected/disconnected devices, misconfigurations or system problems/events, detailed access-list information, and other related messages. Some routers/switches have the capability to configure an actor connector to block an IP address at the device. Generally, these connectors are configured to log remotely from the router/switch.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
<td>Use with Managers</td>
<td>Use with Agents</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>System Scan Reporters</td>
<td>This category lets you configure sensors for use with different asset scanning connectors, such as vulnerability scanners. These connectors provide information about potential vulnerabilities, exposures, and misconfigurations with different devices on the network. Generally, these connectors create events in the 'Asset' categories in the event tree.</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>System Connectors</td>
<td>This category lets you configure the Manager with an external notification system, so LEM can transmit event messages to LEM users via email or pager.</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>VPN and Remote Access</td>
<td>This category lets you configure sensors and actors for use with Virtual Private Network (VPN) server products that provide secure remote access to networks. Normally, you will configure these connectors on the Manager.</td>
<td></td>
<td>● ●</td>
</tr>
<tr>
<td>Web Server</td>
<td>This category lets you configure sensors for use with Web server products. To configure a web server connector, the web server software must already be installed on the Agent or Manager computer.</td>
<td></td>
<td>●</td>
</tr>
</tbody>
</table>
Configure LEM to monitor firewalls, proxy servers, domain controllers, and more

This section includes information to help you configure LEM components to monitor and protect specific systems and devices on your network.

Configure LEM to monitor firewalls for unauthorized access

Configure LEM Manager to monitor your firewalls and detect unauthorized access such as port scans, unusual data packets, network attacks, and unusual traffic patterns.

To set up a firewall monitor, configure your firewalls to log to LEM, and then configure a new connector in the LEM Manager. When an unauthorized user attempts to access your LEM VM or appliance, the event displays in the default Firewall filter running on the LEM console. You can also create custom filters that display network traffic to and from specific computers, as well as view web traffic and other traffic events across your network.

Click the video icon to view a tutorial about the threat intelligence feed available in LEM. For more information, see Using the Threat Intelligence Feed in LEM in the SolarWinds Success Center.

Configure a firewall to log to a LEM appliance

You can configure your LEM appliance to collect firewall information from firewalls manufactured by Cisco®, Check Point® Software Technologies, Juniper® Networks, and others. Set your firewall to log to your LEM appliance to centralize its log data with your LEM events. See the SolarWinds Success Center or contact Technical Support for more information.

Configure a firewall connector on a LEM Manager

After you configure your firewall to log to your LEM appliance, configure the corresponding connector on your SolarWinds LEM Manager. Many of the firewall connectors are similar, and some will include unique settings.

This example describes how to configure a Cisco ASA firewall and IOS connector on your LEM Manager.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

   Log in as an administrator.

2. On the LEM toolbar, navigate to Manage > Appliances.
3. Next to the SolarWinds LEM Manager, click 🔗, and then select Connectors.

4. In the Connector Configuration window search box, enter Cisco ASA.

5. Next to the Cisco ASA and IOS connector, click 🔗, and then click New.

6. Replace the Alias value with a descriptive connector alias.
   
   For example:
   
   ASA Firewall
   
   Include firewall in the Alias field to ensure the default Firewall filter captures your firewall data.

7. Verify the Log File value matches the local facility defined in your firewall settings.

8. Click Save.

9. Next to the new connector instance (indicated by an icon in the Status column), click 🔗, and then select Start.

10. To close the Connector Configuration window, click Close.

The firewall connector is configured in the LEM console.

View network traffic from specific computers

You can create custom filters that highlight specific firewall events. For example, to monitor traffic from a specific computer, create a filter for all network traffic coming from the targeted computer. Use connector profiles and other groups to broaden or refine the scope of custom filters.

The following procedure provides an example of creating a filter to monitor all traffic from a targeted computer.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   
   Log in as an administrator.

2. On the LEM toolbar, click Monitor.

3. In the Filters pane, click 🔗, and then select New Filter.

4. Enter a Name and Description for the filter.

5. In the Filter Creation pane, click Event Groups, and then select Network Audit Alerts.


7. In the Constant field (highlighted with a pencil icon), enter a wild card character (*) to avoid entering the fully qualified domain name of the computer.
   
   Use a Connector instead of a Text Constant to filter for all network traffic coming from a group of similar computers.

8. Click Save.
Clone and enable a LEM rule to identify port scanning traffic

To identify suspicious firewall traffic indicative of port scanning, clone and enable the PortScans rule. This rule generates a default TCPPortScan event, which the SolarWinds LEM console displays in the default Security Events filter. Use this event to monitor suspicious network traffic and prevent unauthorized access to your firewall.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Refine Rules pane, enter PortScans.
4. Next to the rule, click , and then select Clone.
5. Select the folder to store the cloned rule, and then click OK.
6. In the Rule Creation window, select Enable.
7. (Optional) Tune the rule to match your environment.
   For example, you can:
   - Subscribe to the rule to track activity in the Subscriptions report.
   - Increase the number of events in the Correlation Time box to modify how frequently the rule fires.
   - Omit vulnerability scanners from the Correlations by changing the TCPTrafficAudit exists condition to `TCPTrafficAudit .SourceMachine = Your Scanners` where `Your Scanners` is a user-defined group, connector profile, or directory service group that represents the targeted group of computers.
   - Modify the default action or add additional actions to perform tasks such as send an email message or block an IP address.
8. When completed, click Save.
9. In the main Rules screen, click Activate Rules.

Configure LEM to monitor proxy servers for suspicious URL access in LEM

Monitor proxy servers to track network users who attempt to access suspicious websites using partial or complete URL addresses. Configure your proxy server to log to LEM and set up the appropriate connector on your SolarWinds LEM Manager.

Set your proxy server to log to a virtual appliance

Set your proxy server to log to LEM to centralize its log data with your LEM events. You can integrate proxy servers from popular vendors such as Websense and Barracuda.
Because the integration process is different for each vendor, each proxy server is documented separately in the SolarWinds Success Center. If a knowledge base article is not available, contact Customer Support.

Configure a proxy server connector on a LEM Manager

After you configure your proxy server to log to your LEM appliance, configure the corresponding connector on your LEM Manager. Many of the proxy server connectors are similar with some unique settings.

The following procedure describes how to set up a connector for a Websense proxy server. You can find instructions for additional firewall connectors in the SolarWinds knowledge base.

1. Open the console and log in to the LEM Manager as an administrator.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. Locate your LEM Manager in the grid.
4. Click , and then select Connectors.
5. In the Connector Configuration window search box, enter Websense Web Filter.
6. Next to the Websense Web Filter and Websense Web Security connector, click , and then click New.
7. Replace the Alias value with a custom alias or accept the default.
8. Click Save.
9. Next to the new connector instance, click , and then select Start.
10. To close the Connector Configuration window, click Close.

Clone and enable the Known Spyware Site traffic rule

You can track when users attempt to access suspicious websites by partial or complete URL addresses by enabling the Known Spyware Site Traffic rule. This rule generates a HostIncident event by default you can use in conjunction with the Incidents report to notify auditors that you are auditing critical events on your network.

Before you enable this rule, ensure your proxy server transmits complete URL addresses to your LEM Manager by checking the URL field of any WebTrafficAudit event generated by your proxy server. If your proxy server does not log web traffic events with this level of detail, check the events coming from your firewalls, as they can sometimes be used for this rule as well.

1. Open the console and log into the LEM Manager as an administrator.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Refine Results pane, click Default Rules.
4. In the Refine Results search box, enter Known Spyware Site Traffic.
5. Click , and then select Clone.
6. Select the folder where you want to save the cloned rule, and then click OK.
7. In the Rule Creation window, select Enable, and then click Save.
Configure LEM to monitor anti-virus software for viruses that are not cleaned

You can monitor your antivirus software performance by configuring the software to log to LEM. When completed, set up the appropriate connector on the LEM Manager, and then use the LEM console to view events in the default Virus Attack filter.

Configure antivirus software to Log to a LEM appliance

Set your antivirus software to log to LEM. This process centralizes the antivirus log data with your existing LEM events.

You can integrate LEM with antivirus software from manufacturers such as Symantec and McAfee. See the SolarWinds Knowledge Base or contact SolarWinds Support for more information.

Configure the antivirus connector on the LEM Manager

The following procedure describes how to configure the Symantec Endpoint Protection 11 connector on the LEM Manager.

1. Replace the Alias value with a custom alias or accept the default.
2. Ensure that the Log File value matches the Log Facility defined in your antivirus settings.
3. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
4. Log in as an administrator.
5. On the LEM toolbar, navigate to Manage > Appliances.
6. In the Connector Configuration window search box, enter Symantec Endpoint Protection.
7. Next to the Symantec Endpoint Protection 11 connector, click , and then select New.
   For Symantec Endpoint Protection (SEP), the Log Facility is equal to the local facility on LEM, plus 16. For example, the default Log File for /var/log/local6.log on SolarWinds LEM corresponds to Log Facility 22 in your Symantec Endpoint Protection 11 settings.
8. Click Save.
9. Next to the new connector instance, click , and then select Start.
10. To close the Connector Configuration window, click Close.

Create a LEM rule to track when viruses are not cleaned

Clone and enable the Virus Attack – Bad State rule to track virus attacks reported by your anti-virus software. The Bad Virus State User-Defined Group defines a bad state as any virus that is not fully cleaned by your anti-virus software. This includes any virus that is not addressed, quarantined, or renamed.
The default action for this rule is to generate a HostIncident event, which you can use in conjunction with the Incidents report to notify auditors you are auditing the critical events on your network.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the search box, enter Virus Attack - Bad State.
4. Next to the rule, click , and then select Clone.
5. Select the folder to store cloned rule, and then click OK.
6. Select the Enable check box, and then click Save.
7. In the main Rules screen, click Activate Rules.

Configure LEM File Integrity Monitoring (FIM) to monitor Windows files, folders, and registry keys

File Integrity Monitoring (FIM) monitors all file types for unauthorized changes. Using FIM, you can detect changes to critical files to ensure systems have not been compromised.

Please note that FIM does not support the monitoring of network shares. Only local drives are supported.

FIM can detect unauthorized modifications to configuration files, executables, log and audit files, content files, database files, web files, and so on. When FIM detects that a monitored file has changed, it logs an event. The event then prompts LEM to execute the configured action. You can build correlation rules to act as a second-level filter to send an alert if certain patterns of activity occur (not just single instances). When an alert is triggered, the data is in context with your network and other system log data.

Features of FIM

- Monitor real-time access and identify users who change file and registry keys.
- Configure file and directory logic and registry keys and values to monitor different types of access (create, write, delete, change permissions/metadata).
- Standardize configurations across many systems.
- Configure monitoring templates to monitor the basics and create and customize your own monitors.
- Configure templates for rules, filters, and reports to assist in including FIM events.

Add a FIM connector to an Agent to monitor a node

First add the FIM connector to an Agent, and then customize it. You can assign one instance of a FIM File and Directory connector, and one instance of a FIM Registry connector to an Agent.
Task 1: Add a FIM connector to a node

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Select a node to monitor.
4. Click  and then select Connectors.
5. In the Refine Results pane, type FIM.
   FIM Registry and FIM File and Directory connectors display in the search results.
6. Select either the FIM File and Directory connector, or the FIM Registry connector.
7. Click  and then select New.
   The FIM Connector configuration screen opens.
8. Do one of the following:
   - Select a template from the Monitor Templates section. Several monitoring templates are available to assist you in creating custom templates and configurations.
     Click  and then select Add to selected monitors.
     The monitor template moves to the Selected Monitor section.
   - Click Add Custom Monitor in the Selected Monitors section.

Task 2: Configure rules and specific actions for your monitored files

1. In the Selected Monitors section, click  next to the monitor you added in task 1, and then choose Edit Monitor.
2. Enter a monitor name and description.
3. To add conditions to the monitor, click Add New.
4. Complete the Add Condition form, and then click Save. See Add conditions to a directory that FIM is watching for help completing the form.
5. To save the monitor configuration for this FIM connector, click Save Changes.
6. To save the FIM connector configuration for this Agent, click Save.

Edit a Monitor

1. Select a Monitor from the Selected Monitors pane.
2. Click  and then select Edit monitor.

Promote a Monitor to a Template

1. Select the Monitor to be promoted.
2. Click  and then select Promote monitor to template.
3. To promote this monitor to a template, click Yes. The monitor is now available in the Monitor Templates pane.

Delete a Monitor
1. Select a monitor to delete.
2. Click 📐, and then select Delete.
3. Click Remove. The monitor is removed from the Selected Monitors pane.

Add conditions to a directory that FIM is watching
1. In the Conditions window, click Add New.
2. To select a File and Directory or a Registry key to watch, click Browse, and then click OK.
3. Select whether the files are recursive or non-recursive. Refer to the table below for more information.

<table>
<thead>
<tr>
<th>Recursive</th>
<th>The folder selected and all its sub-folders which match the given mask will be monitored for corresponding selected operations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-recursive</td>
<td>Only the files in the selected folders will be monitored.</td>
</tr>
</tbody>
</table>

4. Enter a Mask using the asterisk (*) as a wildcard. For example, *exe or directory*.
5. For a FIM File and Directory, select Create, Read, Write, and Delete for Directory, File, Permissions, and Other operations. For a FIM Registry, select Create, Read, Write, and Delete for Key and Value operations.

   i For information about the "Other" option, refer to the Microsoft MSDN information.

6. Click Save.

Edit Conditions
1. In the Conditions window, select a condition to edit.
2. Click Edit.
3. To select a File and Directory or a Registry key to watch, click Browse, and then click OK.
4. Select whether the files are recursive or non-recursive. Refer to the table below for more information.

<table>
<thead>
<tr>
<th>Recursive</th>
<th>The folder selected and all its sub-folders which match the given mask will be monitored for corresponding selected operations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-recursive</td>
<td>Only the files in the selected folders will be monitored.</td>
</tr>
</tbody>
</table>

5. Enter a mask. For example, *exe or directory*.
6. For a FIM File/Directory, select Create, Read, Write, and Delete for Directory, File, Permissions, and Other operations. For a FIM Registry, select Create, Read, Write, and Delete for Key and Value
operations. For more information on Other, refer to the Microsoft MSDN information.

7. Click Save.

Delete Conditions

1. In the Conditions window, select a condition to delete.
2. Click Delete, and then click Remove.

FIM connector advanced settings

1. Complete the Advanced Connector Settings form according to the device you’re configuring. The following fields/descriptions are common for most connectors:

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Log Directory          | When you create a new alias for a connector, LEM automatically places a default log file path in the Log Directory field. This path tells the connector where the operating system stores the product’s event log file. In most cases, you should be able to use the default log file path that is shown for the connector. These paths are based on the default vendor settings and the product documentation for each product. If a different log path is needed, To manually change the log file location:  
  1. Enter or paste the correct path in the Log Directory field.  
  2. Stop the Agent.  
  3. Manually update the Agent’s spop.conf property  
     - com.solarwinds.lem.fim.minifilter.fs LogLocation for a file and directory connector. This appears as %SystemDrive%\Mylocation\FileSystem in the config file.  
     - com.solarwinds.lem.fim.minifilter.registry LogLocation for a registry connector. This appears as C:\My other log location\Registry in the config file.  
  4. Restart the Agent. |
| Log Data Type to Save  | Select either nDepth, Alert, or Alert, nDepth. To store a copy of the original log data in addition to normalized data, change the Log Data Type to Save to Alert, nDepth. Storage for original log data must also be enabled on the appliance. |
| nDepth Host            | If you are using a separate nDepth appliance (other than LEM), type the IP address or host name for the nDepth appliance. Generally, the default setting is correct. Only change it if you are advised to do so. |
| nDepth Port            | If you are using a separate nDepth appliance (other than the SolarWinds LEM), type the port number to which the connector is to send nDepth data. Generally, the default setting is correct. Only change it if you are advised to do so. |
Enable Windows file auditing for use with LEM

Enable file auditing in Windows to monitor events related to users accessing, modifying, and deleting sensitive files and folders on your network. To maximize the value of this type of auditing, enable auditing on a file server on which you have installed a LEM Agent, and only for the specific files and folders you want to monitor. If you enable auditing on all files or folders, or even a many of them, you will create an unnecessary burden on LEM.

Complete the two-part process below to first enable object auditing on your server, and then enable file auditing on the files and folders that you want to audit. Provided Windows is logging the events and your server has a LEM Agent installed on it, the LEM console will begin displaying the new file auditing alerts immediately.

Enable object auditing in Windows

1. In Windows Control Panel, navigate to Administrative Tools > Local Security Policy.
2. Expand Local Policies and click Audit Policy in the left pane.
3. Select Audit object access in the right pane, and then click Action > Properties.
4. Select Success and Failure, and then click OK.
5. Close the Local Security Policy window.

Enable file auditing on a file or folder in Windows

1. Locate the file or folder you want to audit in Windows Explorer.
2. Right-click the file or folder, and then select Properties.
3. Click the Security tab.
4. Click Advanced.
5. Click the Auditing tab.
6. If you are using Windows Server 2008, click Edit.
7. Click Add.
8. Enter the name of a user or group you want to audit for the selected file or folder, and then click Check Names to validate your entry. For example, enter Everyone.
9. Click OK.
10. Select Success and Failure next to full control to audit everything for the selected file or folder.
11. Optionally, clear Success and Failure for unwanted events such as:
   - Read attributes
   - Read extended attributes
   - Write extended attributes
   - Read permissions
12. Click OK in each window until you are back at the Windows Explorer window.
13. Repeat these steps for all files or folders you want to audit.

Configure Windows audit policy for use with LEM

The Windows audit policy determines the amount of data that Windows Security logs on domain controllers and other computers in the domain.

Verbosity is the amount of known data.

See Microsoft's TechNet knowledge base for details on Windows Audit Policy Definitions. These definitions are effective from both a best-practice and compliance standpoint, and are based on customer experience and recommendations from Microsoft.

See also:
Requirements

Using the Windows Audit Policy with LEM requires:

- Windows Server 2003 or higher
- Permissions to change the Windows Audit Policy at the domain controller and domain level
- SolarWinds LEM installation

Windows Audit Policy

The following events and descriptions are adapted from information available on the Microsoft TechNet knowledge base. You can query relevant articles on TechNet by searching for audit policy best practice.

<table>
<thead>
<tr>
<th>EVENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logon events</td>
<td>Represents user log on or log off instances on a computer logging those events. These events are specifically related to domain logon events and logged in the security log for the related domain controller.</td>
</tr>
<tr>
<td>Audit account management</td>
<td>The change management events on a computer. These events include all changes made to users, groups and machines.</td>
</tr>
<tr>
<td>Audit logon events</td>
<td>Represents user log on or log off instances from a computer logging those events. These events are logged in the security log of the local computer onto which the user is logging, even when the user is logging onto the domain using their local computer.</td>
</tr>
<tr>
<td>Audit object access</td>
<td>Track users accessing objects with their own system access control lists. These objects include files, folders and printers.</td>
</tr>
<tr>
<td>Audit policy change</td>
<td>Represents instances where local or group policy changed. These changes include user rights assignments, audit policies and trust policies.</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>Track users accessing objects based on their privilege level. These objects include files, folders and printers, or any object with its own system access control list defined.</td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>Logs all instances of process, service, and program starts and stops. This can be useful to track both wanted and unwanted processes, such as AV services and malicious programs.</td>
</tr>
<tr>
<td>Audit system events</td>
<td>Includes start up and shut down events on the computer logging them, along with events that affect the system's security. These are operating system events and are only logged locally.</td>
</tr>
</tbody>
</table>
Best practice

Windows audit policy is defined locally for each computer. SolarWinds recommends using group policy to manage the audit policy at both the domain controller and domain levels.

Set the Windows audit policy

Use the Group Policy Object Editor to set your Windows audit policy settings on desktop systems running at least Windows 7, and servers running Windows Server 2008 and 2012. The following procedure applies to setting up sub-category-level auditing.


When enabling the Force Audit Policy Subcategory option, set the subcategory auditing to enabled and the category-level auditing will be disabled.

Default Domain Controllers Policy

Select Success and Failure for all policies except:

- Audit object access
- Audit privilege use

Default Domain Policy

The Default Domain Policy applies to all computers on your domain except your domain controllers. For this policy, select Success and Failure for:

- Audit account logon events
- Audit account management
- Audit logon events
- Audit policy change
- Audit system events

You can also select Success and Failure for audit process tracking critical processes (such as the AV service) or unauthorized programs (such as games or malicious executable files).

Enabling auditing at the audit level will increase the number of events in the system logs. As a result, your LEM database will quickly expand as it collects these logs.

Similarly, there could be bandwidth implications as well. This is dependent upon your network traffic volume and bandwidth capacity. Since Agent traffic is transmitted to the Manager as a real-time trickle of data, bandwidth impact is minimal.

SolarWinds recommends meeting PCI Auditing. However, this may be applicable to other auditing as well. For more information, see PCI Compliance and Log and Event Manager.
<table>
<thead>
<tr>
<th>Category or Subcategory</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Security System Extension</td>
<td>No Auditing</td>
</tr>
<tr>
<td>System Integrity</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>IPsec Driver</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Other System Events</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Security State Change</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Logon/Logoff</td>
<td></td>
</tr>
<tr>
<td>Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Logoff</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Account Lockout</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>IPsec Main Mode</td>
<td>No Auditing</td>
</tr>
<tr>
<td>IPsec Quick Mode</td>
<td>No Auditing</td>
</tr>
<tr>
<td>IPsec Extended Mode</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Special Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Other Logon/Logoff Events</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Network Policy Server</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Object access</td>
<td></td>
</tr>
<tr>
<td>File System</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Registry</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Kernel Object</td>
<td>No Auditing</td>
</tr>
<tr>
<td>SAM</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Certification Services</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Application Generated</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Handle Manipulation</td>
<td>No Auditing</td>
</tr>
<tr>
<td>File Share</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Filtering Platform Packet Drop</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Category or Subcategory</td>
<td>Setting</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Filtering Platform Connection</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Other Object Access Events</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Detailed File Share</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Privilege Use</td>
<td></td>
</tr>
<tr>
<td>Sensitive Privilege Use</td>
<td>Failure</td>
</tr>
<tr>
<td>Non-Sensitive Privilege Use</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Other Privilege Use Events</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Detailed Tracking</td>
<td></td>
</tr>
<tr>
<td>Process Termination</td>
<td>No Auditing</td>
</tr>
<tr>
<td>DPAPI Activity</td>
<td>No Auditing</td>
</tr>
<tr>
<td>RPC Events</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Process Creation</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Policy Change</td>
<td></td>
</tr>
<tr>
<td>Audit Policy Change</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Authentication Policy Change</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Authorization Policy Change</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>MPSSVC Rule-Level Policy Change</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Filtering Platform Policy Change</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Other Policy Change Events</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Account Management</td>
<td></td>
</tr>
<tr>
<td>User Account Management</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Computer Account Management</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Security Group Management</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Distribution Group Management</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>CATEGORY OR SUBCATEGORY</td>
<td>SETTING</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Application Group Management</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Other Account Management Events</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>DS Access</td>
<td></td>
</tr>
<tr>
<td>Directory Service Changes</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Directory Service Replication</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Detailed Directory Service Replication</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Directory Service Access</td>
<td>Failure</td>
</tr>
<tr>
<td>Account Logon</td>
<td></td>
</tr>
<tr>
<td>Kerberos Service Ticket Operations</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Other Account Logon Events</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Kerberos Authentication Service</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Credential Validation</td>
<td>Success and Failure</td>
</tr>
</tbody>
</table>

### Configure the USB Defender local policy connector in LEM

The USB Defender Local Policy connector enables a LEM Agent to enforce restrictions on USB devices, even when the Agent is not connected to the LEM Manager. Instead of using rules when disconnected, the connector uses a list of permitted users or devices. The Agent compares the fields in all USB device-attached events to a locally stored white list of users or devices. If none of the fields match an entry on the list, the Agent detaches the device.

**:i: See also:**

- [Configure the Detach USB Device active response in LEM](#)

When the Agent is connected to the Manager through the network, the Manager rule also applies. Any devices listed in the local white list must be in the User Defined Group for authorized devices. Otherwise, the rule takes effect and the device detaches even though it was allowed by the white list in the USB Defender local policy. When the Agent is connected, the USB Defender Local Policy and the LEM rule are active.
1. Create a text file with one entry per line.
   This file serves as the local policy. Each entry can be a user name or a USB device ID, from the Extraneous Info field of an attached alert.

2. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

3. On the LEM toolbar, navigate to Manage > Nodes.

4. Next to the target node, click <i>», and then select Connectors.

5. In the Refine Results pane, enter <i>USB defender.</i>

6. In the Connectors grid, locate the USB Defender Local Policy connector.

7. Next to the connector, click <i>», and then select New.

8. In the UDLP pane, click the ellipsis (...) button, and then locate the text file you created above.

9. Upload your list to the connector, and then click Save.

10. When the new connector appears in the Connectors list, click <i>», and then select Start.

The authorized devices in the local white list must also be in the UDG for Manager Detach Unauthorized USB rule or the rule on the Manager enforces detachment when the laptop is connected to the network. In reverse, if you are using a blacklist and the device is in the USB Local Policy and not in the User Defined Group of the rule, the device still detaches.

Having a device or user in one white list or black list and not in the other is not recommended and yields inconsistent results.

Configure LEM to monitor Microsoft SQL databases for changes to tables and schemas

You can track successful or failed attempts to access your database tables and schemas by installing MSSQL Auditor for Windows on a LEM Agent running SQL Server 2008 or later with Profiler. This configuration allows you to monitor your local or remote SQL Server databases.

MSSQL Auditor runs as a service in conjunction with the LEM Agent service.

Configure your database servers

Download MSSQL Auditor for Windows from the Customer Portal and install the software on your server. When configured and enabled, the software provides your SolarWinds LEM Agent access to details about any database configuration changes to your database server.

To enable the SolarWinds LEM Agent access to details about your database configuration changes, install the following software on your database server:

- Microsoft SQL Server 2008 or later
- Microsoft .NET 3.5 and 4.0 Framework
SolarWinds LEM Agent for Windows

When completed, install the MSSQL Auditor for Windows on your server.

Install MSSQL Auditor on a LEM Agent

2. To begin the installation, double-click the EXE file.
3. To start the wizard, click Next.
4. Accept the End User License Agreement if you agree, and then click Next.
5. Click Change to specify an installation folder, or accept the default, and then click Next.
6. Click Install.
7. When the installation is finished, select Launch SolarWinds MSSQL Auditor, and then click Finish.

Configure MSSQL Auditor on your servers

If you did not select Launch SolarWinds MSSQL Auditor after installing the application, you can launch the application from the SolarWinds Log and Event Manager program group in your Start menu.

1. Enter the name of the SQL server to monitor in the SQL Server\Instance field, and click Add Server.
   To specify an instance other than the default, enter your server name in the following format: Server\Instance
2. Repeat step 1 for any additional servers you need to monitor.
3. To use an account other than the Local System Account to run MSSQL Auditor on your database server, select This Account in the Run Service As and provide the appropriate credentials.
   SolarWinds recommends using an account in the sysadmin role on your database. The account only requires Execute permissions for any stored procedures with the xp_trace prefix.
4. In the Manage Auditor Service section, click Start Auditor Service, and then click OK.

Configure the MSSQL Auditor Connector on a LEM Agent

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Locate the LEM Agent for your database server and verify it is connected to your LEM Manager.
4. Next to the SolarWinds LEM Agent, click , and then select Connectors.
5. In the Refine Results search box, enter MSSQL.
6. Next to the SolarWinds Log and Event Manager MSSQL Auditor connector, click , and then select
New.

7. Create a new alias name for the connector, or accept the default.
8. Verify that the Log File field value matches the folder name that stores the logs on your database server, and then click Save.
9. Next to the new connector instance, click , and then click Start.
10. Repeat step 1 through step 9 for the MSSQL 2000 Application Log connector.
11. To close the Connector Configuration window, click Close.

Send notifications of Microsoft SQL database change attempts

Clone and enable the MSSQL Database Change Attempt rule to track user attempts to change properties on a monitored Microsoft SQL Server database. The default rule action generates a HostIncident event you can use in conjunction with the Incidents report to notify auditors that you are auditing the critical events in your network.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Refine Results search box, enter MSSQL Database Change Attempt.
4. Next to the rule, click , and then select Clone.
5. Select the folder where the cloned rule will be stored, and then click OK.
6. Select the Enable check box, and then click Save.
7. In the main Rules screen, click Activate Rules.

Configure LEM to monitor Windows domain controllers for brute force hacking attempts

Monitor your Windows domain controllers using the SolarWinds LEM Agent. After you install and configure the Agent, the software tracks brute force and other types of hacking attempts to your domain controllers and reports all events to the LEM Manager.

These events include:

- Unauthorized access to your administrative accounts
- Failed logon attempts
- Account lockouts
- User and group modification
- Change management events

Install the SolarWinds LEM Agent on all domain controllers to ensure the LEM Manager captures all your domain events (even if they are not replicated across all domain controllers).
You can view the events in the LEM console using the change management filter and create custom filters to report all activity on your domain controllers.

Install and configure the LEM Agent

When you install the LEM Agent, you have the option to install USB Defender. This application works together with the LEM Agent to provide real-time notification when a USB drive is installed in your domain controller server. By default, USB Defender generates events related to USB mass storage devices attached to your LEM Agents.

For additional security, Microsoft implemented a method in their operating system to log security events. As a result, SolarWinds LEM Agents on systems running Windows Server 2008, Windows Vista, or Windows 7 require different connectors than the Agents running on systems with the legacy Windows operating systems.

If you are running both old and legacy Windows operating systems in your environment, create a connector profile for each operating system.

For LEM Agent software and hardware requirements, see the "LEM 6.6 system requirements" in the LEM Installation Guide.

Install a LEM Agent on a single Windows domain controller

2. Extract the ZIP file contents to a local or network directory.
3. Run Setup.exe.
4. To start the installation wizard, click Next.
5. Accept the End User License Agreement if you agree, and then click Next.
6. In the Manager Name field, enter the host name of your LEM Manager, and then click Next.
   
   "Do not change the default port values."

7. Confirm the Manager Communication settings, and then click Next.
8. (Optional) To install USB Defender with the LEM Agent, select the check box.
9. Confirm the settings on the pre-Installation summary, and then click Install.
10. When the installation is complete, click Next to start the LEM Agent service.
11. Inspect the Agent log for any errors, and then click Next.
12. To exit the installer, click Done.

The LEM Agent is installed on your system and begins sending events to your LEM Manager and LEM console.

The LEM Agent continues running on your system until you uninstall the software or manually stop the LEM Agent service.
Configure additional connectors on your LEM Agent

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Manage > Nodes.

3. In the list, locate the LEM Agent.

   - Use the Refine Results pane, if needed.

4. Next to the LEM Agent, click , and then select connectors.

5. Locate and select the connector you want to configure.

   - Use the Refine Results pane if needed.

6. Next to the connector, click , and then select New.

7. Modify the connector (if required), and then click Save.

8. Next to the new connector instance, click (indicated by an icon in the Status column), and then select Start.

9. To close the Connector Configuration window, click Close.

10. Configure the following connectors that apply to your installation on your Windows domain controllers:

    - Windows Directory Service Log
    - Windows DNS Server Log
    - Windows DHCP Server version

Maintain and monitor multiple domain controller Agents

Connector Profiles help you maintain and monitor multiple domain controllers in your LEM console. You can use these profiles to configure and modify connector settings at the profile level, as well as provide a group you can use to filter incoming event traffic from your LEM Agents to your LEM console.

Create a connector profile based on a single SolarWinds LEM Agent

Follow this procedure to create a connector profile based on a single LEM Agent and a corresponding filter to monitor activity on all systems in the profile.

1. Install the LEM Agent software on all systems you want to include in your new connector profile.

2. Configure a single LEM Agent to serve as the template for your connector profile.

3. On the LEM toolbar, navigate to Build > Groups.

4. Click , and then select Connector Profile.

5. Enter a profile name and description.

6. From the Template list, select the new LEM Agent, and then click Save.

7. In the Groups list, locate your new connector profile.
8. Next to your connector profile, click and then select Edit.
9. In the Available Agents pane, locate the SolarWinds LEM Agents you want to add to your connector profile.
10. Click the arrow next to each LEM Agent you want to add to the Contained Agents pane.
11. When complete, click Save.

Create a filter for all activity in a Connector Profile

1. Open the LEM console and log on to the LEM Manager as an administrator or auditor.
2. On the LEM toolbar, click Monitor.
3. In the filters pane, click and then select New Filter.
4. Enter a Name and Description for the filter.
5. In the Filter Creation list, click Event Groups.
6. Click Any Alert.
7. In the Fields: Any Alert list, drag DetectionIP into the Conditions box.
8. In the Filter Creation list, click Connector Profiles.
9. Drag your connector profile into the Conditions box, replacing the Text Constant field denoted by a pencil icon.
10. Click Save.

Clone and enable the Critical Logon Failures rule

Clone and enable the Critical Account Logon Failures rule to track failed logon attempts to the default Windows Administrator account. The default action for this rule is to generate a HostIncident event, which you can use in conjunction with the Incidents report to notify auditors you are auditing the critical events on your network.

1. Open the LEM console and log on to the LEM Manager as an administrator.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Refine Results pane search box, enter Critical Account Logon Failures.
4. Next to the rule, click , and then select Clone.
5. Select the folder where you want to save the cloned rule, and then click OK.
6. In the Rule Creation window, select Enable, and then click Save.
7. On the main Rules screen, click Activate Rules.

The rule is enabled.
Tune Windows Logging for LEM implementation

After you install and configure your LEM Agents, optimize your LEM deployment by tuning your Windows operating system to log the specific events you want to see in your LEM console and store in your LEM database. Set your group and local policies according to your environment requirements. See Configure Windows audit policy for use with LEM for more information.

Configure LEM to track Cisco buildup and teardown events

You can enable LEM to track buildup and tear-down events that occur on your network.

To monitor accepted traffic, use the log target in your accepted ACLs instead of the buildup logging. This lets you control the accepted traffic that will generate an alert. To monitor the information about the actual NAT, consider the event load this will create. Plan a test phase where you turn it on and determine if it is valuable to you for further investigation.

If you need to monitor unmodified log data (versus the normalized data), consider the nDepth original log message store. Remember that this process requires additional disk space.

Also, consider whether you need both builds and tears, or just build messages. The tear-down NAT messages include the same information as the built messages, along with some duration and size information that may or may not be useful. Colleges and universities that use the built messages do not rely on the tear-down messages. They only need to know a connection was established for verification, analysis, and correlation.

Be sure to check your syslog data to determine and enable only those buildup or teardown events are of use.

Tracking Buildup Events

LEM is preconfigured to capture Cisco events 302003, 302009, and 603108.

You can configure LEM to capture Cisco firewall buildup events as well. The primary buildup event to use for TCP tracking is 302013. Other buildup events include 302015, 302017, 302020, 302303, 305009, 305011, and 609011. Check the description of these events in the Cisco System Log Messages Guide located on the Cisco website to ensure you need to capture these events.

Tracking teardown Events

Out of the box, LEM captures Cisco event 603019.

You can also enable LEM to capture Cisco firewall teardown NAT events. The teardown sibling to buildup even 302013 is 302014. Other events include 302016, 302018, 302021, 302304, 305010, 305012, 617100, and 609002. You can see description of these events in the Cisco System Log Messages Guide to make sure they are ones you want to capture.
Enabling LEM to track buildup and teardown events

1. Ensure that your firewalls are sending log events to LEM, and that the appropriate LEM connector is monitoring your firewall data.

2. Access the firewalls that contain the buildup and tear-down messages you need to monitor and adjust the severity level of those events from 6 (the default) to 0.

   For more information, see the Changing the Severity Level of a Syslog Message section in the Monitoring the Security Appliance page on the Cisco site.
LEM groups: Organize data elements for use with rules and filters

In LEM, a group is an object that organizes elements for use with rules and filters. This chapter describes the seven types of groups in LEM, and provides information about managing groups.

About LEM groups

Groups in LEM are objects that organize related elements for use with rules and filters. Groups can contain elements such as events, IP addresses, computer names, user accounts, and so on. After a group is defined, it can be referenced from multiple rules and filters.

Do not confuse groups and roles:

- Groups organize related elements into logical units so that they can be used in rules and filters.
- Roles restrict the actions that users can perform in LEM. See About LEM roles for information about LEM role types.

About LEM Group Types

There are seven group types in LEM:

- User-defined groups
- Event groups
- Directory Service groups
- Time-of-day sets
- Connector profiles
- Email template
- State variables

Each group type is briefly described below.

User-defined groups

User-defined groups contain data specific to your environment, such as user and computer names, the names of sensitive files, trusted IP addresses, and so on. User-defined groups are typically used in rules and filters to whitelist or blacklist events that LEM should include or ignore when evaluating rules and filters. LEM ships with more than two dozen user-defined groups that need to be populated with values for your environment. See Configure user-defined groups in LEM for more information. You can also create rules that auto-populate user-defined groups with values. See Auto-populate user-defined groups using a LEM rule for details.
Event groups

Event groups gather similar events into a single category for use with rules and filters. For example, create an event group for events that should all trigger the same response from LEM. If an event in the group occurs, LEM will fire the rule for that group. LEM ships with more than a dozen predefined event groups, such as: virus(scanner) events, process start/stop events, change management events, and so on.

Directory Service groups

Directory Service groups (DS groups) are groups of users or computers that LEM imports from Microsoft Active Directory. DS groups are synchronized with Active Directory every five minutes. Use DS Groups in rules and filters to match specific users or computers. For example, use a DS group in a filter to limit the scope of events to only users or computers in that group.

Time-of-day sets

Time-of-day sets are defined time periods that you can use in rules and filters. Use time-of-day sets to perform specific actions at different hours of the day. For example, if you define a time-of-day set for Working Hours, and another for Outside Working Hours, you can assign different rules to each set. LEM ships with the following predefined time-of-day sets: business hours, early shift, graveyard shift, late shift, normal shift, and reboot cycle.

Connector profiles

Connector profiles are groups of Agents with common connector configurations. Most Agents in a network only have a few different network security connector configurations. Using connector profiles, you can group Agents by their common connector configurations, and enable your rules and filters to include or exclude the Agents associated with a profile.

Email template

Email templates are pre-formatted email messages that your rules use to notify you when an event occurs.

State variables

State variables are used in rules to represent temporary or transitional states. For example, you can create a state variable to track the state of a system, setting it to a different value depending on whether the system comes online or goes offline.
How groups are added to filters and rules in the LEM console

This section demonstrates how groups are used in filters and rules.

The following image shows the Filter Creation screen in the LEM console. On the left side, groups are organized by group type. On the right side, the filter definition pane shows that the Service Audit Alerts event group is included as a condition of the filter.

The next image shows the Rule Creation screen in the LEM console. Again, groups are organized by group-type on the left side. On the right side, the rule definition pane shows two different groups in the Correlations section: the Network Audit Alerts event group, and the Approved DNS Servers user-defined group. Four child fields are specified in the Network Audit Alerts event group: SourcePort, DestinationPort, SourceMachine, and DestinationMachine.
Manage LEM groups: Add, edit, view, and more

Default groups that have not been saved under a new name will revert to their original settings the next time you upgrade LEM. SolarWinds recommends that you clone any group that is included with LEM before you make changes to the group. This practice will prevent groups with custom values from being overwritten. See Clone a group for more information.

Open the Groups View in the LEM console

To open the Groups view in the LEM console, navigate to Build > Groups. Use the Groups view to create, name, configure, and organize your groups.

The following screen capture shows the Groups view in the LEM console.

Refer to the table for descriptions of the columns in the Groups grid.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opens a menu of commands you can perform on a selected grid item.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>The group type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The group name.</td>
</tr>
<tr>
<td>Description</td>
<td>The group description. Pointing to this field displays the complete description as a tooltip.</td>
</tr>
<tr>
<td>Created By</td>
<td>The console user who created the group.</td>
</tr>
<tr>
<td>Created Date</td>
<td>The group creation date.</td>
</tr>
<tr>
<td>Modified By</td>
<td>The console user who last modified the group.</td>
</tr>
<tr>
<td>Modified Date</td>
<td>The recent date when the groups were modified.</td>
</tr>
</tbody>
</table>
The Groups grid lists every group associated with a LEM Manager instance. If you manage multiple LEM Managers from a single console, and each LEM Manager has a copy of a group, the group will appear multiple times in the grid.

To sort groups by LEM Manager or by group type, click the corresponding column headings.

### Find a group with the Refine Results pane

Use the Refine Results pane to filter the groups grid and reduce the number of groups displayed. The Refine Results pane displays items that match the filter criteria, and hides everything else. For example, to only view Time of Day Set items, type *Time of Day Set* in the search field. To restore hidden items, either click Reset, or select All in the refinement lists.

The following screen capture shows the Refine Results pane.

![Refine Results pane](image)

Refer to the table for descriptions of the controls in the Refine Results pane.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset</td>
<td>Returns the form and the Groups grid to their default settings.</td>
</tr>
<tr>
<td>Search</td>
<td>Enter your search text in the text box. The grid displays only those groups that match or include your entered text. For example, type <em>Email Template</em> to only view Email Template items.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the group type that appears in the grid.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select a Manager to display groups associated with the Manager.</td>
</tr>
</tbody>
</table>
Add a new group

When you create a group, it is only added to the LEM Manager that is selected when you create the group. To copy a group for use with another LEM Manager, export the group and then import it into the other Manager's Groups grid. See Export a group for steps.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. In the upper-right corner of the Groups grid, click +, and then select the group type you want to create.
   - The Group Details pane opens to display an editable form for your selected group type.
4. Complete the form, and then click Save.
   - Choose from the following topics for help completing the form:
     - Create or edit a user-defined group
     - Create or edit an event group
     - Create a directory service group and synchronize it with Active Directory
     - Create or edit a Time of Day Set

Edit a group

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. Next to the group that you want to edit, click ⚙️, and then choose Edit.
   - The Group Details pane opens to display an editable form for your selected group type.
4. Edit the form, and then click Save.
Clone a group

When you clone a group, you copy an existing group and label it with a new name. Cloning allows you to create group variations for use with your rules and filters.

Cloned groups are created on the same LEM Manager instance as the original instance. To duplicate a group for use with another LEM Manager, export the group and import it from the Groups grid. See Export a group for steps.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. Next to the group that you want to clone, click ⚒, and then choose Clone.
   The cloned group appears in the Groups grid below the original instance.

   A cloned group uses the same group name as the original group, followed by an integer. For example, a clone of the Disk Warning group would be called Disk Warning 2. A second clone would be called Disk Warning 3, and so on.

4. Rename and edit the group’s settings as needed.

Export a group

Export a group to save a copy of the group outside of LEM. You can also export a group from one LEM Manager and import it into another Manager. You can only export one group at a time.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. Click ⚒ next to the group that you want to export, and choose Export.
   The Save As dialog box opens.
4. Choose a location to save the group file, and then click Save.
   The exported group file is saved with a .swgrp file extension.
   You can now import the group for use with another Manager.

Import a group

You can import groups from a remote source into the Groups grid. You can import a group that you exported from another LEM Manager instance, or you can import a group provided by SolarWinds. You can only import one group at a time.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. In the upper-right corner of the Groups grid, click 📜, and then choose Import.
   The Open dialog box opens.

4. Navigate to the group file that you want to import, and then select it.
   Group files have a .swgrp file extension.

5. Click Open.
   The group is added to the Groups grid.

6. In the Group Details pane, assign the group to a LEM Manager instance.
   Complete the remaining selections.

7. To send the imported group to the LEM Manager, click Save.

8. If you are working with email templates or state variables, drag the new group from the Groups grid into the folder (in the Folders pane) that stores the group.

Delete a group

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Build > Groups.

3. Next to the group that you want to delete, click ⚒, and then choose Delete.

4. When prompted, click Yes to confirm the delete.
   The group is removed from the Groups grid.
Configure user-defined groups in LEM

User-defined groups contain values relevant to your IT environment, such as user and computer names, sensitive file locations, trusted IP addresses, and so on. Like other groups, they contain information that you can use in rules and filters. This topic provides steps to add and edit values in user-defined groups. You can also create rules that auto-populate user-defined groups with values. See Auto-populate user-defined groups using a LEM rule for details.

If Active Directory is available, use directory service groups to add user and computer accounts to rules and filters. A user-defined group cannot be synchronized with Active Directory, but a directory service group can synchronize with Active Directory every five minutes. See Configure directory service groups in LEM for details.

How rules and filters use user-defined groups

Following are a few rules that depend on user-defined groups:

- A rule that stops LEM from blocking accounts in a user-defined group of trusted administrator accounts.
- A second rule that sends out an alert when an account in the same user-defined group of trusted admin accounts logs in or makes changes.
- A rule that checks a user-defined group containing trusted IP addresses to see if it should block a certain IP address.

Rules and filters typically make use of user-defined groups in slightly different ways:

- In a rule, user-defined groups are typically used like a white list or black list that tell LEM which events it should include or ignore.
- In a filter, user-defined groups limit the scope of the filter to items that belong to the group.

Rules that use user-defined groups include:

- Authentication - Unknown User
- Critical Account Logon Failures
- Detach Unauthorized USB Devices
- File Audit - Delete Sensitive Files
- Non-Admin Server Logon
- Vendor - Unauthorized Server Logon

Filters that use user-defined groups include:

- Admin Account Authentication
- Domain Controllers (all)
Create or edit a user-defined group

See Add a new group or Edit a group to get started adding or editing a group. You can create as many user-defined groups as you need to support your rules and filters. Well-planned groups provide flexibility.

ℹ️ You can only add a group to one LEM Manager at a time. To copy a group for use with another LEM Manager, export the group and then import it into the other Manager's Groups grid. See Export a group for steps.

The following image shows the user-defined group form. The form lists the elements that are configured for the group.

The following table describes how to configure the form fields for user-defined groups.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the group.</td>
</tr>
<tr>
<td>Description</td>
<td>Briefly describe the purpose of the group.</td>
</tr>
<tr>
<td>LEM Manager</td>
<td>Click the Manager drop-down list and select the Manager that will host the group. If you are editing an existing group, this field displays the hosting Manager.</td>
</tr>
<tr>
<td>+</td>
<td>Click + at the bottom of the form to add an element to the group. When you finish entering values, click Save at the bottom of the Element Details form.</td>
</tr>
<tr>
<td>−</td>
<td>Click − to remove an element from the group.</td>
</tr>
<tr>
<td>Element Details</td>
<td>Name – The name of the data element. Data – The specific element that you want to include or ignore in your rules and filters. You can use an asterisk (*) as a wild card to include all similar data elements. Description – A description of the element and its intended use.</td>
</tr>
<tr>
<td>Save</td>
<td>Click Save in the lower-right corner to make your group changes permanent.</td>
</tr>
</tbody>
</table>
Customize the blank and sample user-defined groups included with LEM

SolarWinds recommends customizing the following blank and sample user-defined groups for your environment:

- Admin accounts
- Admin groups
- Approved DNS servers
- Authorized USB devices
- Authorized VPN users
- Sensitive files
- Service accounts
- Suspicious external machines
- Suspicious local machines
- Trusted IPs
- Trusted server sites
- Vendor and contractor accounts
- Vendor-authorizes servers

The Admin Accounts group is used in several template rules as a placeholder for a custom list of administrative users. This group represents the default administrative accounts in Windows and Unix/Linux environments. SolarWinds recommends that you clone this group before you customize it so that you can use it in both capacities. See Clone a group for more information.

Customize user-defined groups

SolarWinds recommends cloning any group that contains a default or suggested value before you alter it. This practice ensures that you have a backup of the default group should you need it later. See Clone a group for more information.

Complete the following procedure to customize any or all the user-defined groups listed above.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. Locate the group you want to edit.
   Use the search box or Type menu on the Refine Results pane, if necessary.
4. Next to the group, click ⚙, and then select Edit.
   If you want to clone the group, select Clone instead, and then repeat this step for the cloned group.
5. Add an element to the group.
   a. Click Add Element, denoted by + at the bottom of the details pane.
   b. In the Name field, enter a nickname for the element. This value is for reference only.
   c. In the Data field, enter a value to define the element (required). Consider using wildcard characters, such as asterisks (*), to abbreviate these entries as illustrated in the example at the end of this procedure.
   d. In the Description field, enter a description (Optional).
   e. Click Save.

6. To modify an element, click the element in the details grid, and then modify it in the Element Details form just as you would when adding a new element.

   To remove an element, click the element in the details grid, and then click Remove Element, denoted by - at the bottom of the details pane.

7. If you are finished editing the group, click Save.

Use the pre-populated user-defined groups as examples of what your custom groups might look like. The Data field is used for the correlation, while the Name field is for reference, and the Description is optional.

The following is an excerpt from the default Admin Groups User-Defined Group:

**Group Name: Admin Groups**

<table>
<thead>
<tr>
<th>NAME</th>
<th>DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td><em>Administrators</em></td>
</tr>
<tr>
<td>Backup Operators</td>
<td><em>backup oper</em></td>
</tr>
<tr>
<td>DNS Admins</td>
<td>DNSAdmin*</td>
</tr>
</tbody>
</table>

**Configure event groups in LEM**

Event groups organize similar events for use with rules and filters. For example, if you add an event group to a rule, the rule will fire any time an event in the group occurs. LEM ships with more than a dozen predefined event groups, for example: virus/scanner events, process start/stop events, change management events, and so on.

**Create or edit an event group**

See Add a new group or Edit a group to get started adding or editing a group.

The following table describes how to configure the form fields for event groups.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the event group.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Briefly describe the purpose of the event group.</td>
</tr>
<tr>
<td>LEM Manager</td>
<td>Click the Manager drop-down list and select the Manager that will host the group. If you are editing an existing group, this field displays the hosting Manager.</td>
</tr>
</tbody>
</table>

**Events**

Select the events to include in the group.

- Click to search for a specific event.
- Click to view the events lists in tree view.

![Event Group](image)

- Click to view an itemized list of events.

![Event Group](image)

**Save**

To save your changes, click Save.

### Configure directory service groups in LEM

This section explains how to manage Active Directory groups for use with LEM rules and filters.

[i] Complete the following tasks before you configure directory service groups for the first time:

- Configure the Directory Service Query Connector
- Sync Active Directory with LEM
About directory service groups

Active Directory groups that are configured to sync with LEM are called directory service groups. Directory service groups contain either Windows users or computer accounts. Any changes that you make in Active Directory propagate to LEM rules and filters.

If Active Directory is available, use directory service groups to add user and computer accounts to rules and filters. A user-defined group cannot be synchronized with Active Directory. Allowing LEM to access Active Directory directly via a directory service group means you do not have to maintain duplicate groups of user and computer records in LEM, saving time and reducing the risk of human error. Following integration, you can white-list or black-list select Active Directory groups using LEM rules and filters.

Create a directory service group and synchronize it with Active Directory

Complete these steps to select which Active Directory groups to synchronize with LEM. The synchronization process runs every five minutes if the connector is running.

Before you begin, the Directory Service Query connector must be configured on the LEM Manager.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. In the upper-right corner of the Groups toolbar, click  and then select Directory Service Group.
   The Select Directory Service Group form opens.
4. From the list, select the LEM Manager that will use the DS groups.
5. Use the folder tree on the left to populate the Available Groups pane on the right. The form displays the actual contents (folders and Group categories) of your directory service system.
   Each folder contains the group categories associated with that area of your directory service. You can maximize a folder to display the group categories within the folder.
   The Available Groups section lists a different set of group categories with each folder you select. For example, clicking the Users folder displays a different set of group categories compared to the Laptops folder.
6. Select the DS groups that you want to import into LEM Manager.
7. Repeat the previous two steps until you have selected all the groups that you want to import.

8. Click Save.

The system synchronizes the DS groups to LEM and adds them to the Groups grid.

You can now use the DS groups with your rules and filters.

View a directory service group member in the LEM console

The Groups grid displays various LEM groups, including each directory service group synchronized with LEM. Select a DS group in the grid to view the members of that group in the Directory Service Group pane.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Build > Groups.

3. In the Groups grid, select the directory service group you want to view.

To sort groups by group type, click the Type column heading.

The Directory Service Group pane lists the group members.

Directory service group grid columns

The Directory Service Group pane lists each computer account and user account associated with the DS group. The following table describes each grid column.

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Displays an icon that shows if the group member is a user or a computer. The computer icon represents a computer account. The person icon represents a user account.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the group member.</td>
</tr>
<tr>
<td>Description</td>
<td>The description associated with the group member.</td>
</tr>
<tr>
<td>SAM Name</td>
<td>The account name of the member.</td>
</tr>
<tr>
<td>COLUMN</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Principal Name</td>
<td>The principal name of the member.</td>
</tr>
<tr>
<td>Distinguish Name</td>
<td>The complete distinguished name of the member.</td>
</tr>
<tr>
<td>Email</td>
<td>The email address of the member.</td>
</tr>
</tbody>
</table>

Remove a directory service group from LEM

Directory service groups can be deleted from LEM the same as any other group. See [Delete a group](#) for steps. Deleting a DS group does not remove the group from Active Directory, however. You can restore a DS group at any time.

Configure the connector-profile group type in LEM

Use the connector-profile group type to maintain and monitor LEM Agents that share a common connector configuration. For example, a connector profile can help you maintain and monitor multiple domain controllers. Most Agents in a network only have a few different connector configurations. By using connector profiles, you can create rules and filters that include or exclude Agents that share the same connector configuration.

For more information about connector profiles, see [Create connector profiles to manage and monitor LEM Agents](#).

Configure state variables in LEM

Use the Groups grid to add, edit, and delete state variables and the number, text, and time fields associated with each variable.

State variables are used in rules to represent temporary or transitional states. For example, you can create a state variable to track the state of a system, setting it to a different value depending on whether the system comes online or goes offline.

You can also configure rules to monitor the contents of a state variable to validate or invalidate a rule. For example, you can set a DEFCON value and ensure that the DEFCON value is over 3 before notifying your on-call staff.

If you require permanent lists of data that can be preserved over long periods of time, you can use user-defined groups in a similar manner.

Add a new state variable field

1. On the LEM toolbar, navigate to Build > Groups.
2. In the Groups grid, click ⚙, and then select State Variable.
   - If you are editing a state variable, click 🗝, next to the variable, and then select Edit.
The State Variables pane displays as an editable form. If you are editing an existing state variable, the form displays any preconfigured fields.

3. In the Name box, enter a name for the state variable.
4. Click the Manager drop-down list and select the LEM Manager instance that will host the state variable. If you are editing an existing group, this field displays the hosting Manager.
5. To display the Add Variable Field form, click .
6. In the Name box, enter a name for the state variable field.
7. In the Type list, select the type of state variable the field represents (Text, Number, or Time).
8. To save the field, click Save in the first column.
   The new State Variable field appears in the State Variables grid with the field name and comparison type.
9. Repeat steps 5 through 8 for each field you want to add to the state variable.
10. To save the state variable settings, click Save in the right column.
    The new state variable displays in the Groups grid and the State Variables list in Rule Builder. You can incorporate this state variable whenever you add or edit a rule.

**Edit a state variable field**

1. On the LEM toolbar, navigate to Build > Groups.
2. In the Groups grid, select a state variable.
3. Click , and then select Edit.
   The State Variables pane opens as an editable form.
4. In the Fields grid, select the state variable field you want to edit.
   The Add Variable Field form appears, showing the current field configuration.
5. Edit the field Name or Type as required.
6. To apply your changes, click Save.
   The updated field appears in the fields grid.

7. To save your changes to the state variable, click Save in the lower-right corner below the Comparison Type column.

Delete a state variable field

1. On the LEM toolbar, navigate to Build > Groups.
2. Select a state variable you want to delete.
3. Click ⌁, and then select Edit.
4. In the Groups grid, do either of the following:
   The State Variables pane opens as an editable form.
5. In the Fields grid, select the field you want to delete.
6. Click ✗ to delete the field.
   The field is removed from the Fields grid.
7. To save the changes, click Save.

Manage state variable folders

As with rules and email templates, you can use the Folders pane to organize your state variables into folders and sub-folders. You can add, rename, move, and delete state variable folders.

Configure Time of Day Sets in LEM

Use Time of Day Sets in filters and rules to target specific time frames, such as business hours, off hours, or specific shifts. For example, if you define two different sets for Business Hours and Outside Business Hours, you can assign different rules to each of these sets. During working hours, you may want your rules to alert a system administrator through email, whereas outside of business hours the rule can send an alert and shut down the offending PC.

LEM includes the following Time of Day Sets by default:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Hours</td>
<td>6:30 AM to 12:00 PM and 1:00 PM to 4:30 PM, Monday through Friday</td>
</tr>
<tr>
<td>Early Shift</td>
<td>3:30 AM to 1:30 PM, 7 days a week</td>
</tr>
<tr>
<td>Graveyard Shift</td>
<td>9:00 PM to 4:30 AM, 7 days a week</td>
</tr>
<tr>
<td>Late Shift</td>
<td>3:00 PM to 12:00 AM, 7 days a week</td>
</tr>
<tr>
<td>Normal Shift</td>
<td>7:30 AM to 5:30 PM, 7 days a week</td>
</tr>
<tr>
<td>Reboot Cycle</td>
<td>2:00 AM to 3:00 AM, Sunday only</td>
</tr>
</tbody>
</table>
Create or edit a Time of Day Set

See [Add a new group](#) or [Edit a group](#) to get started adding or editing a Time of Day Set.

You can only add a new Time of Day Set to one LEM Manager at a time. To copy a Time of Day Set for use with another LEM Manager, export it and then import it into the other Manager’s Groups grid. See [Export a group](#) for steps.

![The Time of Day Set form](image)

The following table describes the Time of Day Set form fields.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this Time of Day Set.</td>
</tr>
<tr>
<td>Description</td>
<td>Briefly describe the purpose of the set.</td>
</tr>
<tr>
<td>LEM Manager</td>
<td>Click the Manager drop-down list and select the Manager that will host the Time of Day Set. If you are editing an existing Time of Day Set, this field displays the hosting Manager.</td>
</tr>
<tr>
<td>Time grid boxes</td>
<td>The time grid is based on a one-week period and includes:</td>
</tr>
<tr>
<td></td>
<td>- Seven rows, where each row represents one day of the week.</td>
</tr>
<tr>
<td></td>
<td>- 24 numbered columns, where each column represents one hour of the day. The white column headers represent morning hours (midnight to noon). The shaded column headers represent evening hours (noon to midnight).</td>
</tr>
<tr>
<td></td>
<td>- Columns with two check boxes that divide each hour into two 30-minute periods. (Each box represents a half-hour.)</td>
</tr>
<tr>
<td></td>
<td>Select the boxes for the half-hour increments that you want to include in the Time of Day Set.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Click and drag to select or clear a range of boxes with one click." /></td>
</tr>
<tr>
<td>Save</td>
<td>Click Save in the lower-right corner to make your group changes permanent.</td>
</tr>
</tbody>
</table>
Use a Time of Day Set in a filter or rule

1. Locate and click the alert or alert group you want to use in your filter or rule.
2. In the Fields list, locate and drag DetectionTime to the Conditions box.
3. In the Components pane, click Time of Day Sets.
4. Locate the time of day set you want to use and drag it into the conditions area to replace the Text Constant field, (denoted by a pencil icon).
5. To view all events outside your selected period, click the operator between the field and your Time of Day Set in the conditions area.
   The operator changes to Does Not Contain.
6. If you are finished creating or editing your filter or rule, click Save.
   If you modified a rule, click Activate Rules in the Rules view.
LEMM filters: Capture real-time events and historical data with filter criteria

About LEM filters and filter categories

This section introduces filters and briefly describes the default filters included with LEM.

Filters capture events and alerts that take place on your network. (In LEM, the terms event and alert are interchangeable.)

The LEM console uses event filters to manage events. You can turn filters on and off, pause filters to sort or investigate events, perform actions to respond to events, and configure filters to notify you when they capture an event. Filters can also display widgets, which are charts and graphs that visually represent the event data.

Filter conditions can be broad or specific. For example, you can create a filter without conditions that captures all events, regardless of the source or event type, or you can create a filter that has one specific condition, such as "UserLogon Exists," which only captures user logon events.

Create filters when you want to group a type of event. For example, you can create filters to collect all events from your domain controllers, or all events for a specific type of user.

Create rules when you want LEM to take action in response to one or more events.

Use filters to group a type of event or to monitor specific events

You can create filters to collect:

- All events from your firewalls
- All events from your domain controllers
- All events for a specific type of user
- All events except for recurring, expected events

Create custom filters to monitor specific events, such as:

- Change Management filters to monitor configuration changes users create in your network.
- High Volume Event filters to monitor traffic spikes or unexpected off-peak traffic.
- General Interest filters to monitor log in failures and failed authentications.

A failed authentication is an event triggered by three logon failures by the same account within an extremely short period of time.

- Rule Scenario Event filters to determine if you have the appropriate events to create a rule for a specific scenario.
- Daily Problem Event filters to monitor basic operational problems (such as account lockouts) in real time.

About the default filters included with LEM

SolarWinds LEM ships with filters that support best practices in the security industry. You can modify these filters to meet your needs, or you can create an unlimited number of custom filters. A single set of filters can monitor data collected across multiple LEM Managers.

Find and view filters in Monitor view

To find a filter in LEM, open the Monitor tab in the LEM console, and click Filters in the top-left part of the screen to open the Filters sidebar. Expand a category to view its filters. To view a brief description of a filter, hover your cursor over it.

Filtered events are listed in the event grid, or you can view filtered event data using a variety of charts and graphs called widgets. Filters can also use the console to signal that they have captured an event by displaying a pop-up message, by playing a sound, or by using blinking text.

Filters are in the Filters pane, where they are grouped into different categories.

![Filters pane](image)

About LEM filter categories

By default, filters are grouped into the following seven categories in the Filters pane:

- Overview
- Security
- IT Operations
- Change Management
- Authentication
- Endpoint Monitoring
- Compliance

You can also add, edit, rename, export, import, and delete filter categories. See Manage LEM filter categories: Add, edit, view, and more for details.
About the Filters sidebar

The number to the right of each filter name shows the number of events associated with that filter. Filters shown in gray italics are currently turned off. To move a filter from one category to another, click and drag it to its new location.

Default filters included with LEM

This section lists the default filters included with LEM.

Overview Filters

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>DEFAULT STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Events</td>
<td>Displays all events from all sources.</td>
<td>On</td>
</tr>
<tr>
<td>Subscriptions</td>
<td>Filters events related to rules subscribed to the specified user.</td>
<td>On</td>
</tr>
<tr>
<td>LEM Internal Events</td>
<td>Filters events related to LEM operations, including informational, warning, and audit events.</td>
<td>On</td>
</tr>
<tr>
<td>Rule Activity</td>
<td>Displays all activated rules.</td>
<td>On</td>
</tr>
</tbody>
</table>

Security Filters

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>DEFAULT STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents</td>
<td>Filters all events categorized as Incidents.</td>
<td>On</td>
</tr>
<tr>
<td>Security Events</td>
<td>Filters events categorized as attack activity or potentially suspicious.</td>
<td>On</td>
</tr>
<tr>
<td>Network Event Threats</td>
<td>Filters events with source or destination detected in the threat intelligence feed as potentially bad actors.</td>
<td>On</td>
</tr>
<tr>
<td>All Firewall Events</td>
<td>Filters events from firewall devices that match the targeted name.</td>
<td>On</td>
</tr>
<tr>
<td>All Threat Events</td>
<td>Filters all events with the source or destination detected in the threat intelligence feed as potentially bad actors.</td>
<td>On</td>
</tr>
<tr>
<td>Denied ACL Traffic</td>
<td>Filters events from network devices that indicate denied ACL activity.</td>
<td>Off</td>
</tr>
<tr>
<td>Unusual Network Traffic</td>
<td>Filters unusual network traffic and scans.</td>
<td>On</td>
</tr>
<tr>
<td>Blocked Web Traffic</td>
<td>Filters events from proxy servers or other web servers that blocked an attempt to access a URL.</td>
<td>On</td>
</tr>
<tr>
<td>NAME</td>
<td>DESCRIPTION</td>
<td>DEFAULT STATUS</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Proxy Bypassers</td>
<td>Filters web traffic users who are bypassing your proxy server.</td>
<td>Off</td>
</tr>
<tr>
<td>Web Traffic - Spyware</td>
<td>Filters web traffic events to potential spyware sites.</td>
<td>Off</td>
</tr>
<tr>
<td>Virus Attacks</td>
<td>Filters events that indicate potential virus detection.</td>
<td>On</td>
</tr>
<tr>
<td>IDS Scan / Attack Activity</td>
<td>Filters security events detected by IDS tools (such as Snort).</td>
<td>On</td>
</tr>
<tr>
<td>Security Processes</td>
<td>Filters security-related process activities.</td>
<td>On</td>
</tr>
<tr>
<td>File Audit Failures</td>
<td>Filters events that indicate failed attempts to access files.</td>
<td>On</td>
</tr>
</tbody>
</table>

**IT Operations Filters**

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>DEFAULT STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Domain Controller Events</td>
<td>Displays all traffic from machines in the Domain Controllers tool profile.</td>
<td>Off</td>
</tr>
<tr>
<td>All Web Traffic</td>
<td>Filters all web traffic-related events from network devices, proxy servers, and web servers.</td>
<td>On</td>
</tr>
<tr>
<td>Software Installation/Update</td>
<td>Filters events related to software installation and updates.</td>
<td>On</td>
</tr>
<tr>
<td>Service Events</td>
<td>Filters events related to starting and stopping services, as well as service warnings and information.</td>
<td>On</td>
</tr>
<tr>
<td>System Events</td>
<td>Filters events related to system availability and status information.</td>
<td>On</td>
</tr>
<tr>
<td>Error Events</td>
<td>Filters events from all sources that contain &quot;error&quot;.</td>
<td>On</td>
</tr>
<tr>
<td>Warning Events</td>
<td>Filters events from all sources that contain &quot;warning&quot;.</td>
<td>On</td>
</tr>
<tr>
<td>Windows Error Events</td>
<td>Filters events from Microsoft Windows event logs that contain &quot;error&quot;.</td>
<td>On</td>
</tr>
<tr>
<td>Error Events for Device</td>
<td>Filters events from a specific device that contain &quot;error&quot;.</td>
<td>Off</td>
</tr>
<tr>
<td>Web Traffic for Source Machine</td>
<td>Filters web traffic emanating from a certain source machine.</td>
<td>Off</td>
</tr>
<tr>
<td>All Network Traffic</td>
<td>Filters all network traffic-related events from all devices and systems.</td>
<td>On</td>
</tr>
<tr>
<td>FTP Traffic</td>
<td>Filters TCP traffic events between one or more FTP ports reported by any device or system.</td>
<td>On</td>
</tr>
</tbody>
</table>
### SNMP Traffic Filters

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>DEFAULT STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Traffic</td>
<td>Filters UDP traffic events between one or more SNMP ports reported by any device or system.</td>
<td>On</td>
</tr>
<tr>
<td>SMTP Traffic</td>
<td>Filters UDP traffic events between one or more SMTP ports reported by any device or system.</td>
<td>On</td>
</tr>
</tbody>
</table>

### Change Management Filters

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>DEFAULT STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Change Management</td>
<td>Filters all events that indicate changes to devices, systems, users, groups, and domains.</td>
<td>On</td>
</tr>
<tr>
<td>User Account Changes</td>
<td>Filters changes to existing user accounts.</td>
<td>On</td>
</tr>
<tr>
<td>Machine Account Changes</td>
<td>Filters changes to existing machine accounts.</td>
<td>On</td>
</tr>
<tr>
<td>Group Changes</td>
<td>Filters creation, deletion, and changes to groups.</td>
<td>On</td>
</tr>
<tr>
<td>Domain &amp; Membership Changes</td>
<td>Filters new and deleted domain accounts (including users/groups) and domain changes.</td>
<td>On</td>
</tr>
<tr>
<td>Device/System Policy Changes</td>
<td>Filters events related to policy changes on devices and systems.</td>
<td>On</td>
</tr>
<tr>
<td>All File Audit Activity</td>
<td>Filters events related to all types of audited file access.</td>
<td>On</td>
</tr>
<tr>
<td>USB File Auditing</td>
<td>Filters file-related alerts from Agents running USB Defender</td>
<td>On</td>
</tr>
</tbody>
</table>

### Authentication Filters

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>DEFAULT STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Logons</td>
<td>Filters all types of user logons.</td>
<td>On</td>
</tr>
<tr>
<td>Interactive User Logons</td>
<td>Filters background network logon types.</td>
<td>On</td>
</tr>
<tr>
<td>Remote User Logons</td>
<td>Filters events that indicate remote Windows system logons.</td>
<td>On</td>
</tr>
<tr>
<td>Failed Logons</td>
<td>Filters events that indicate failed logon attempts to devices and systems.</td>
<td>On</td>
</tr>
<tr>
<td>Account Lockouts</td>
<td>Filters events that indicate an account was locked out.</td>
<td>On</td>
</tr>
<tr>
<td>Authentication Event Threats</td>
<td>Filters authentication events with a source or destination detected in the threat intelligence feed as potentially bad actors.</td>
<td>On</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Status</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Admin Account Authentication</td>
<td>Filters authentication events related to specified administrative accounts.</td>
<td>Off</td>
</tr>
</tbody>
</table>

Endpoint Monitoring Filters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation Logon/Logon Failure Activity</td>
<td>Filters non-network workstation logon/logon failure to a domain or local account.</td>
<td>On</td>
</tr>
<tr>
<td>Local Account Authentication/Changes</td>
<td>Filters any user-related audit events that are not to or from the corporate domain.</td>
<td>On</td>
</tr>
<tr>
<td>Software Installed on Workstations</td>
<td>Filters software installations on workstation systems.</td>
<td>On</td>
</tr>
<tr>
<td>USB-Defender Events</td>
<td>Filters USB Defender events.</td>
<td>On</td>
</tr>
<tr>
<td>Workstation Events with Threats</td>
<td>Filters all events detected on endpoints with a source or destination detected in the threat intelligence feed as potentially bad actors.</td>
<td>On</td>
</tr>
</tbody>
</table>

Compliance Filters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top PCI Events</td>
<td>Filters the most common PCI events of interest, which include change management, unexpected file access, incidents, and attacks.</td>
<td>Off</td>
</tr>
<tr>
<td>Top HIPAA Events</td>
<td>Filters file activity, changes, and incidents related to HIPAA events.</td>
<td>Off</td>
</tr>
<tr>
<td>Top Banking Compliance Events</td>
<td>Filters common banking compliance events, including change management, users and groups, and potentially suspicious attack activity.</td>
<td>Off</td>
</tr>
</tbody>
</table>

Create a new LEM filter for real-time monitoring

This section describes how to create a new LEM filter. It covers how to create a filter by clicking New Filter in the Filters pane, and how to create a new LEM filter from an existing event.

See also:
Create a new LEM filter

You can create custom filters from the Monitor view in your LEM console to display real-time traffic from your monitored computers and devices.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or auditor.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, click , and then select New Filter.
4. Enter a filter name and description.
5. Change the Lines Displayed value to modify the number of events your filter can store in memory.
   ![Lines Displayed: 1000]
   The default value is 1000.
6. Configure the correlations (or relationships) that define the filter. These correlations define the events that must occur for the filter to take effect.
   a. Drag Event or Event Group items from the filters and groups list pane into the Correlations box. Click \( \square \) to add a group.

You can create custom correlations in Monitor view and nDepth view using the filters and groups list pane. It contains categorized lists of events, event groups, event fields, Groups (from the Groups grid), profiles, and constants that you can use to create conditions for your filters, rules, and search queries.
b. Click the correlations connector bar. Select AND [ ] to determine if the alert conditions must all apply or OR [ ] if any alert conditions apply to prompt a response.

If your correlations require a value, populate the value using one of the following procedures:

- Enter a static text value in the Text Constant field, denoted by a pencil icon. Use asterisks (*) as wildcard characters to account for any number of characters before, within, or after your text value.
- Drag a group from the list pane to replace the Text Constant field. The most commonly used groups include User Defined Groups, Connector Profiles, Directory Service Groups, and Time Of Day Sets.
- Drag an Event field from an existing event in your Correlations to replace the Text Constant field. This will result in a parameter that states whether values from different Events in your Correlations should match.

7. If you want to change the operators in your conditions, click the operator until you find the one you want.

There are two types of operators: Condition and Group.

- Condition operators are found between your events and their values. Examples include Equals, Does Not Equal, Contains, and Does Not Contain. Rule Creation only displays the operators that are available for the values in your Correlations.
- Group operators are found outside of your correlation groups. The two options are And (blue) and Or (orange).

For more information see Comparing values with operators in LEM filters and rules.

8. Maximize the Notifications group and drag a notification into the Notifications box.

9. Set your AND [ ] and OR [ ] operators as required.

10. Click Save.
Create a LEM filter from a specific event

To create a new LEM filter for a specific event type, click Create a Filter From This Event at the top of the Event Details pane.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or auditor.
2. On the LEM toolbar, click Monitor.
3. In the Event Grid, select the event that you want to create a filter for.
4. From This Event, click Create a Filter.
   A new filter appears in the Filters pane.
5. Modify the new filter to display more specific data (Optional).
   a. Select the filter in the Filters pane.
   b. Click the gear icon at the top of the Filters pane, and then select Edit.
   c. Edit the filter by selecting the Events tab in Filter Creation, selecting fields to monitor more specific details of this event type, and then clicking Save.

Manage LEM filter categories: Add, edit, view, and more

This topic describes how to work with filter categories (which the LEM console calls filter groups). Use these steps to customize filter categories to suit your needs. See About LEM filters and filter categories for general information about filter categories.

Add a new filter category

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, click  , and then select New Group.
   A new filter category appears in the Filters pane.
4. Enter a name for the category and press Enter.
   The new filter category appears in the Filters list.

Rename a filter category

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select the category you want to rename.
4. Click 📚, and then select Edit.
5. Enter a new name for the category, and then press Enter.
   The category name is changed.

**Move a filter category up in the list**

By default, new filter categories appear at the bottom of the Filters pane. You can rearrange them so that they appear in a different order.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, drag the filter category title bar to a new position.

**Move a filter to another category**

You can click and drag filters between categories.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, click to expand the filter category that contains the filter you want to move.
4. Click and drag the filter to another category.

The filter appears in its new category.

**Move a filter category to another workstation**

See Export a filter or filter category for steps.
Create a backup copy of a filter category for archival purposes

See Export a filter or filter category for steps.

Export a filter or filter category

Export filters when you need to:

- Move one or more filters to another workstation so that another LEM console user can use the same filters
- Export one or more filters to a folder for backup or archival purposes
- Send SolarWinds Technical Support a copy of the filter for troubleshooting purposes

Use the Export Filter command to export a single filter. Use the Export Filter Group command to export all of the filters in a filter category.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select the filter or the filter category that you want to export.
4. Click , and then select Export Filter or Export Filter Group.
   The Save As dialog box opens.
5. Choose the location that you want to save the file to, and click Save.
   The exported filter file is saved with a .swfil file extension.
   The exported filter group file is saved with a .swfgp file extension.

Import a filter or filter category

Use the Import Filters/Group command to import either a .swfil filter file, or a .swfgp filter group file into LEM. See Export a filter or filter category to create the .swfil or .swfgp file.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. If importing a single filter, select the filter category that you want to add the imported filter to.
4. Click , and then select Import Filters/Group.
   The Open dialog box opens.
5. Navigate to the filter or filter group file that you want to import.
   Filter files have a .swfil file extension; filter group files have a .swfgp file extension.
6. Click Open.
   The filter or filter category is added to the Filters pane.
Delete a filter category

Before you delete a filter category, move any filters that you want to save to another filter category.

Deleting a filter category deletes all the filters stored within that category, as well as all of the widgets associated with the filters.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select the filter category you want to delete.
4. In the filter header, click 🗑.
5. To confirm the delete, click Yes.

The filter category and all its filters are deleted. The filter category no longer appears in the Filters pane.

Manage LEM filters: Add, edit, view, and more

This section describes how to work with filters in the LEM console. See About LEM filters and filter categories for general information about filter categories.

Open filters in the LEM console

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, click a filter category to expand it and view its filters.
4. Click a filter to view its events in the event grid.

Manage filter-based widgets in Monitor view

See "The Monitor view" on page 1.

Create a new filter

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, click to select a filter category for the new filter. This tells LEM which category to add the filter to.

4. In the Filters toolbar, click \( \text{+} \), and then select New Filter.

   The Filter Creation window opens.

5. Complete the form.

   See **Building custom filter and rule expressions in LEM** to learn how to write filter and rule expressions.

   - See the following table for help completing the Filter Creation page.
   - Use the Filter Status section to verify, troubleshoot, and resolve any problems with the filter logic.

6. Click Save.

   The new Save displays in the selected filter group.

The Filter Creation form fields

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a filter name. This name will identify the filter in the Filters pane.</td>
</tr>
<tr>
<td>Lines Displayed</td>
<td>Select the total number of events to display for this filter. You can select up to 2,000 lines. The default value is 1,000 lines.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a short description of the filter.</td>
</tr>
<tr>
<td>Conditions (box)</td>
<td>Drag one or more event(s) and/or LEM group(s) into the Conditions box. See <strong>Create conditions to filter event reporting</strong> for more information.</td>
</tr>
<tr>
<td>COLUMN</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Notifications (box)</td>
<td>To have LEM display a notification when a filter captures an event, drag the notification from the Notifications group into the Notifications box and configure the notification method. Notifications include displaying a pop-up message, displaying new events as unread, playing a sound, or using blinking text to display the filter name.</td>
</tr>
</tbody>
</table>

**Edit an existing filter**

You can edit an existing filter using the Filter Creation window. After you open the filter, you can change the name, description, configuration, and notification settings.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, expand the filter group that contains the filter that you want to edit.
4. Select the filter to edit, click 🏢 on the Filters toolbar, and then select Edit. The selected filter opens in the Filter Creation window.
5. Edit the Filter Creation form as needed.
   - Use the Filter Status section to verify, troubleshoot, and resolve any problems with the filter logic.
     - See The Filter Creation form for help completing the form.
     - See Get started building custom filter expressions in LEM for information about constructing filters.
6. To save your changes, click Save.

**Share a filter with another user**

See Export a filter or filter category for steps.

You need the Administrator or Auditor role to share a filter with another user. To share a filter with Monitor-role users, see Specify the filters that users assigned the Monitor role can use in the LEM console.

**Clone a filter**

When you clone a filter, you copy an existing filter and label it with a new name. Cloning allows you to quickly create filter variations.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select the filter that you want to clone.
4. On the Filters toolbar, click 🔄, and then select Clone.
LEM creates a cloned copy of the filter below the original filter and appends Clone to the name.

5. To edit the filter and rename it, select the filter, click ⌘, and then select Edit.

6. Edit the Filter Creation form, and then click Save.
The cloned filter is saved to your Filters list.

Copy a filter

Copy a filter if you want the filter to appear in more than one filter category.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, open the filter group that contains the filter that you want to copy.
4. In the Filters pane, select the filter category that you want to copy the filter to.
5. Select the filter that you are copying, and then press Ctrl and drag the filter to the targeted group.
   A copy of the filter appears in the new filter group.

Create a backup copy of a filter for archival purposes

See Export a filter or filter category for steps.

Export a filter

See Export a filter or filter category for steps.

Export a filter when you need to:

- Move a filter to another workstation so that another LEM console user can use the same filter
- Export a filter to a folder for backup or archival purposes
- Send SolarWinds Technical Support a copy of a filter for troubleshooting purposes

Import a filter

See Import a filter or filter category for steps.

Use the Import a filter command to import a .swfil file into LEM.

Delete a filter

⚠️ Deleting a filter will also delete any widgets associated with the filter. Deleted filters and widgets cannot be restored.
1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select the filter that you want to delete.
4. Next to the filter, click ✕.
5. To confirm the delete, click Yes.
   The filter disappears from the Filters pane.

Send a filter to nDepth

To view historical filter data about a filter while in Monitor mode, select the filter, click ✟, in the Filters pane, and then select Send to nDepth. The console will open the filter in the nDepth search engine under Explore mode. See Choose a filter in Monitor view to send to nDepth for historical search for steps.

Start, stop, and pause filters in LEM

This section describes how to start, stop, and pause filters in the LEM console.

About starting, stopping, and pausing filters

Filters starts collecting events from the moment they are turned on. Turn off LEM filters that you do not need to conserve system resources. Pause a filter if you need to inspect a set of event messages and you do not want to see new incoming messages scrolling across the grid. You can pause one filter or all filters in the console.

See About LEM filters and filter categories for general information about filters.

Turn a LEM filter on

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select the filter that you want to turn on.
4. In the Filters pane, click ✗, and then select Turn On.
   The filter is now active and the title no longer appears grayed out.

Turn a LEM filter off

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select the filter you want to turn off.
4. In the Filters pane, click ⬇️, and then select Turn Off.
   The filter title changes to gray italics to indicate that it is off.

Pause one LEM filter

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select the filter you want to pause.
   *The event grid updates to display the filter you selected.*
4. Click ⬇️, and then select Pause.
   A label with the word Paused appears next to the filter.

To resume, click ⬆️, and then select Resume.

<table>
<thead>
<tr>
<th>Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Incidents</td>
</tr>
<tr>
<td>Security Events</td>
</tr>
<tr>
<td>Network Event Threats</td>
</tr>
</tbody>
</table>

Pause all LEM filters

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, click ⬇️, and then select Pause All.
   A label with the word Paused appears next to all filters that are not turned off.

To resume, click ⬆️, and then select Resume All.
LEM widgets and the Ops Center: Visually monitor network events in LEM

About LEM widgets

This section provides general information about widgets.

Widgets present important high-level information in an easy-to-read graphical format, such as a chart or a graph. They provide special dashboard functionality, such as displaying real-time information about network activity, or providing tools for investigating events and related details.

LEM provides a library of widgets, or you can create your own by using filters that you have customized to monitor specific activity. If your widget includes charts, you can click a specific line, bar, or pie wedge to open the source filter. The corresponding filter opens the Monitor view, and displays the targeted filter information. The filter lists only the events that correspond with the selected chart item.

See Open a filter from a widget for information about using widget filters.

In the LEM console, widgets are primarily displayed in OpsCenter View. You can add and arrange widgets on this page as needed to help troubleshoot network issues and recognize potential problems before they occur. Widgets also appear in Monitor view and Explore > nDepth view.

- In Monitor view, widgets allow you to view graphical views of your filters along with their grid-based views. See for more information.
- In nDepth view, each widget represents a high-level graphical view of the specific network activity associated with your nDepth search results. See Using nDepth widgets in LEM for details.

You can edit or remove existing widgets, or rearrange widgets to meet your personal preferences. Widgets can be resized, but sizes and aspect ratios are enforced to keep the Ops Center tidy and organized.

To get started with widgets, click a widget and review its ToolTips for more information, or use the control options on the toolbar to change the widget setting display format.

Widget icons

The following table describes the function of each button on a widget toolbar.

<table>
<thead>
<tr>
<th>BUTTON</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit</td>
<td>Opens the widget in the Widget Builder to edit the settings.</td>
</tr>
<tr>
<td></td>
<td>Rotates the widget interface to display the presentation format settings.</td>
</tr>
<tr>
<td>refresh</td>
<td>Refreshes the widget data.</td>
</tr>
</tbody>
</table>
### Button Function

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximize</td>
<td>Maximizes the widget to full-screen mode.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the widget from the dashboard (in normal dashboard mode).&lt;br&gt;When you edit a rotated (or flipped) widget, it closes the widget edit mode and returns it to the normal desktop view.</td>
</tr>
<tr>
<td>Legend</td>
<td>Opens the widget legend.</td>
</tr>
</tbody>
</table>

**View specific widget data**

Widget graphs and charts display basic high-level information. Each widget includes tooltips that provide specific data about each bar, line, or wedge in the chart. This information is typically the reported event, event group, or event field and its corresponding occurrences.

To view specific chart data, mouse over a bar, line, or pie slice and the tooltip appears, providing specific data about your targeted item.

![User Logons by User Account](image.png)

**Refresh widget data**

On the widget toolbar, click refresh to display the latest data from your network. Widgets automatically refresh according to the refresh rate configured in the widget. If a widget has a slow refresh rate (as indicated at the bottom of the widget), you can click refresh or edit the Refresh setting in the widget. Refreshing a widget displays the most current real-time data from your network traffic.
View a widget legend

Each widget bar chart, graph, and pie chart includes a legend that defines the items in the illustration. Click 🔄 to view the legend.

![Legend Example](image)

Widgets that ship with the LEM console

The following table describes the widgets that ship with the LEM console.

<table>
<thead>
<tr>
<th>Widget Name/Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Events</td>
<td>Displays all events from all filters.</td>
</tr>
<tr>
<td>Events by Event Type</td>
<td>Displays a count of the top 10 events by event type (event name).</td>
</tr>
<tr>
<td>Events by Connector Name</td>
<td>Displays the number of events captured by each configured connector, over time.</td>
</tr>
<tr>
<td>Events per Minute</td>
<td>Displays the total count of events per minute for the last 15 minutes.</td>
</tr>
<tr>
<td>Change Management</td>
<td>Displays events related to changes occurring on the network.</td>
</tr>
<tr>
<td>Change Management Events by Agent</td>
<td>Displays the top 10 Agents generating change management events</td>
</tr>
<tr>
<td>Change Management Events by Type</td>
<td>Displays the top 10 change management events by event type.</td>
</tr>
<tr>
<td>Failed Logons</td>
<td>Displays all user account failed logon attempts.</td>
</tr>
<tr>
<td>Failed Logons by User Account</td>
<td>Displays the top five failed logons by user account name.</td>
</tr>
<tr>
<td>Widget Name/Filter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File Audit Failures</td>
<td>Displays <code>FileAuditFailure</code> events that show failed attempts to access audited files.</td>
</tr>
<tr>
<td>File Audit Failures by File Name</td>
<td>Displays the top 10 file names generating file audit failures.</td>
</tr>
<tr>
<td>File Audit Failures by Source Account</td>
<td>Displays the top 10 source accounts generating file audit failures.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Displays all events from firewall devices.</td>
</tr>
<tr>
<td>Firewall Events by Firewall</td>
<td>Displays the top five firewalls generating firewall events</td>
</tr>
<tr>
<td>Firewall Events by Type</td>
<td>Displays the top five firewall events by event type.</td>
</tr>
<tr>
<td>Incidents</td>
<td>Displays all Incident events.</td>
</tr>
<tr>
<td>Incidents by Rule Name</td>
<td>Displays the top five incidents by the name of the rule that generated the Incident.</td>
</tr>
<tr>
<td>Interactive Logons by User Account</td>
<td>Displays the top 10 user logons by user account name.</td>
</tr>
<tr>
<td>My Rules Fired by Rule Name</td>
<td>Displays the top five subscribed events by the name of the rule that generated them.</td>
</tr>
<tr>
<td>Network Events</td>
<td>Displays all Network events.</td>
</tr>
<tr>
<td>Network Events by Source Machine</td>
<td>Displays the top 10 machines generating network events.</td>
</tr>
<tr>
<td>Network Event Trends</td>
<td>Displays the top 10 network-related events by event type.</td>
</tr>
<tr>
<td>Rule Activity</td>
<td>Shows all the rules that have fired.</td>
</tr>
<tr>
<td>Rules Fired by Rule Name</td>
<td>Displays the top five rules fired by rule name.</td>
</tr>
<tr>
<td>Security Processes</td>
<td>Displays process launches and exits from processes in the &quot;Security Processes&quot; User-Defined Group, which is used to monitor critical security-related processes.</td>
</tr>
<tr>
<td>Security Processes by Agent</td>
<td>Displays the top 10 Agents generating security process events.</td>
</tr>
<tr>
<td>Subscriptions</td>
<td>Displays events created by rules you are &quot;Subscribed&quot; to in the Rules area.</td>
</tr>
<tr>
<td>SolarWinds Events</td>
<td>Displays all Internal events (events generated during operation of the LEM).</td>
</tr>
<tr>
<td>Unusual Network Traffic</td>
<td>Displays events that indicate unusual or suspicious network traffic.</td>
</tr>
<tr>
<td>Widget Name/Filter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unusual Network Traffic by Destination</td>
<td>Displays the top five destinations for unusual network traffic.</td>
</tr>
<tr>
<td>Unusual Network Traffic by Source</td>
<td>Displays the top 10 sources of unusual network traffic.</td>
</tr>
<tr>
<td>USD Defender</td>
<td>Displays all USB-Defender events.</td>
</tr>
<tr>
<td>USB-Defender Activity by Detection IP</td>
<td>Displays the top 5 Agents with the most USB-Defender events.</td>
</tr>
<tr>
<td>USB File Auditing</td>
<td>Displays USB-Defender's File Auditing events.</td>
</tr>
<tr>
<td>USB File Auditing by Detection IP</td>
<td>Displays the top five Agents with the most USB file auditing events.</td>
</tr>
<tr>
<td>User Logons</td>
<td>Displays all user account logons.</td>
</tr>
<tr>
<td>User Logons by Agent</td>
<td>Displays the top five Agents reporting user logons.</td>
</tr>
<tr>
<td>User Logons by Source Machine</td>
<td>Displays the top five user logons by source machine.</td>
</tr>
<tr>
<td>User Logons by User Account</td>
<td>Displays the top 10 user logons by user account name.</td>
</tr>
<tr>
<td>User Logons (Interactive)</td>
<td>Displays interactive user account logons.</td>
</tr>
<tr>
<td>Virus Attacks</td>
<td>Displays all virus attack events.</td>
</tr>
<tr>
<td>Virus Attacks by Source Machine</td>
<td>Displays the top 5 sources of virus attacks or infections.</td>
</tr>
</tbody>
</table>

**Manage LEM widgets with Widget Manager: Add, edit, and more**

Use the Widget Manager to create, add, edit, and delete your dashboard widgets.

**About the Widget Manager**

Widget Manager includes Widget Builder, which provides the tools you need to create new master widgets. Master widgets are widget templates located in LEM's Widget Manager categories list. Copy a master widget to the OpsCenter dashboard or to Monitor view to create a dashboard widget. Because all dashboard widgets operate independently of the master widget, editing a master widget will not impact the corresponding dashboard widget.

Using Widget Manager, you can:
- Create, edit, and delete master widgets
- Add or delete widgets from the dashboard

To access Widget Manager, click the Ops Center view and then click Widget Manager.

This screen capture shows the "Widget manager" portion of the Ops Center view in the LEM console:

---

**Locate widgets**

Widgets are stored in the Ops Center and Monitor views.

The Ops Center view stores all master widgets in the Widget Manager Categories list. Dashboard widgets cannot be stored in the Widget Manager.

The Monitor view displays master widgets in the Widgets pane based on the filter you select as a data source. Dashboard widgets do not appear in the Widgets pane.

**Add a master widget to the dashboard**

You can add a copy of a master widget to the dashboard from the Widgets pane or Widget Builder. After you copy the widget to the dashboard, you can edit the widget as required. The original widget remains with its filter in the Categories pane.

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, click Ops Center.
3. On the Ops Center toolbar, click Widget Manager.
4. In the Categories pane, select a filter.
5. In the Widgets pane, select an available widget.
6. Click Add to Dashboard or drag the widget to the dashboard.

   The widget is saved to the Ops Center dashboard.

   To re-position the widgets on the dashboard, drag them to a new position.
Edit a dashboard widget

You can edit a dashboard widget without affecting the corresponding master widget. During the edit, the Save to Dashboard option is disabled.

1. Locate a widget on the Ops Center dashboard.
2. On the widget toolbar, click ⌁ ⌘ ⌘ .
3. Edit the widget in Widget Builder as required.
4. Click Save.

   The widget is updated based on your new settings.

Delete a dashboard widget

Widgets can only be deleted from the Ops Center. You can delete dashboard widgets directly from the dashboard.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Ops Center.
3. In the dashboard, locate the widget you want to delete.
4. On the widget toolbar, click ⌘ .
5. When prompted, click Yes.

   The widget is deleted from the dashboard.

   You can recreate the dashboard widget from the master widget.

Open a filter from a widget

1. On the LEM toolbar, click Ops Center.
2. On the dashboard, locate the appropriate widget.
3. On the widget, click a chart element (line, bar, or pie wedge).

   The Monitor view appears displaying the filter used for the widget data source.

   If your selected item does not appear in the Monitor event grid, modify the Scope setting in the widget.

4. To return to the dashboard, click Ops Center in the upper-left corner.

Move (relocate) a widget

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Ops Center.
3. To close the Categories and Widgets panes, click Widget Manager (if required).
4. Click and hold the targeted widget header.
5. Drag the widget to a new location.
   The remaining widgets rearrange on the dashboard to accommodate the new location.
6. Release the mouse button and drop the widget in the new location.

### Resize a widget

To view a widget in full-screen mode, click maximize ▶️ in the widget toolbar. To return the widget to its original size, click maximize ▶️ again.

To resize a widget in the dashboard, drag the bottom right corner of the widget until your desired size is highlighted in the dashboard grid. When you release the mouse button, the widget adjusts to your new size.

### Create and edit widgets with Widget Builder

This section describes how to configure the Widget Builder form when creating and editing widgets.

Widget Manager includes Widget Builder, which you will use to edit an existing widget or to create a new master widget. After you create a widget, you can save a copy to the Ops Center dashboard.

Use the Widget Manager to edit any master widget associated with a filter. Edit a widget to change the widget's name, behavior, or appearance, or if you want to create a new dashboard widget based on a master widget configuration. When you save the widget, the widget appears in the Widget Manager and the Widgets pane in the Monitor view.

---

> Because all dashboard widgets operate independently of the master widget, editing a master widget will not impact the corresponding dashboard widget. As a result, you can use a master widget as a template for creating variations of the same widget for the dashboard.

### Create a new widget

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, click Ops Center.
3. On the Ops Center toolbar, click Widget Manager.
4. To open Widget Builder, click ☐ in the Categories toolbar.
5. Complete the Widget Builder form:
a. See Enter the general widget settings for help.
b. See Enter the visual configuration settings for help.
c. See Enter the data configuration settings for help.

6. To save a copy to the Ops Center dashboard, select the Save to Dashboard check box (optional).

7. Click Save.

The new widget appears in the Widgets pane and is stored in the Categories pane under your selected filter category.

If you select the Save to Dashboard check box, the widget also appears in the Ops Center dashboard.

Edit a master widget

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, click Ops Center.

3. On the Ops Center toolbar, click Widget Manager.

4. In the Categories pane, select a filter.

The associated widgets display in the Widgets pane.

5. Drag the scroll bar to locate your targeted widget.

6. On the Categories toolbar, click ☀.

7. In Widget Builder, edit the widget configuration as required.

   a. See Enter the general widget settings for help.

   b. See Enter the visual configuration settings for help.

   c. See Enter the data configuration settings for help.

8. To save a copy to the Ops Center dashboard, select the Save to Dashboard check box (optional).

9. Click Save.

The new widget configuration appears in the Widgets pane.

If you selected the Save to Dashboard check box, the widget also appears in the Ops Center dashboard.

Edit a dashboard widget

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, click Ops Center.

3. Select a widget window, and then click Edit at the top of the widget window.
4. Update the form as needed:
   a. See Enter the general widget settings for help.
   b. See Enter the visual configuration settings for help.
   c. See Enter the data configuration settings for help.

5. Click Save.
   The updated widget configuration appears in the Op Center Widget Manager, and the Widget pane appears in the Monitor tab.

Configure the Widget Builder form

The following topics document the Widget Builder form.

Enter the general widget settings

1. In the Name field, enter a name for the widget.

2. In the Description field, enter a description for the widget (up to 80 characters).

3. From the Filter drop-down list, select the filter data source.

When you select your filter data source, use the following conventions:

- If the filter appears in italics, the filter is turned off.
- If you create a widget from a disabled filter, the widget will not display any chart information until the filter is re-enabled.
- When you create a widget in the Monitor tab, this field defaults to the currently-active filter. If you select a different filter, the widget will be associated with your targeted filter and not the active filter.
- When you create a widget in the Ops Center tab, this field defaults to the first option in the list.

4. Enter the visual configuration settings.
Enter the visual configuration settings

1. From the Visualization Type drop-down list, select the appropriate graph.

   ![Visualization Configuration](image)

   - **Visualization Type**: From the drop-down list, select the appropriate graph.
   - **Color**: Choose a color palette for the chart.
   - **X Axis Label**: Enter a name for the chart or graph horizontal axis (optional).
   - **Y Axis Label**: Enter a name for the chart or graph vertical axis (optional).

2. Click Color and select a color palette for the chart or graph.

3. In the X Axis Label field, enter a name for the chart or graph horizontal axis (optional).

4. In the Y Axis Label field, enter a name for the chart or graph vertical axis (optional).

5. Enter the data configuration settings.

Enter the data configuration settings

1. From the Field drop-down list, select a data field to report in the widget.

   ![Data Configuration](image)

   - **Field**: Select a data field to report in the widget.
   - **Show**: Choose the data frequency reported in the widget.
   - **Sort**: Select the data sort method.
     - a. To list the data from highest to lowest (Z to A or 10 to 1), select Descending.
     - b. To list the data from lowest to highest (A to Z or 1 to 10), select Ascending.
   - **Versus**: Select another data field for a second data dimension in the chart (optional).
   - **Split By**: Select another data field for a third data dimension in the chart (optional).

2. From the Show drop-down list, select the data frequency reported in the widget.

   - **To count the number of occurrences for the selected Field value, select Count. For example, if you select EventID in the Field drop-down menu, the widget will count the number of events.**
   - **To count the number of occurrences when a unique event occurs, select Distinct Count. For example, if you select a Field value such as Event Name or Detection IP, the widget counts each specific value once. This option reports all values as 1 in a single-dimension chart. As a result, this option is best suited for multidimensional charts.**

3. From the Sort drop-down list, select the data sort method.
   - a. To list the data from highest to lowest (Z to A or 10 to 1), select Descending.
   - b. To list the data from lowest to highest (A to Z or 1 to 10), select Ascending.

4. From the Versus drop-down list, select another data field for a second data dimension in the chart (optional).

5. From the Split By drop-down list, select another data field, for a third data dimension in the chart...
6. From the Limit drop-down list, select a value to limit the number of items to chart. The default value is 5.

7. From the Scope drop-down lists, select the appropriate time frame reported by the chart or graph. For example, selecting a scope of 30 minutes will display the last 30 minutes of data in the chart or graph.

   Choose a narrow scope for frequent events. Choose a wide scope for events that rarely occur.

8. From the Resolution drop-down lists, select the time values (displayed as tick marks) for the horizontal X-axis in the chart. This value is required when Versus is a time field.

   For example, if your Scope is 30 minutes, you can set the Resolution to five minutes to indicate five-minute tick marks on the X-axis.

9. From the Refresh drop-down, select the data refresh rate for the widget display.

10. Click Save.

Using nDepth widgets in LEM

This section documents how to use widgets in the Explore > nDepth view of the LEM console. For general information about widgets, see About LEM widgets

About nDepth widgets

nDepth includes a variety of commonly-used widgets like the widgets in the Ops Center. Each widget represents a high-level graphical view of the specific network activity associated with your nDepth search results. The widget displays the primary items generating an activity, as well as the count (or number of incidents) for each item.

Use nDepth explorer views to create new widgets, change the look of existing widgets, add widgets to the nDepth Dashboard, and remove widgets you no longer use. To display the latest data from your network, click refresh on the widget.
View nDepth widget details

Click or point to an item in the widget to view details and statistics about the item.

Create a search string from a widget item

You can use items in widgets or any of the nDepth graphical tools to create new search strings, or to append existing search strings.

1. On the search bar, click \( \times \) to delete the existing search string.
2. Click an item on a widget.
   
   A new search string associated with the widget item appears in search box.

To append an existing search string with an item from a widget, click an item on the widget. In the search box, a new search string associated with the widget item is appended to the existing search string.

Add a new nDepth widget

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. Click a view on the nDepth toolbar, such as bar charts, line charts, pie charts, or bubble charts.
   
   The corresponding view appears.
4. On the view title bar, click \( + \) to open the nDepth widget builder.
5. Complete the Widget Builder selections to configure the new widget. See Configure the Widget Builder form for help.

   The new widget appears at the bottom of the chart view. When you configure the widget and choose the Save to Dashboard option, the new widget also appears at the bottom of the nDepth dashboard.
Edit an nDepth widget

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. Click a view on the nDepth toolbar, such as bar charts, line charts, pie charts, or bubble charts.
4. On the widget you want to edit, click .
5. Use the nDepth Widget Builder to reconfigure the widget. See Configure the Widget Builder form for help.
   The updated widget appears at the bottom of the view.
   When you configure the widget and choose the Save to Dashboard option, the new widget also appears at the bottom of the nDepth dashboard.
6. To refresh the widget data, click .

Add a chart widget to the nDepth dashboard

You can add an nDepth view (such as word cloud, tree view, or result details) to the nDepth Dashboard. The word cloud, tree view, and result details view display by default. If you remove a view from the dashboard, use this procedure to restore the view.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. Use the nDepth explorer toolbar to open the chart view you want to work with.
4. In the view, locate the chart widget you want to add to the dashboard.
5. In the widget toolbar, click to move the widget to the dashboard.
   The widget is copied to the bottom of the nDepth Dashboard.
   To minimize the widget in the dashboard, click . To restore the widget, scroll down and click the widget title bar.
LEM rules: Automate how LEM responds to events

About LEM rules

Rules monitor event traffic and automatically respond to security events in real time, whether you are monitoring the console or not. When an event (or a series of events) meets a rule condition, the rule prompts the LEM Manager to act. A response action can be discreet (for example, sending a notification to select users by email), or active (for example, blocking an IP address or stopping a process).

See About LEM response actions for information about response actions.

Rules can respond to one or more events. In many cases, you can base rules on several events that LEM correlates to trigger an action. You can also configure a rule to look for a single event.

Rules can only fire on normalized data and not on raw log data that is received.

Rules play a key role in detecting operational and compliance issues on your network, such as external breaches, insider abuse, and policy violations. The LEM console ships with a set of preconfigured rules to help you get started.

To view a short introductory video about rules and learn how to add preconfigured rules to LEM, see: http://video.solarwinds.com/watch/2imHNpmWYYZJtV2r8ZMqB

To get started customizing preconfigured rules, see Find and add LEM rules

LEM rule scenarios

Countless scenarios may warrant a rule. Consider these combinations of rules and actions:

- Respond to change management events with the Send Email Message action.
- Respond to port scanning events with the Block IP action.
- Respond to isolated spikes in network traffic with the Send Email Message or Disable Networking action.
- Respond to users playing games on monitored computers with the Send Popup Message or Kill Process action.
- Respond to users attaching unauthorized USB devices to monitored computers using the Detach USB Device action.

Any activity or event that can pose a threat to your network might warrant a LEM rule.
View rules, rule categories, and rule templates in the LEM console

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Build > Rules.
   Saved rules are listed in the Rules grid. The sidebar includes a search bar, and a menu of rule categories and tags.

3. To view a list of matching templates in the Rule Templates grid (located below the Rules grid), select a rule category in the sidebar.

Rule configuration requirements and best practices
Review the following requirements and best practices about creating LEM rules.

Use descriptive rule names
To keep rules simple to manage, SolarWinds recommends creating the rule with a name that describes the event.

Set the Correlation, Correlation time, and Action
Each rule requires you to define three settings:

- Correlation: The number of events that occur within a selected amount of time and the amount of time allocated to responding to the events.
- Correlation time: The volume of events that match the correlation conditions and the rolling time window to evaluate the correlation.
- Action: The action that occurs when the rule is triggered.

Activate a rule to upload local changes
When you create a new rule, or change an existing rule, you are working on a local copy of the rule. The LEM Manager cannot use the rule change until you activate it. Activating a rule tells the LEM Manager to reload its enabled rules and upload updates from your local copies.

Click the Activate button to activate rules whenever you create a new rule, edit an existing rule, or change the Enabled/Disabled or Test On/Test Off status. Otherwise, the LEM Manager will not recognize your changes. After activating rules, LEM begins processing all enabled rules.

i See Enable and activate rules prior to testing for details.

Check the rule status for errors
Check the Rule Status below the Description field to view the rule status and errors. If the rule status is good, the status displays in green.

![Rule Status: OK]
If the rule status is not good, maximize Rule Status to view the errors.

Verify that a rule fired

Check your console for InternalRuleFired events using either a filter or nDepth search. These events will show the triggered rule and when it occurred.

Test new rules before putting them into production

Before you put a rule into production, try it out in test mode. In test mode, the LEM Manager processes the rule alert messages, but does not execute any rule actions. This lets you see how the activated rule will behave without disrupting your network.

Create email templates for use with LEM rules

Email templates are pre-formatted messages that LEM sends to users when alert events trigger a rule.

About LEM email templates

You can use email templates to customize your email notifications when triggered as responses in your rules. An email template includes static and dynamic text (or parameters). The static text lets you customize the appearance of the email. The dynamic text is filled in from the original event that triggered the rule to fire.

Create email templates to report specific information about an alert event and variables that capture specific parameters about that event. For example, you can report which server is affected, what time the event occurred, or which Agent was shut down. Or you can create an Account Lockout template to notify key personnel when an account is locked out, or automatically file a trouble ticket. Create static text to describe the event, and incorporate dynamic text that provides the account information from the original event.

Create templates that are specific to an event type to avoid having to create one email template per rule. For example, you can have one template for Account Modification that can provide a notification when a user is added or removed from a group, when a password is reset, or when other account details are changed. There is no limit to the number of templates you can create.
Managing email templates and template folders

You can organize your email templates into folders and sub-folders. Manage templates and folders using the following operations:

- Email templates – You can add, edit, clone, and delete templates, and organize them into folders.
- Template folders – You can add, rename, move, and delete template folders as needed.

Best practices to keep rules, events, and emails simple to manage

To keep rules, events, and emails simple to manage, SolarWinds recommends the following:

- Create the rule with a name that describes the event.
- Create the email template with a name that describes the event.
- In the email template subject or message, enter the event or rule name to describe the event or alert.

When you receive the email, you can identify the email template, the rule that fired, and the event that caused the rule to fire.

Create or edit an email template

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Groups.
3. In the Groups grid, click + and select Email Template, or select one of the existing email templates. The Email Template form displays.
   
   If you are editing an existing template, the form shows the parameters that are configured for the template. Clone the template, and then modify the name and parameters of the template.

4. Complete the Email Template form.
a. In the Details pane, enter a template name. This will be used in rules to reference the template.

b. To create dynamic text (parameters) for the rule:
   i. Type a name in the Name field under the Parameters list and click . For example, DetectionIP, DestinationAccount, EventInfo, and so on. This name is a reference to the actual event data.
   ii. Repeat this for all the parameters you want to add.

   Each parameter is a variable that holds your data and places it in the right location in the email. For example, for an Account Lockout template, consider using the Time, Account, DC, and Machine parameters.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEM Manager menu (unlabeled)</td>
<td>Select the LEM Manager that will host the template. If you are editing an existing template, this field displays the Manager associated with the template.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for the template. The name will be used in rules to reference the template. The name should describe the event that occurred or the destination of the email message.</td>
</tr>
<tr>
<td>From</td>
<td>Enter who sent the message. For example, you can enter SolarWinds or Manager.</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter a subject for the message. The subject should indicate the nature of the alert event. To use a Parameter, enter the name as it appears in the parameters list, including the dollar sign, or drag it from the Parameters list into where you want it to appear in the subject. Using a dynamic Parameter in the Subject provides a subject that includes the user account name, source, or any other text from the originating event.</td>
</tr>
<tr>
<td>Message</td>
<td>Enter the email message that LEM sends when an event occurs. Select and drag a parameter from the Parameters list to the appropriate place in the message text. Parameters serve as placeholders for information that LEM Manager fills in when the email is sent. You can use a combination of static and dynamic text, such as Account $Account locked out at $Time on DC $DC from computer $Machine. This would display the following: Account testuser locked out at 7/21/2016 8:05am on DC DC1 from computer PC1</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parameters</td>
<td>Lists the variables that provide placeholders for specific items within the message text. When LEM sends the message, LEM Manager prompts you to fill in the message variables from the Events or Event Groups lists. LEM then completes the message by filling in the variable parameters with the appropriate text. You can create a variable for Agents, servers, or time, and you can add as many parameters as you need. For example, you may want to add a parameter to be filled in with the affected Agent or server name, and another parameter to be filled in with the time the event occurred. To add and delete parameters, use the controls in the Name row at the bottom of the screen.</td>
</tr>
<tr>
<td>(parameter)</td>
<td>To add a message parameter to the email template, enter the parameter name and click +. Add additional parameters as needed for use with the message. To delete a message parameter from the template, select the parameter that you want to delete and then click −.</td>
</tr>
</tbody>
</table>

5. To save the template, click Save.

The Email template is added to the Groups grid and will be available in the Actions component list when you drag Send Email Message or Send Pager Message to the Actions box. LEM will prompts you to fill in the message variables from the Events or Event Groups lists.

### Find and add LEM rules

This section describes how to find and customize preconfigured LEM rules.

### Find and add rules based on categories of interest

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, click OpsCenter.
3. In the Getting Started widget, click Define Rules and Configure Alerts.
   
   By default, the Getting Started widget is in the top left part of the page.

   ![Specify conditions where you want LEM to alert you](#)  

   » Define Rules and Configure Alerts

4. Select the check box next to the types of rules that you want to enable, and then click Next.
5. Complete the fields and selections to define the condition, correlation time, and action for each new rule, and then click Apply.

6. On the LEM toolbar, navigate to Build > Rules.

7. In the Rules grid, locate a new rule, click ☑, and then select Enable.

   A ☑ displays next to the enabled rule.

8. Complete step 5 for each additional rule.

9. Enable your rule. See Enable and activate rules prior to testing for details.

10. Test the rules to verify they work as expected. See Testing rules in LEM for details.

Clone, customize, and enable a specific preconfigured rule

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Build > Rules.

3. Use Refine Results in the sidebar to browse, search, or filter for specific rules or scenarios, or browse for a rule in the Rule Categories and Tags section.

4. Select a rule to clone, click the corresponding ☑, and then choose Clone.

5. In the Clone Rule dialog box, select a Custom Rules folder, rename the rule, and then click OK.

6. On the Rule Creation screen, customize the rule (if desired), and then select Enable.

7. Click Save.

8. To sync your local changes with the LEM appliance, click Activate Rules in the Rules grid. See Enable and activate rules prior to testing for details.

9. Test the rules to verify they work as expected. See Testing rules in LEM for details.
Change Management rule example

Change management rules notify you when a user makes network configuration changes. For example:

- Adding, changing, or deleting users in Active Directory
- Installing software on monitored computers
- Making changes to the firewall policy

You can create a general change management rule to instruct LEM to notify you when a user changes your network configuration, or you can create a more specific rule that applies to specific users, groups, or types of changes. Generally, if you can see an event in your console, you can create a rule for the event. Use your filters as a starting point for creating custom rules.

The following change management rule example notifies you by email when a user adds another user to an administrative group.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. To create a new rule, click .
4. Enter an appropriate name for the rule. For example:
   
   New Admin User
5. In the rule Correlations box, enter the event or event group.
   
   For example, you can use the NewGroupMember.EventInfo Equals *admin* condition to execute anytime LEM receives a NewGroupMember event with admin included anywhere in the Event Info field.
   
   a. In the left pane, click Events.
   
   b. At the top of the Events list, enter NewGroupMember to search for this event, and then select it in the list.
   
   c. In the Fields: NewGroupMemberList, locate EventInfo, and then drag it into the Correlations box.
   
   d. To account for all variations on the word administrator, enter *admin* in the text field (denoted by a pencil icon in the Correlations box).
6. Leave the Correlation Time box as is so your rule fires anytime LEM captures this type of event.
7. Add the Send Email Message action to the Actions box.
   
   a. In the left pane, click Actions.
   
   b. Locate Send Email Message, and then drag the action into the Actions box.
   
   c. From the Email Template drop-down list, select a template.
   
   d. In the Recipients menu, select a LEM user.
   
   e. To complete the action, drag event fields or constants from the left pane into the Send Email Message form.
Always use event fields for events in the Correlations box. For example, you can use `NewGroupMember.DetectionTime` to populate the Detection Time field in this example.

8. In the Rule Creation form, select the Enable check box, and then click Save.

9. To sync your local changes with the LEM appliance, click Activate Rules in the Rules grid.

   The LEM appliance will send an email anytime a user adds a user to any group in Active Directory that contains `admin` in its name.

Create a new LEM rule to monitor and respond to events

This section describes how to create a custom rule to monitor and respond to events from your monitored computers and devices.

See also:

- Rule configuration requirements and best practices
- Building custom filter and rule expressions in LEM to learn how to write filter and rule expressions

For a video presentation about creating rules in the LEM console, open the following URL in a web browser:

http://embed.vidyard.com/share/k6zhzKv9V9d5EibvfGTaN

Create a new rule

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Build > Rules.


4. Enter a name and description for the rule.

5. From the drop-down list, select the LEM Manager that will host this rule.

   If you are editing a rule, this field displays the LEM Manager instance associated with the rule.
6. Click Add Tags.

Select the categories and tags for this rule, and then click OK.

7. Configure the correlations (or relationships) that define the rule. These correlations define the events that must occur for the rule to take effect. You can coordinate multiple alert events into a set of conditions that prompt the LEM Manager to issue an active response.

   a. From the list pane, drag Event or Event Group items into the Correlations box. To add a group, click [ ].

   b. Click the correlations connector bar. Select AND [ ] to determine if the alert conditions must all apply, or OR [ ] if any alert conditions apply to prompt a response.

If your correlations require a value, populate the value using one of the following procedures:

   - Enter a static text value in the Text Constant field, denoted by a pencil icon. Use asterisks (*) as wildcard characters to account for any number of characters before, within, or after your text value.
   - To replace the Text Constant field, drag a group from the list pane. The most commonly used groups include User Defined Groups, Connector Profiles, Directory Service Groups, and Time Of Day Sets.
   - To replace the Text Constant field, drag an Event field from an existing event in your Correlations. This will result in a parameter that states whether values from different Events in your Correlations should match.

8. If you want to change the operators in your conditions, click the operator until you find the one you want.

   There are two types of operators: Condition and Group.

   - Condition operators are found between your events and their values. Examples include Equals, Does Not Equal, Contains, and Does Not Contain. Rule Creation only displays the operators that are available for the values in your Correlations.
- Group operators are found outside of your correlation groups. The two options are And (blue) and Or (orange).

For more information see Comparing values with operators in LEM filters and rules.

9. Configure the correlation time to establish the allowable frequency and time span that the correlation events must occur before the rule applies.

![Correlation Time]

- Set the Events within and Response Window settings for your rule.
- If the Events within value is 2 or more, click Advanced to select advanced threshold fields and define an advanced response window for the alert fields within the grouping.

10. Configure the actions that occur when the events in the Correlations and the Correlations Time boxes occur (for example, sending an email message to the system administrator or blocking an IP address).

Use the following guidelines:

- All rules must have at least one action.
- Populate your action with constants or event fields as appropriate.

a. Click the Actions list.

![Actions]

b. Select and drag an action from the list into the Actions box.

For more information, see About LEM response actions.

For more information, see LEM response actions: Respond to network and system events in LEM.

11. Apply the appropriate Enabled, Test, and Subscribe settings as appropriate.

- To enable the rule after you click Save, select the Enable check box. See Enable and activate rules prior to testing for details.
- To operate the rule in test mode before it is enabled, select the Test check box. SolarWinds recommends running each new rule in test mode to confirm that the rule behaves as expected. See Testing rules in LEM for details.

You must enable a rule before you can test it.
12. Click Save.

The new rule appears in the Rules grid.

13. After your rule is in your Custom Rules folder, click Activate Rules to sync your local changes with the rules folders on your LEM Manager and allow the new or updated rules to function properly.

Example: Create a Change Management rule

This section shows you how to create a rule in LEM by stepping you through an example.

About the Change Management rule example

Rules in the Change Management category notify you when a user makes a network configuration change, for example:

- Adding, changing, or deleting users in Active Directory
- Installing software on monitored computers
- Making changes to the firewall policy

You can create a general change management rule to instruct LEM to notify you when a user changes your network configuration, or you can create a more specific rule that applies to specific users, groups, or types of changes. Generally, if you can see an event in your console, you can create a rule for the event. Use your filters as a starting point for creating custom rules.

The following change management rule example notifies you by email when a user adds another user to an administrative group.

Create the example Change Management rule

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Build > Rules.

3. To create a new rule using the Rule Creation screen, click .

4. Enter an appropriate name for the rule. For example:
New Admin User

5. In the rule Correlations box, enter the event or event group.
   For example, you can use the `NewGroupMember.EventInfo Equals *admin*` condition to execute anytime LEM receives a `NewGroupMember` event with `admin` included anywhere in the Event Info field.
   a. In the left pane, click Events.
   b. At the top of the Events list, enter `NewGroupMember` to search for this event, and then select it in the list.
   c. In the Fields: `NewGroupMember` list, locate `EventInfo`, and then drag it into the Correlations box.
   d. In the text field (denoted by a pencil icon in the Correlations box), enter `*admin*` to account for all variations on the word administrator.

6. Leave the Correlation Time box as is so your rule fires anytime LEM captures this type of event.

7. Add the Send Email Message action to the Actions box.
   a. In the left pane, click Actions.
   b. Locate `Send Email Message`, and then drag the action into the Actions box.
   c. In the Email Template, click the menu, and then select a template.
   d. In the Recipients menu, select a LEM user.
   e. To complete the action, drag event fields or constants from the left pane into the Send Email Message form.

   ![Tips]
   Always use event fields for events in the Correlations box. For example, you can use `NewGroupMember.DetectionTime` to populate the Detection Time field in this example.

8. In the Rule Creation form, select Enable, and then click Save.

9. Test the rules to verify they work as expected. See Testing rules in LEM for details.

10. In the main Rules view, click Activate Rules to sync your local changes with LEM.
    The LEM Manager will send an email anytime a user adds a user to any group in Active Directory that contains `admin` in its name.

Manage LEM rules: Edit, view, export, and more

This section describes how to manage rules in the LEM console. Use the Build > Rules view to manage your rules.
See the following topics to find, add, or create LEM rules:

- Find and add LEM rules
- Create a new LEM rule to monitor and respond to events

Activate a rule

See Enable and activate rules prior to testing for details.

Add tags to a rule

Tags make it easier to categorize and find rules. For example, if you want a rule to appear in several different categories, select the corresponding tags.

1. Open the rule for editing. (See the next section for steps.)
2. At the top of the Rule Builder form, click Add Tags.
   The Tags dialog box opens.
3. Select one or more tags to add to the rule, and then click OK.

Edit a rule

Use the Rule Creation connector to modify or update a rule. When required, you can edit multiple rules at the same time.

Disabling a rule is not required to edit a rule. When you edit a rule, you are editing a local copy until you save and activate the rule. If the rule was enabled when you added your modifications, it will continue to be enabled while you work on the new version. When you save the new version and click Activate Rules, the LEM Manager replaces the original rule with the new version.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rules Categories and Tags pane, maximize the category that contains the rules that you want to edit.
4. In the Rules grid, select the rule (or rules) that you want to edit.
5. To edit a single rule, click 💼 next to the rule, and then select Edit. To edit multiple rules, click 🌼 in the Rules toolbar, and then select Edit.
   The Rule Builder form displays with your selected rule. If you have multiple rules, they appear as cascaded windows on the screen.
6. Edit your rules as required.
7. To save your rule changes, click Save.
Edit a locked rule

If a rule is locked, another user is currently editing the rule. You can open the rule in read-only mode to see the rule details or break the lock and take control over the rule. The other user will not be able to save any changes to the rule.

Clone a rule

The Clone command copies any existing rule, make changes to the copy, and then saves the copy with a new name in one of your Custom Rules sub-folders. Use the Clone command to create variations of existing rules. For example, you can clone a preconfigured rule and then adjust the cloned copy to suit your specific needs.

A cloned rule must apply to the same LEM Manager as the original rule. You cannot clone a rule from one Manager and save it for another Manager.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. From the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, maximize the category that contains the rules you want to enable.
4. In the Rules grid, select the rule you want to clone.
5. Click , and then select Clone.
6. In the Clone Rule form, enter a name for the rule in the Clone Name box.
7. In the Rule Categories and Tags pane, select which Custom Rules folder will store the cloned rule.
8. Click OK.

The cloned copy opens in Rule Creation so you can make changes.

Share a rule with another user

See Export a rule for steps.

Create a backup copy of a rule for archival purposes

See Export a rule for steps.

Export a rule

You can export a rule from one LEM Manager instance and import it into another LEM Manager instance. You can also export rules to:

- Save archived copies in a safe place.
- Provide SolarWinds with a copy of your rule for technical support or troubleshooting purposes.
You can export multiple rules at the same time. The rules are saved to a new folder that contains each rule.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, select the category that contains the rule you want to export.
4. In the Rules grid, select the rules you want to export.
5. On the Rules grid toolbar, click  and then select Export.
6. In the Save in box, locate the general area in which you want to save the exported rule folder.
7. In the File name box, enter folder name to contain the exported rules.

   Rules are saved as swrul files.

8. Click Save.

   The rules are exported and saved in your selected folder. Each exported rule retains its name and the export date and time.

   If an Export Error message displays, one or more rules failed to export. If you are exporting multiple rules, the message lists the failed and succeeded exported rules. Click OK to close the form.

Import a rule

You can import a rule from a remote source into a rule category. For example, you can import a rule from one LEM Manager to another, or import a rule provided by SolarWinds. You can only import one rule at a time.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. On the Rules grid toolbar, click  and then select Import.
4. Locate and open the folder that contains the rule you want to import.
5. Select the rule file you want to import. These files are in XML format.
6. To import the file, click Open.
7. In the Import Rules form, click the Manager drop-down list and select the Manager to associate with this rule.
8. In the Rule Categories and Tags pane, select the category that will store the imported rule.
9. Click Import.

   The system imports the rules into the designated rule folder.
Delete a rule

You can delete one rule at a time, or you can delete multiple rules. Once a rule is deleted, it can only be restored by re-creating it or by importing a previously exported rule.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, select the folder that contains the rule you want to delete.
4. In the Rules grid, select the rule (or rules) you want to delete.
5. To delete a single rule, click 🗑️, and then select Delete. To delete multiple rules, click 🗑️ in the Rules toolbar, and then select Delete.
6. At the Confirm Delete prompt, click Yes.
   The rules disappear from the Rules grid.
7. To notify the LEM Manager component that the rules were deleted, click Activate Rules.

Test, enable, and disable rules in LEM

About selecting multiple rules to test, enable, or disable

You can select two or more rules at the same time to test, enable, or disable by selecting the rules in the grid and clicking 🛡️ in the Rules toolbar. This command, however, acts as a toggle on each selected rule. For example, if one rule is Test On and another is Test Off, performing this command on both rules at the same time inverts the settings of both rules. As a result, the first rule is Test Off and the second rule is Test On. When you perform this command on multiple rules, select rules that are in the same state—Test On or Test Off, or Enabled or Disabled.

Enable and activate rules prior to testing

You must enable a rule before you can test it.

![i] When selecting two or more rules at the same time to enable, select rules that are in the same state—Enabled or Disabled. See About selecting multiple rules to test, enable, or disable for more information.

Enable rules from the Rules grid or directly from the Rules Creation screen. Instructions for both tasks are provided.

⚠️ Do not forget to activate your rule by clicking Activate Rules in the Rules toolbar. This step is frequently overlooked.
Enable rules from the Rules grid

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, maximize the category that contains the rules you want to enable.
4. In the Rules grid, select the rule (or rules) you want to enable.
5. To enable a single rule, click ✏ next to the rule, and then select Enable. To enable multiple rules, click ✏ in the Rules toolbar, and then select Enable.
   The Enabled ✏ icons for each selected rule become active, indicating the rules are enabled.
6. Click Activate Rules in the Rules toolbar to activate the rule.
   The rule is enabled.

Enable rules from the Rule Creation screen

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, maximize the category that contains the rules you want to enable.
4. In the Rules grid, select the rule (or rules) you want to enable.
5. In the Rules toolbar, click ✏, and then select Edit.
6. In the Rule window, click the Enable check box. Repeat this step for each additional opened rule.
7. Click Save.
   The Rules grid appears with ✏ in the Enabled column for each enabled rule.
8. Click Activate Rules in the Rules toolbar to activate the rule.
   The rule is enabled.

Testing rules in LEM

Before you put a rule into production, try it out in test mode. In test mode, the LEM Manager processes the rule alert messages, but does not execute any rule actions. This lets you see how the activated rule will behave without disrupting your network.

When selecting two or more rules at the same time to test, select rules that are in the same state—Test On or Test Off. See About selecting multiple rules to test, enable, or disable for more information.
Enable test mode in the Rules grid

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, maximize the category that contains the rule you want to test.
4. Ensure that your selected rule has an Enabled 📝 icon in the Enabled column.
   If the rule displays a disabled 📝 icon, enable the rule by clicking 📝, and then selecting Enable.
5. To place a single rule in test mode, click 📝, and then select Test On/Test Off. To place multiple selected rules in test mode, click 📝, and then select Test On/Test Off.
   In the Rules grid, the 📝 icon displays in the Test column for each rule in test mode.
6. Click Activate Rules.
   The rules are now functional, but in test mode.

Disable test mode in the Rules grid

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, maximize the category that contains the rule you want to test.
4. In the Rules grid, select the rule (or rules) you want to work with.
5. To disable test mode in a single rule, click 📝, and then select Test On/Test Off. To disable test mode on multiple selected rules, click 📝, and select Test On/Test Off.
   In the Rules grid, the disabled 📝 icon appears in the Test column to indicate the rule is no longer in test mode.
6. Click Activate Rules.
   The rules are now fully functional.

Enable test mode from the Rule Creation screen

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, maximize the category that contains the rule you want to test.
4. In the Rules grid, click to select the rule you want to test.
5. In the Rules grid toolbar, click Edit.
   Rule Creation displays, showing the current rule configuration.
6. Select the Enable check box.
7. Select the Test check box.
To test a rule, the Enable and Test check boxes must be selected. If only Enable is checked, the rule is enabled and ready for use. If only Test is checked, the rule will not be enabled, and the LEM Manager will not be able to use it for testing.

8. Click Save.

   The rule is now in test mode.

Disable test mode from the Rule Creation screen

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, maximize the category that contains the rule you want to test.
4. In the Rules grid, click to select the rule you want to test.
5. In the Rules grid toolbar, click Edit.
   Rule Creation displays, showing the current rule configuration.
6. Clear the Test check box.
7. Click Save.
8. In the Rules toolbar, click Activate Rules.
   The rule is now fully functional and no longer in test mode.

Disable rules in LEM to stop them from processing

The LEM Manager continues to use active rules if they are enabled. Turn off rules by disabling them and clicking the Activate Rules command. Note that the Manager will continue to use disabled rules until you confirm their disabled state with the Activate Rules command.

When selecting two or more rules at the same time to disable, select rules that are in the same state—Enabled or Disabled. See About selecting multiple rules to test, enable, or disable for more information.

Disable rules from the Rules grid

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, maximize the category that contains the rules you want to disable.
4. In the Rules grid, select the rule (or rules) you want to disable.
5. To disable a single rule, click ✗ next to the rule, and then select Disable.
   To disable multiple rules, click ☑ in the Rules toolbar, and then select Disable.
6. The Disabled 📨 icons for each selected rule become active, indicating the rules are now inactive.

7. Click Activate Rules.

The Manager stops processing the disabled rules.

Disable rules from the Rule Creation screen

1. Open the rule you want to disable in Rule Creation.
2. Clear the Enable check box.
3. Click Save.

The Manager stops processing the disabled rule.

**Use the Send Email Message action in LEM rule creation**

Use the Send Email Message action to create a rule. Before you add an action, perform the following steps:

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Refine Results search field, enter user account lockout.
4. In the Rule Templates grid, locate the User Account Lockout template.
5. Next to the template, click 🌟, and then select Clone.
6. Edit the rule Correlations as required, and then click Save.

**Add or edit a Send Email Message action**

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. To create a new rule, click ⌃ in the Rules toolbar.
4. Expand the Actions list.
5. Drag Send Email Message into the Actions box.

If you make a mistake, or decide you want to clear out the actions and start over, hover over any action and click X or click Undo.

6. From the Email Template drop-down list, select your template.

If you forgot the name, you can always go back to Build > Groups to view your template details.

Your rule will still be open when you come back to Build > Rules.

7. From the Recipients drop-down list, select the users who need to be notified about this event.
8. Populate the Send Email Message action with dynamic values from the event firing the rule.
   a. Locate the Event or Event Group that contains your desired action. In this example, the User Account Lockout (Updated) Rule uses the UserDisable event. Expand Events on the components pane and type UserDisable in the search box.
   b. Click the Event to populate its available fields in the Fields listing under the Events listing.
   c. From the Fields listing, drag the appropriate fields into the Correlations box.
      For example, the Email Template created in the related articles below require the following fields: DetectionTime for the Time variable, SourceMachine for the Machine variable, DestinationMachine for the DC variable, and DestinationAccount for the Account variable.

9. Select the Enable check box.

   ! After you enable the rule, you can also use the Test check box to place your rule in Test Mode. When a test rule fires, InternalTestRule events display in the console to verify the trigger and actions, but no action is taken.

10. To save your changes, click Save.
    Activate Rules is enabled in the Rule Creation toolbar. This allows you to batch up all your rule changes in case you want to make multiple changes before changing the running state of the Manager.

11. Click Activate Rules to send your changes to the LEM Manager and enable your changes.
    Your rule is active and your template is set up.
    The next time your rule fires, the recipients specified in your rule will receive an email that matches your specified format.

**Notify a LEM user when a rule triggers an alert (Subscribe a user to a rule)**

You can assign rules to specific console users by adding them as a subscriber. The system will notify each subscriber when the subscribed rule triggers an alert. These alerts display in the Monitor view for each subscriber.

You can use rule subscriptions in conjunction with filters and reports to monitor activity for specific rules. Each user can subscribe to as many different rules as required. You can also assign subscriptions when you are creating the rule or from the Rules grid at a later time.

**Subscribe users from the Rules grid**

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. In the Rule Categories and Tags pane, maximize the category that contains your targeted rule.
4. In the Rules grid, select the targeted rule.

5. In the Rules grid toolbar, click the Subscribe drop-down list.
   This list contains console users who are associated with the same LEM Manager as the selected rule. A check box with a gray background indicates the user is subscribed to one or more of the selected rules, but not all rules.

6. Select one or more users to subscribe to the rule.
   - Select a clear check box to subscribe the user to all selected rules.
   - Clear a gray check box to remove the user subscription to all selected rules.

7. To close the list, click Subscribe again.
   The selected console users are subscribed to the selected rules.

**Subscribe users from the Rule Creation screen**

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Build > Rules.

3. In the Rule Categories and Tags pane, maximize the category that contains your targeted rule.

4. In the Rules grid, select the targeted rule.

5. Next to the rule, click ⚙, and then select Edit.

6. On the Rule Creation screen, click the Subscribe drop-down list.
   This menu contains console users who are associated with the same LEM Manager as the selected rule. A check box with a gray background indicates the user is subscribed to one or more of the selected rules, but not all rules.

7. Select the check box for each console user who is to subscribe to this rule. Clear the check box for each subscriber who is no longer to subscribe to this rule.

8. To close the list, click Subscribe.

9. Click Save.
   The selected console users are subscribed to the rule.
LEM response actions: Respond to network and system events in LEM

About LEM response actions

See Create a new LEM rule to monitor and respond to events to learn how to create an active response rule.

About LEM active response

An active response (also called an event response) in LEM is an action that LEM takes in response to suspicious activity or an attack. Active response actions include the Block IP active response, the Disable Networking active response, the Log off User active response, the Kill Process active response, the Detach USB Device active response, and so on.

The Respond drop-down menu in Monitor view provides a list of actions you can execute for a specific event message. Each Respond command opens the Respond form. This form includes data from the field you selected and options for customizing the action—similar to configuring the active response for a rule in the Rule Creation.

The Respond menu is context-sensitive. The event type or cell currently selected in the event grid determines which responses you can choose.

Select an event response

In the Respond form, you can use the default field information to complete the form.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor, select an event in the event grid, and then click Pause.
3. Click Respond, and then select an action.

   The drop-down menu contains a list of commonly-used actions. If your action does not appear in the list, select All Actions.

4. In the Respond form, click the Action drop-down list, and then verify the action to your selected event.
5. Complete any remaining fields in the form.
6. To execute the action, click OK.
7. To receive new events in the event grid, click Resume.

Select an event response using drag-and-drop text

In the Respond form, drag and drop information from the Event and Information fields into the configuration fields to complete the form. Use this method to add content to a blank configuration field or replace the content of an existing configuration field.

1. On the LEM toolbar, click Monitor, select an event in the event grid, and then click Pause.
2. Click Respond, and then select an action.

   The drop-down menu contains a list of commonly-used actions. If your action does not appear in the list, select All Actions.

3. In the Respond form, click the Action drop-down list, and then verify the action to your selected event.

4. In the Respond form's event information grid, scroll to locate the field that contains the data element needed to configure the action.
5. Drag an event field into the appropriate action configuration field.
6. Complete any remaining fields as required.
7. To execute the action, click OK.
8. To receive new events in the event grid, click Resume.

Use LEM active responses to perform Windows actions related to users, groups, and domains

Use the following user-based active responses to perform Windows-based actions related to users, groups, and domains on your LEM Agents.

- Add Domain User To Group
- Add Local User To Group
- Create User Account
- Create User Group
- Delete User Account
- Delete User Group
- Disable Domain User Account
- Disable Local User Account
- Enable Domain User Account
- Enable Local User Account
- Log Off User
- Remove Domain User From Group
- Remove Local User From Group
- Reset User Account Password
These actions are useful to respond to unauthorized change management activity and to automate user-related maintenance. They can be automated in a LEM rule, or executed manually from the Respond menu in the LEM console.

**Configure an active response connector on a LEM Agent**

Configure the Windows active response connector on each LEM Agent that requires active responses.

You can deploy your LEM Agents and configure the Windows active response connector based on where you want to perform these actions. To perform actions at the domain level, deploy a LEM Agent to at least one domain controller. To perform actions at the local level, deploy a LEM Agent to each computer that requires a response.

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
   
   Log in as an administrator.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Locate the Agent in the Nodes grid that requires a connector.
4. Next to the Agent, click ![Connector Icon](#) and then select Connectors.
5. In the search box at the top of the Refine Results pane, enter *Windows Active Response*.
6. Next to the connector, click ![New Icon](#) and then select New.
7. Enter a custom alias for the new connector, or accept the default.
8. Click Save.
9. Next to the new connector, click ![Start Icon](#) and then select Start.
10. To exit the Connector Configuration window, click Close.

**Actions LEM can take to respond to events**

The following table lists the various actions a LEM Manager can take to respond to events. These actions are configured in the Respond form when you are initiating an active response, and in the rules window's Actions box when you are configuring a rule's automatic response.

The table's Action column lists the actions that are available. They are alphabetized for easy reference. The Description column briefly states how the action behaves. The Fields column lists the primary data fields that apply with each action. Some data fields will vary, depending on the options you select.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Fields</th>
</tr>
</thead>
</table>
| Add Domain User To Group | This action adds a domain user to a specified user group that resides on a particular Agent. | Domain Controller Agent  
Select the event field or constant that defines the Agent on which the group to be modified resides.  
To modify a group at the domain level, specify a domain controller as the Agent.  
Group Name  
Select the event field or constant that defines the group that is to be modified.  
Username  
Select the event field or constant that defines the user who is to be added to the group. |
| Add Local User To Group | This action adds a local user to a specified user group that resides on a particular Agent. | Agent  
Select the event field or constant that defines the Agent on which the group to be modified resides.  
To modify a group at the domain level, specify a domain controller as the Agent.  
Group Name  
Select the event field or constant that defines the group that is to be modified.  
Username  
Select the event field or constant that defines the user who is to be added to the group. |
| Add User-Defined Group Element | This action adds a new data element to a particular user-defined group. | User-Defined Group Element  
From the User-Defined Groups list, select the User-Defined Group that is to receive the new data element.  
Value  
Select the event field or constant that defines the data element that is to be added to the specified User-Defined Group. The fields will vary according to which User-Defined Group you select. |
<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
<th>FIELDS</th>
</tr>
</thead>
</table>
| Append Text To File | This action appends text to a file. This allows you to data from an event and put it in a text file. | Agent - Select the event field or constant that defines the Agent on which the file to be appended is located.  
File Path - Select the event field or constant that defines the path to the Agent file that is to be appended with text.  
Text - Select the event field or constant that defines the text to be appended to file. |
| Block IP            | This action blocks an IP address.                                            | IP Address - Select the event field or constant that identifies the device's IP address. |
| Create User Account | This action creates a new user account on an Agent.                         | Agent - Select the event field or constant that defines the Agent on which the new user account is to be added.  
To create a user account at the domain level, specify a domain controller as the Agent.  
Account Name - Select the event field or constant that names the account that is to be created.  
Account Password - Select the event field or constant that defines the password that is to be assigned to the new account. |
| Create User Group   | This action creates a specified user group on an Agent.                      | Agent - Select the event field or constant that defines the Agent on which the new user group is to reside.  
To create a user group at the domain level, specify a domain controller as the Agent.  
Group Name - Select the event field or constant that defines which user group is to be created. |
<table>
<thead>
<tr>
<th><strong>ACTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
<th><strong>FIELDS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete User Account</td>
<td>This action deletes a user account from an Agent.</td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the Agent on which the user account is to be deleted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete a user account at the domain level, specify a domain controller as the Agent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Account Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that names the account that is to be deleted.</td>
</tr>
<tr>
<td>Delete User Group</td>
<td>This action deletes a user group from a particular Agent.</td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the Agent on which the user group to be deleted resides.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete a user group at the domain level, specify a domain controller as the Agent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the user group that is to be deleted.</td>
</tr>
<tr>
<td>Detach USB Device</td>
<td>This action detaches a USB mass storage device that is connected to an Agent.</td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the Agent from which the USB device is to be detached.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the device ID of the USB device that is to be detached.</td>
</tr>
<tr>
<td>Disable Domain User Account</td>
<td>This action disables a Domain User Account on a Domain Controller Agent.</td>
<td>Domain Controller Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the Domain Controller Agent on which the domain user is to be disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Account</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the account that is to be disabled.</td>
</tr>
<tr>
<td><strong>ACTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
<td><strong>FIELDS</strong></td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable Local User Account</td>
<td>This action disables a local user account on an Agent.</td>
<td>Agent&lt;br&gt;Agent&lt;br&gt;Select the event field or constant that defines the Agent on which the local user is to be disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Account&lt;br&gt;Select the event field or constant that defines the account that is to be disabled.</td>
</tr>
<tr>
<td>Disable Networking</td>
<td>This action disables an Agent's network access.</td>
<td>Agent&lt;br&gt;Agent&lt;br&gt;Select the event field or constant that defines the Agent that is to be disabled from the network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Message&lt;br&gt;Type the message that is to appear on the Agent.</td>
</tr>
<tr>
<td>Disable Windows Machine Account</td>
<td>This action disables a Windows machine account that resides on a Domain Controller Agent.</td>
<td>Domain Controller Agent&lt;br&gt;Select the event field or constant that defines the Domain Controller Agent on which the account is to be disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Account&lt;br&gt;Select the event field or constant that specifies which Windows account is to be disabled.</td>
</tr>
<tr>
<td>Enable Domain User Account</td>
<td>This action enables a Domain User Account on a Domain Controller Agent.</td>
<td>Domain Controller Agent&lt;br&gt;Select the event field or constant that defines the Domain Controller Agent on which the domain user is to be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Account&lt;br&gt;Select the event field or constant that defines the account that is to be enabled.</td>
</tr>
<tr>
<td>Enable Local User Account</td>
<td>This action enables a local user account on an Agent.</td>
<td>Agent&lt;br&gt;Select the event field or constant that defines the Agent on which the local user is to be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Account&lt;br&gt;Select the event field or constant that defines the account that is to be enabled.</td>
</tr>
<tr>
<td>ACTION</td>
<td>DESCRIPTION</td>
<td>FIELDS</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Windows Machine Account</td>
<td>This action enables a Windows machine account that resides on a Domain Controller Agent.</td>
<td>Domain Controller Agent&lt;br&gt;Select the event field or constant that defines the Domain Controller Agent on which the account is to be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Account&lt;br&gt;Select the event field or constant that specifies which Windows account is to be enabled.</td>
</tr>
<tr>
<td>Incident Event</td>
<td>This action escalates potential issues by creating an Incident Event.</td>
<td>Event&lt;br&gt;Select which Incident Event the rule is to create.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Fields&lt;br&gt;From the list pane, select the events and constants that define the appropriate data elements for each event field. The fields vary, depending on which Incident Event is selected.</td>
</tr>
<tr>
<td>Infer Event</td>
<td>This action escalates potentially irregular audit traffic into security events by creating (or inferring) a new event with a higher severity.</td>
<td>Event&lt;br&gt;Select which Event the rule is to infer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Fields&lt;br&gt;From the list pane, select the events and constants that define the appropriate data elements for each event field. The fields vary, depending on the which event is selected.</td>
</tr>
<tr>
<td>Kill Process by ID</td>
<td>This action terminates the specified process on an Agent by using its process ID value.</td>
<td>Agent&lt;br&gt;Select the event field or constant that defines the Agent on which the process is to be terminated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process ID&lt;br&gt;Select the event field or constant that identifies the ID number of the process that is to be terminated.</td>
</tr>
<tr>
<td><strong>ACTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
<td><strong>FIELDS</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Kill Process by Name| This action terminates the specified process on an Agent by referring to the process name. | Agent  
Select the event field or constant that defines the Agent on which the process is to be terminated.  
Process Name  
Select the event field or constant that identifies the name of the process that is to be terminated.  
Account Name  
Select the event field or constant that identifies the name of the account that is running the process to be terminated. |
| Log Off User        | This action logs the user off of an Agent.                                      | Agent  
Select the event field or constant that defines the Agent from which the user is to be logged off.  
Account Name  
Select the event field or constant that identifies the specific account name that is to be logged off. |
| Modify State Variable| This action modifies a state variable.                                          | State Variable  
From the State Variables list, drag the state variable that the rule is to modify.  
State Variable Fields  
From the appropriate component list, type or drag the data element that is to be modified in the state variable. The fields vary, depending on the which state variable is selected. |
| Remove Domain User From Group| This action removes a domain user from a specified user group that resides on a particular Agent. | Domain Controller Agent  
Select the event field or constant that defines the domain controller Agent on which the group to be modified resides.  
Group Name  
Select the event field or constant that defines the group that is to be modified.  
User Name  
Select the event field or constant that defines the user who is to be removed from the group. |
<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
<th>FIELDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Local User From Group</td>
<td>This action removes a local user from a specified user group that resides on a particular Agent.</td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the Agent on which the group to be modified resides.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the group that is to be modified.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the user who is to be removed from the group.</td>
</tr>
<tr>
<td>Remove User-Defined Group Element</td>
<td>This action removes a data element from a particular user-defined group.</td>
<td>User-Defined Group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>From the User-Defined Groups list, select the user-defined group from which the specified data element is to be removed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the data element that is to be removed from the specified user-defined group. The fields will vary according to which user-defined group you select.</td>
</tr>
<tr>
<td>Reset User Account Password</td>
<td>This action resets a user account password on a particular Agent.</td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that identifies the Agent on which the user password is to be reset.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To reset an account at the domain level, specify a domain controller as the Agent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Account Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that identifies the user account that is to be reset.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New Password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the user's new password.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td><strong>Description</strong></td>
<td><strong>Fields</strong></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Restart Machine</td>
<td>This action reboots an Agent.</td>
<td>Agent Select the event field or constant that identifies the Agent that is to be rebooted. Delay (sec) Type the time (in seconds) after the event occurs that the Manager is to wait before rebooting the Agent.</td>
</tr>
<tr>
<td>Restart Windows Service</td>
<td>This action restarts the specified Windows service on an Agent.</td>
<td>Agent Select the event field or constant that identifies the Agent on which the Windows service will be restarted. Service Name Select the event field or constant that identifies the name of the service that is to be restarted.</td>
</tr>
<tr>
<td>Send Email Message</td>
<td>This action sends a preconfigured email message to a predetermined email distribution list.</td>
<td>Email Template Select the template that the email message is to use. Recipients Click the check boxes to select which users are to receive the email message. Email Fields Either drag a field from the components list, or select a constant from the components list to select the appropriate data elements that are to appear in each email template field. The fields vary, depending on which email template is selected.</td>
</tr>
<tr>
<td>Send Popup Message</td>
<td>This action displays a pop-up message to an Agent.</td>
<td>Agent Select the event field or constant that identifies the Agent that is to receive the pop-up message. Account Name Select the event field or constant that identifies the user account to receive the message. Message Select the event field or constant that defines the message that is to appear on the Agent's monitor.</td>
</tr>
</tbody>
</table>
### Action Description Fields

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown Machine</td>
<td>This action shuts down an Agent.</td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that identifies the Agent that is to be shut down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delay (sec)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type the time (in seconds) after the event occurs that the Manager is to wait before shutting down the Agent.</td>
</tr>
<tr>
<td>Start Windows Service</td>
<td>This action starts the specified Windows service on an Agent.</td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that identifies the Agent on which the Windows service is to be started.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the Windows service that is to be started.</td>
</tr>
<tr>
<td>Stop Windows Service</td>
<td>This action stops the specified Windows service on an Agent.</td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that identifies the Agent on which the Windows service is to be stopped.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the event field or constant that defines the Windows service that is to be stopped.</td>
</tr>
</tbody>
</table>

### Use Computer-based active responses in LEM

To perform Windows-based actions related to computers and computer services on your LEM Agents, use the following Computer-based active responses. These actions are useful to respond to insider abuse, computer infections, and other suspicious activity. They can be automated in a LEM rule, or executed manually from the Respond menu in the LEM console.

- Disable Windows Machine Account1
- Enable Windows Machine Account1
- Disable Networking
- Detach USB Device
- Restart Machine
- Restart Windows Service
- Send Popup Message
- Shutdown Machine
- Start Windows Service
- Stop Windows Service
Requirements

Configure the Windows Active Response connector on each LEM Agent on which you want to be able to use these active responses.

Deploy your LEM Agents and configure the Windows Active Response connector based on where you want to perform these actions. To perform actions at the domain level, deploy a LEM Agent to at least one domain controller. To perform actions at the local level, deploy a LEM Agent to each computer you want to be able to respond to.

To configure the Windows active response connector on a LEM Agent

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Locate the LEM Agent on which you want to enable the connector.
4. To the left of the LEM Agent, click , and then select Connectors.
5. Enter Windows Active Response in the Search box at the top of the Refine Results pane.
6. Next to the connector, click , and then select New.
7. Enter a custom Alias for the new connector, or accept the default.
8. Click Save.
9. Next to the new connector, denoted by an icon in the Status column, Click , and then select Start.
10. To exit the Connector Configuration window, click Close.

Create or clone rules to perform the action:

1. When creating or cloning a rule, locate the action in the lower left part of the Rule Creation screen.
2. Drag the action under the rule Actions.
3. Fill in the appropriate fields.

Use the Append Text to File active response in LEM

Use the Append Text To File active response to append static or dynamic text to a flat text file on your network. This action is useful for keeping a running list of deployed LEM Agents or tracking certain types of activity across several users and computers. You can automate this response with a LEM rule, or execute it manually from the Respond menu in the LEM console.

Requirements

To use this active response, ensure that the file you want to append already exists. Follow these guidelines when creating the file:
Use a .txt file, or a similar flat-text file format.

- Avoid using spaces in the file path or name.
- Note the complete file path and name, because you will need it to configure the active response.

Configure the Append Text to File active response and Windows active response connectors on each LEM Agent on which you want to be able to use this active response.

To configure the Append Text to File action in a rule:

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. Create a new rule or edit an existing rule that triggers on a specific event.
4. Open the rule to edit, and then select Actions in the left pane.
5. Drag the Append Text to File action from the left to the Actions box under the rule.
6. In the left pane, click Constants, and then drag the Text field to the empty box next to File Path under the Append Text to File action.
7. Using the same event stated in the Correlations, select the event from the Events list on the left and drag the DetectionIP field from the Fields list to the Agent under this action.
8. Fill in the directory structure in the File Path under this action, indicating the name of the file.
9. The Text field under the Append Text to File label will contain the text that you are inserting into the file. If using plain text, drag the Text constant from the left to the empty box in the Text field.
10. Save the rule.

To configure the Append Text to File Active Response connector on a LEM Agent:

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Locate the LEM Agent on which you want to enable the connector.
4. To the left of the LEM Agent, click Ⓡ, and then select Connectors.
5. In the search box at the top of the Refine Results pane, enter Append Text to File.
6. Next to the connector, click Ⓡ, and then select New.
7. Enter a custom Alias for the new connector, or accept the default.
8. Specify whether you want the connector to append data to a new line in the How to append menu.
9. Specify a Maximum file size(MB) or accept the default.
10. Click Save.
11. Next to the new connector, denoted by an icon in the Status column, click Ⓡ, and then select Start.
12. To exit the Connector Configuration window, click Close.
To configure the Windows active response connector on a LEM Agent:

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Locate the LEM Agent on which you want to enable the connector.
4. To the left of the LEM Agent, click  and then select Connectors.
5. In the Search box at the top of the Refine Results pane, enter Windows Active Response.
6. Next to the connector, click  and then select New.
7. Enter a custom Alias for the new connector, or accept the default.
8. Click Save.
9. Next to the new connector, denoted by an icon in the Status column, click  and then select Start.
10. To exit the Connector Configuration window, click Close.

Auto-populate user-defined groups using a LEM rule

You can automate how you populate User-Defined Groups using the Add User-Defined Group Element active response in a LEM rule. This active response populates a pre-defined user-defined group with static or dynamic values, as defined by that rule.

Complete the following task to populate a user-defined group based on a specific type of event, such as when you attach a USB device you want to tag as authorized, or when a user attempts to visit a prohibited website.

For additional information about working with LEM rules, see About LEM rules.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. To create a new rule, click  in the Rules toolbar.
4. Enter a name and description for your rule.
5. Populate the Correlations box with conditions that represent the event you want to trigger your rule. For the USB example:
   a. In the components pane on the left, click Events, and then enter SystemStatus without any spaces in the search box.
   b. Click SystemStatus, and then locate EventInfo from the Fields: SystemStatus list.
   c. Drag EventInfo into the Correlations box. The left side of your new condition should read, SystemStatus.EventInfo.
   d. Enter *Attached* into the Text Constant field, denoted by the pencil icon, on the left side of your new condition.
e. To specify a computer for this procedure, create a second condition with
   
   ```systemstatus.detectionIP = *computerName*, where computerName is the
   hostname of the computer you want to specify.```

   In this example, the computer you attach your authorized devices to must have a LEM
   Agent with USB Defender installed, whether you specify it in your rule or not.

6. In the components pane, click Actions, and then locate Add User-Defined Group Element.
7. Drag Add User-Defined Group Element into the Actions box.
8. Within the Add User-Defined Group Element, select the appropriate User-Defined Group, such as
   Authorized USB Devices. If you do not find the User-Defined Group, perform the following:
   a. Close the action and navigate to Build > Groups.
   b. To create your own User-Defined Group, or to clone an existing group, click [+ on the upper
      right.
9. Populate the action using the alerts present in your Correlations. For the USB example:
   a. Select Authorized USB Devices from the User Defined Group menu.
   b. Click Alerts on the components pane, and then verify that SystemStatus is still selected.
   c. Drag ExtraneousInfo from the Fields: SystemStatus list into the blank Value field in the action.
10. Select Enable at the top of the Rule Creation window, and then modify the Test and Subscribe
    settings if you want.

    Putting a rule into Test allows the rule to function as needed, but the rule will not perform any of the
    actions listed. In this example, it will not add any information to the User-Defined Group.
11. At the bottom of the Rule Creation window, click Save.
12. At the top of the main Rules view, click Activate Rules.

Any time the event you defined in your rule occurs, the value you defined in the Value field of the action
gets added to the user-defined group you specified. In the USB example, the attached device is added to
the Authorized USB Devices group.

**Use the Block IP active response in LEM**

Use the Block IP active response to block an IP address at your firewall using your LEM Manager. This
action is useful for blocking port scanners, and can be automated in a LEM rule, or executed manually
from the Respond menu in the LEM console.

**Requirements**

You can use the Block IP active response with the following firewalls/modules.

- Cisco PIX
- Cisco ASA
- Cisco Firewall Services Module
Configure the Active Response tool for one of the firewalls listed above on your LEM Manager.

To configure the Active Response connector for your firewall:

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. To the left of the LEM Manager, click ⚙, and then select Connectors.
4. From the Category list, select Firewalls, and then enter Active Response in the search box at the top of the Refine Results pane.
5. Next to the connector for your firewall, click ⚙, and then select New.
6. Complete the Connector Configuration form according to your firewall's specifications.
7. Click Save.
8. Next to the new connector, denoted by an icon in the Status column, click ⚙, and then select Start.
9. To exit the Connector Configuration window, click Close.

To configure the Rule:

1. Identify the type of data that would trigger the rule. If needed, perform an nDepth search or view the real-time data being received under Monitor in the Console (filters).
2. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
3. On the LEM toolbar, navigate to Build > Rules.
4. To create a new rule, click + in the upper-right corner, and then enter a descriptive name.
5. Locate the event type in the Events tab, the desired fields from the Field tab, and then drag to the Correlations box.
6. Click the Actions tab on the left, and then drag Block IP to the Actions box under the rule being created.
7. Enter the IP address to be blocked, and then save the rule.
8. Click Activate Rules.

Additional Information

The Block IP active response creates a rule on your firewall to block the IP addresses you specify. To allow an IP address through your firewall, delete or modify the rule on your firewall as appropriate.
Configure the Detach USB Device active response in LEM

Use the Windows active response to detach a USB device from a LEM Agent running USB Defender. This action is useful for allowing only specific devices to be attached to your Windows computers or detaching any device exhibiting suspicious behavior, and can be automated in a LEM rule, or executed manually from the Respond menu on the Manage > Nodes page.

USB Defender is an option when the Agent is originally installed. If not installed at the time of Agent install, re-install the Agent with USB Defender. Additionally, configure the Windows Active Response tool on each LEM Agent where you require an active response.

Verify that USB Defender is installed on a LEM Agent

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. If you have a long list of nodes, filter your list using the Node, OS, or USB drop-down menus.
   - You can install USB Defender only on Windows Agents.
4. Locate 📱 in the USB column, indicating that USB Defender is installed on the node.
5. If USB Defender is not installed on one or more LEM Agents, reinstall the Agent and ensure that you select Install USB-Defender after you confirm the Manager Communication Settings.

Configure the Windows Active Response connector on a LEM Agent

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Locate the LEM Agent that requires a new connector.
4. Next to the Agent, click 📷, and then select Connectors.
5. In the Refine Results search box, enter Windows Active Response.
6. Next to the connector, click 📷, and then select New.
7. Enter a custom alias name for the new connector, or accept the default.
8. Click Save.
9. Next to the new connector, click 📷, and then select Start.
10. To exit the Connector Configuration window, click Close.
Detach USB devices

By default, USB devices are audited and the USB File Audit Activity filter will display those events. The filter is set for `FileAuditAlerts.ProviderSID=*USB*` To monitor all USB device activity, create a filter for `AnyAlert.ProviderSID=*USB*`

USB devices are not detached by default. You must configure a rule to detach the device. The Templates grid includes several templates you can clone and modify as needed.

You can enforce USB Defender policy locally. See Configure the USB Defender local policy connector in LEM for details.

Configure the Disable Networking active response in LEM

Use the Disable Networking Active Response to disable networking on a LEM Agent at the Windows Device Manager level. Use this active response for isolating network infections and attacks. You can automate the active response in a LEM rule or manually execute the response from the Respond menu in the LEM console.

Use caution with this active response, because it responds to the LEM Agent at the Device Manager level. To avoid disabling networking unintentionally, consider placing new rules with this action in Test mode until you are sure your correlations are configured appropriately.

Configure the Windows Active Response connector on each LEM Agent where you need a Disable Networking active response.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Locate the LEM Agent that requires a new connector.
4. Next to the Agent, click Edit, and then select Connectors.
5. In the Refine Results search box, enter Windows Active Response.
6. Next to the connector, click Edit, and then select New.
7. Enter a custom alias name for the new connector, or accept the default.
8. Click Save.
9. Next to the new connector, click Edit, and then select Start.
10. To exit the Connector Configuration window, click Close.

Re-enable networking on a computer affected by the active response

1. Log in to the computer locally with administrative privileges.
2. Open Control Panel, and then navigate to System and Security > Administrative Tools > Computer Management.
4. Expand the Network adapters group.
5. Select the network adapter, and then click Action > Enable.

**Configure the Kill Process active response in LEM**

Use the Kill Process active response to end Windows-based processes in your LEM Agents. This response helps to stop suspicious or unauthorized processes. You can automate the response using a LEM rule or manually execute the response from the Respond menu in the LEM console.

Configure the Windows Active Response connector on a LEM Agent where you need an active response.

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Locate the LEM Agent that requires a new connector.
4. Next to the Agent, click ![Connectors](#), and then select Connectors.
5. In the Refine Results search box, enter Windows Active Response.
6. Next to the connector, click ![New](#), and then select New.
7. Enter a custom alias name for the new connector, or accept the default.
8. Click Save.
9. Next to the new connector, click ![Start](#), and then select Start.
10. To exit the Connector Configuration window, click Close.

**Configure a Kill Process active response rule**

You can configure the rule a process by the detection IP address or the process name. Determine the type of event that trigger the rule, which is typically an event like ProcessAudit.

The Kill Process active response functions according to the ProcessID field value of the corresponding LEM alert. Use Kill Process By ID when the ProcessID value is a number, and use Kill Process By Name when the ProcessID value is a name.

When you create LEM rules that utilize these actions, consider using both to account for variations in Windows logging.

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. To create a new rule, select a rule template or an existing rule, or click ![new](#) in the toolbar.
4. Enter a name and description for the rule.

   ![Kill Process](image)

   **Kill Process**

   - **Name:** Kill Process
   - **Description:** Active response rule
   - **Rule Status:** Errors (3)

5. To kill a process by the detection IP address:
   a. In the left pane, click Events, and then select ProcessAudit.
   b. In the Fields: ProcessAudit list, drag DetectionIP into the Correlations box.

   ![Rule Creation](image)

   - In the Fields: ProcessAudit list, drag SourceAccount into the Correlations box.

   To kill a process by name:
   a. In the left pane, click Events, and then select ProcessAudit.
   b. In the Fields: ProcessAudit list, drag DetectionIP into the Correlations box.
   c. In the Fields: ProcessAudit list, drag SourceAccount into the Correlations box.

6. In the left pane, click Actions, and then drag Kill Process By ID or Kill Process By Name into the the Actions box.

7. Click Save.

8. Click Activate Rules.
Building custom filter and rule expressions in LEM

Comparing values with operators in LEM filters and rules

This section documents how to use operators to create custom filter and rule expressions in LEM.

About operators in LEM

When configuring a LEM rule or a filter, if you drag an item from the list pane and position it next to an event variable, an operator icon appears between them. The operator states how the event variable must compare with the other item to be subject to the rule's or filter's conditions. For example, an operator might state that an event must be contained within a Time of Day Set, or it may state that an event only applies to a particular Connector Profile.

There are two types of operators: Condition and Group.

- Condition operators are found between your events and their values. Examples include Equals, Does Not Equal, Contains, and Does Not Contain. Rule Creation only displays the operators that are available for the values in your Correlations.
- Group operators are found outside of your correlation groups. The two options are And (blue) and Or (orange).

The operators that appear between two elements vary depending on your selections. The creation form only allows comparisons that are logical for the specified elements.

Select a new operator

There are two ways to select an operator for a condition:

- To open a menu of valid operators, Ctrl+click the operator, and then click the operator that you want to use.
- Click the operator to cycle through the options that are valid for the current condition.

Operator tips

The following tips apply to operators:

- When comparing two numeric values, the full range of mathematical operator options is available.
- An IP address is treated as a string (or text) value. Therefore, operators are limited to equal and not equal.
- DateTime fields have a default value of > Time Now, which means, greater than the current date and time.
# Table of operators

The following table describes each operator and how it should be interpreted when used as a filter condition.

A list item (indicated with an * in the following table) can be another event variable, such as an event field. For example, you may want to evaluate if an event's source is equal to a certain destination. In this case, you would compare two event fields, such as `SourceMachine = DestinationMachine`.

<table>
<thead>
<tr>
<th>OPERATOR</th>
<th>MEANING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Exists</td>
<td>Use these operators to specify if a particular event or Event Group exists. Read conditions with these operators as follows: This [event/Event Group] must [exist/not exist].</td>
</tr>
<tr>
<td>✗</td>
<td>Not exist</td>
<td>Not exist is only used in rules.</td>
</tr>
<tr>
<td>📦</td>
<td>is in</td>
<td>Use these operators when comparing event fields with groups (such as Event Groups, User-Defined Groups, etc.). They determine the filter's behavior, based on whether or the field is contained a specific Group.</td>
</tr>
<tr>
<td>🧵</td>
<td>is not in</td>
<td>Read conditions with these operators as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• This [event field] must be in this [Group].</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• This [event field] must not be in this [Group].</td>
</tr>
<tr>
<td>=</td>
<td>Equals</td>
<td>Read conditions with these operators as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• This [event variable] must equal this [list item*].</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• This [event variable] must not equal this [list item*].</td>
</tr>
<tr>
<td>≠</td>
<td>Does not equal</td>
<td>Text comparisons (for IP addresses, host names, etc.) are limited to equal or not equal operators.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than</td>
<td>Read conditions with these operators as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• This [event variable] must be greater than this [list item*].</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• This [event variable] must be greater than or equal to this [list item*].</td>
</tr>
<tr>
<td>≥</td>
<td>Greater than OR equal to</td>
<td></td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than</td>
<td></td>
</tr>
<tr>
<td>≤</td>
<td>Less than OR equal to</td>
<td></td>
</tr>
</tbody>
</table>
**OPERATOR** | **MEANING** | **DESCRIPTION**
---|---|---
AND | Conditions and groups of conditions are subject to AND and OR comparisons.  
- The AND symbol means two or more conditions (or groups) must occur together for the filter to apply. This is the default comparison for new groups.  
- The OR symbol means any one of several conditions (or groups) may occur for the filter to apply. When comparing groups of distinct events, you must use the OR symbol.

OR | If you click an AND operator, it changes to an OR, and vice versa.

**Examples of AND and OR conditions**

Filter groups and conditions, and rule groups and correlations, are all subject to AND and OR conditions. By default, new groups, conditions, and correlations appear with an AND condition. Both AND and OR conditions can surround nested groups, and they can be used between groups on the same level to create complex filter conditions or rule correlations.

**EXAMPLE** | **DESCRIPTION**
---|---
If x AND y AND z occur, report the event. | If all the conditions apply, report the event.
If x OR y OR z occurs, report the event. | If any of the conditions apply, report the event.
If (x AND y) OR z occurs, report the event. | If conditions x and y occur, or if condition z occurs, report the event.
If (a AND b) OR (x AND y) OR (z), occurs, report the event. | In this case, you would create three groups, two nested within the third:  
- The nested groups are configured as (a AND b) and (x AND y), joined with an OR.  
- The outer group is configured as (z), surrounding the nested groups with an OR.
Condition1 AND Condition2 AND Condition3 OR Condition4 AND Condition5. | In this example, the filter reports the event when it meets the following conditions: Condition1 and Condition2 and Condition3, or Condition1 and Condition4 and Condition5.

**Get started building custom filter expressions in LEM**

This section provides information to help you write custom filter expressions in LEM.

See also:
Create a new LEM filter for real-time monitoring for step-by-step instructions. For help creating filters in Monitor view, see The Filter Creation form.

About custom filter expressions

The Filter Creation screen is similar to the Rule Creation screen, but creating filters is more forgiving. Filters report when events occur, so there is no harm if you create an unusual filter with logic issues. Create filters using the Filters Creation screen to familiarize yourself with the logic and tools required to create well-crafted rules.

When creating filter expressions, your conditions can be broad or specific. For example, the All Events filter does not include specific conditions. As a result, it captures all events, regardless of the source or event type. Conversely, the User Logons filter includes one condition: UserLogon Exists. This filter only captures events with the UserLogon event type.

To create a custom filter, click Monitor, click ± in the Filters toolbar, and then select Create. When completed, the Filter Creation screen appears, providing the tools you need to create a custom filter.

Event filters are based on specific events or event groups listed in the left window pane. You can configure your new event by dragging and dropping the event attributes into the Conditions and Notifications configuration boxes. When a LEM Agent or Manager reports an event that matches the event filter conditions, the event message appears in the events grid when the filter is active.

Each new filter is added to the Filters pane. Selecting a filter activates the filter in the events grid. The events grid only displays event messages that meet your filter requirements.

For a video presentation about creating filters and monitoring events in LEM, open the following URL in a web browser:

http://embed.vidyard.com/share/LVjS7MZPtX6MDG9n3E9LLr
Examine the default filters included with LEM

The LEM console includes a variety of filters that support security industry best practices. The following steps describe how to open a filter and view the filter expression.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select the filter you want to examine.
4. Click , and then select Edit.
   The filter expression opens in the Filter Creation pane.

Create conditions to filter event reporting

The Conditions box appears in the Monitor view when you click in the Filters toolbar and select New Filter. Use the Conditions box in conjunction with the Filters pane to configure the conditions that determine events reported by a filter. Conditions are the various rules that state when the filter is to display an event message.

To define conditions, drag event variables from the events, event groups, and fields lists into the conditions box. Use the Conditions connectors to configure how these variables compare to other items, such as time of day sets, connector profiles, user-defined groups, constants, and other event fields.

You can also compare groups with AND/OR conditions. The AND conditions state which events must occur together before the filter shows an event. The OR conditions state that if any one of several conditions occur, the filter shows the event. The combined conditions dictate when the event filter displays an event. The filter ignores (and does not display) any events that do not meet these conditions.

The Conditions connectors enable you to configure relationships between events in the Conditions box and to establish conditions when the event filter displays the event message.

Below is an example of the Conditions box.
The following table describes each feature of the Conditions box.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Group</td>
<td>Configures groups based on the fields you drag from the Filters pane. Click ▼ to collapse an expanded group.</td>
</tr>
<tr>
<td>2</td>
<td>Nested group</td>
<td>Deletes a condition or group, as well as any nested groups. Click to create the nested group.</td>
</tr>
<tr>
<td>3</td>
<td>Delete</td>
<td>Deletes a condition or group, as well as any nested groups. Click to delete the group.</td>
</tr>
<tr>
<td>4</td>
<td>Event variable</td>
<td>Stores event variables (such as events, event groups, and fields) dragged from the Filters pane. As event messages stream into the console, the filter analyzes the values associated with each event variable to determine if the event message meets the filter conditions.</td>
</tr>
<tr>
<td>5</td>
<td>Operator</td>
<td>Describes how the filter compares the event variable to another item to determine if the event meets the filter conditions. Click the operator icon to cycle through and select an operator. Press Ctrl and click the operator icon to select an operator from a drop-down list.</td>
</tr>
<tr>
<td>6</td>
<td>List item</td>
<td>Displays the non-event items from the Filters pane. Drag and drop a list item into this field to define conditions based on your selected filter. Some event variables automatically add a blank constant as the list item. You can overwrite the constant with another list item or click the constant to add a specific value for the constant. For example, clicking a text Constant turns the field into an editable text box so you can type specific text. The text field also allows wildcard characters.</td>
</tr>
<tr>
<td>7</td>
<td>Nested group</td>
<td>Refines your conditions by comparing one group of conditions to another. You can drag event variables and other items from the list pane into the nested group boxes to create the logic for highly-complex and exact conditions. This example above shows one nested group.</td>
</tr>
<tr>
<td>8</td>
<td>Boolean AND operator</td>
<td>Combines or excludes keywords or fields in a search using the Boolean AND operator.</td>
</tr>
<tr>
<td>9</td>
<td>Boolean OR operator</td>
<td>Combines or excludes keywords or fields in a search using the Boolean OR operator.</td>
</tr>
</tbody>
</table>
Configure event filter notifications in LEM

In Filter Creation, the Notifications box defines how the Console is to notify a user when the filter receives an event. Each notification option instructs the console to announce the event in a particular way. You can have the filter display a pop-up message, display the event in bold text, play a warning sound, have the filter name blink, or configure a combination of these methods.

Selecting the notification method

1. In the list pane, click Notifications.
2. From the Notifications list, drag one or more notification options to the Notifications box.
3. Configure each option as described in the Notifications table below.

Notifications table

The following table lists the various notification methods that can be employed to notify a user that a filter’s event threshold has been met.

- The Notification column lists each option that is available in the Notifications list.
- The Description column briefly states how each option behaves.
- The Fields column explains the data fields that can be configured for each option.

<table>
<thead>
<tr>
<th>NOTIFICATION</th>
<th>DESCRIPTION</th>
<th>FIELDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Popup Message</td>
<td>This option causes the filter to display the Popup Notification form when receiving an event. This form states the name of the filter that is receiving the events, and that the filter’s event threshold has been met. From the form, the message recipient can choose to view the filter, to turn off the pop-up form for that filter, or to turn off the pop-up form for all filters.</td>
<td>Notify on x events received</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type the number of events the filter must receive before displaying the Popup Notification form. Repeat on x events received</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you want the pop-up form to appear again after receiving repeated events, select the Repeat on check box. Then in the events received box, type how many more events the filter should receive before issuing the pop-up form another time.</td>
</tr>
<tr>
<td>Notification</td>
<td>Description</td>
<td>Fields</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Display New Events As Unread</td>
<td>This option displays new events in the filter with bold text.&lt;br&gt;They remain bold until you acknowledge them by clicking them or by opening them in the Event Explorer.</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Enable Blinking Filter Name</td>
<td>This option causes the filter name to blink in the Filters pane.</td>
<td>Color</td>
</tr>
<tr>
<td></td>
<td>Click the Color button to open the Blink Color form. Choose a color from one of the three color palettes. Then click OK. The filter name will blink in this color.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time (ms)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Move the slider to select the amount of time between blinks, in milliseconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Notify on x events received</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type the number of events the filter must receive before the filter tab begins blinking.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Repeat on x events received</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The filter tab stops blinking once you acknowledge it by selecting it. If you want the tab to begin blinking again after receiving repeated events, select the Repeat on check box. Then in the events received box, type how many more events the filter should receive before it starts blinking again.</td>
<td></td>
</tr>
</tbody>
</table>
### Get started building custom rule expressions in LEM

This section provides information to help you write custom rule expressions in LEM.

**See also:**
- Rule Creation screen and the Rule Builder form
- Create a new LEM rule to monitor and respond to events for step-by-step instructions.
- The Rules view

### About custom rule expressions

Use caution when creating rules. SolarWinds recommends that you practice creating filters before you start creating rules. Creating rules is similar to creating filters, but filters report event occurrences whereas rules act on them.

**Begin configuring rules when you are comfortable with configuring filters. Always test your rules before implementing them.**
You can create rules by configuring conditions between alert variables and other components (such as time of day sets, user-defined groups, constants, and so on). Using rules, you can correlate alert variables with other alerts and their alert variables.

You can configure rules to fire after multiple alerts occur. LEM remembers alerts that meet the basic rule conditions and waits for additional conditions to be met. The rule does not execute until the alerts meet all the conditions and correlations defined for the rule.

When you correlate alert variables, you specify how often and in what time frame the correlations must be met before the rule is triggered. The combined correlations dictate when the rule initiates an active response.

**Use the ToolAlias field in LEM rules and filters to capture traffic from a specific device**

The ToolAlias field is a useful field to know if you have to create filters, rules, and searches that target traffic from a specific device. Every device that sends events to LEM has an Alias property that you can customize with a device-specific name. Use the ToolAlias field to examine the Alias property and find events that match your filter criteria.

You can also use the DetectionIP event to monitor events from a device that has a specific IP address, for example AnyAlert.DetectionIP=10.1.1.1.

**Create a filter to capture events from a specific device**

Use the ToolAlias field to create a filter that captures traffic from a specific device.

This procedure can also be applied to rules and searches.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, click +, and then select New Filter.
4. Select one of the following conditions from the Events or Event Group (but don’t drag it into the Conditions box, yet):
   - To view all traffic from your device, select Any Alert from the Events group.
   - To view all network events from your device, select Network Audit Alerts in the Event Groups.
   - To view web traffic from your device, select WebTrafficAudit from the Events group.
5. Below your selection, in the Fields list, select ToolAlias and drag it into the Conditions box.
6. In the Constant field in the Group box, enter filter criteria to match the Alias property of the device that you want to track. Use asterisks (*) as wildcard characters to avoid entering the entire value.
For example, consider the default Firewall filter. Its condition is Any Alert. ToolAlias = *firewall*. This assumes that the firewall connector was configured with a Tool Alias that includes firewall in the name.

7. Click Save.

If your filter does not generate events in the LEM console, verify that the Tool Alias value matches the Alias property for your device. See the next section for steps.

Verify that the correct Alias value is associated with the connector

The following procedure applies to devices configured to send logs to LEM. To verify Agent connectors, use this same procedure, but apply it to the Agent associated with the connector instead.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. Next to the appropriate LEM Manager, click ✗, and then select Connectors.
4. At the bottom of the Refine Results pane, select Configured.
5. Select the connector instance that you want to verify.

   Configured tool instances appear with a ✗ in the Status column.

6. Verify that the Alias field value is correct.
   To change the Alias property (optional):
   a. Next to the connector, click ✗, and then select Stop.
   b. Next to the connector, click ✗, and then select Edit.
   c. Edit the Alias field value, and then click Save.
   d. Next to the connector, click ✗, and then select Start.

7. Click Close.
nDepth search: Explore event history using nDepth and other LEM utilities

These sections describe how to perform a basic search with nDepth search, use nDepth's graphical tools, use nDepth with other explorers, and respond to your results.

About LEM nDepth search

The nDepth search engine can locate any event data that passes through a particular LEM Manager instance. You can use nDepth to conduct custom searches, investigate your search results with graphical tools, investigate event data in other explorers, and act on your findings.

Click the video icon to learn how to use nDepth in LEM.

nDepth visual tools

nDepth summarizes and displays search results with several different visual tools that can also be combined into a customizable dashboard. The tools are intuitive and interactive—you can point and click to refine your searches. Each graphical tool provides an alternative view of the same data, so you can examine your data from several perspectives. You can also view and explore a text-based view of the actual data.

nDepth employs drag-and-drop tools that let you configure simple or even complex search criteria. You can use these tools to dig deeper into your findings by adding search conditions, or by appending text to existing search strings. nDepth also includes a tool called Search Builder that lets you configure complex search criteria using the same sort of drag-and-drop interface found in Filter Creation.

nDepth primary uses

Use nDepth to do the following:

- Search normalized event data.

  If the nDepth log retention option is enabled, nDepth search can also search raw (non-normalized) log messages that are stored separately. See Configure LEM to store original log messages (nDepth log retention) to learn more about nDepth log retention.

- View, explore, and search significant event activity. nDepth summarizes event activity with simple visual tools that you can use to easily select and investigate areas of interest.

- Use existing filter criteria from the Monitor view to create similar searches.

- Conduct custom searches. You can also create complex searches with the Search Builder, which is a tool that behaves just like the Filter Builder. You can also save any search, and then reuse it at any
time by clicking it.

- Save and reuse custom searches.
- Schedule saved searches.
- Create your own custom widgets for the nDepth Dashboard.
- Export your findings to a printable report in PDF format, or your search results to a spreadsheet file in CSV format.
- Use the Explore menu to investigate nDepth search results with other explorers.
- Use the Respond menu to act on any of your findings.
- Export your findings to a report in PDF format.

Events and Log Messages

If the nDepth log retention option is enabled, LEM uses two data stores: the first data store is for normalized event data, and the second data store is for original (raw) event data. Use the following nDepth modes if nDepth log retention is enabled:

- **Events mode.** nDepth summarizes and explores your normalized event data. Normalized data appears in Monitor view and is stored in the LEM database.
- **Log Messages mode.** nDepth summarizes and explores raw log messages received from the original event logs. Use this mode if you have specific data analysis needs and understand how to interpret raw log messages generated by network devices and tools.

⚠️ Data storage is limited. If you have not configured a CMC option for archiving data, LEM will delete the oldest data to make room for new data.

Common data fields in nDepth search

See [Common data field categories in LEM nDepth search](#)

**Open nDepth search in LEM**

To conduct custom searches in the LEM console, choose Explore > nDepth. Log in as an administrator or auditor to use nDepth.

By default, the nDepth search period includes the last 10 minutes. Specifically, the search period starts at the time you open nDepth, and stops 10 minutes prior.

The following illustration provides an overview of the nDepth view.
<table>
<thead>
<tr>
<th>NUMBER</th>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>History</td>
<td>Displays links to your recent nDepth search results.</td>
</tr>
<tr>
<td>2</td>
<td>Saved Searches</td>
<td>Displays links to your saved nDepth search results.</td>
</tr>
<tr>
<td>3</td>
<td>List pane</td>
<td>Displays categorized lists of events, event groups, event variables, and additional options you can use to create conditions for your filters.</td>
</tr>
<tr>
<td>4</td>
<td>Search bar</td>
<td>Searches all event data or the original log messages that pass through a LEM Manager. Drag the toggle switch to select Drag &amp; Drop or Text Search mode.</td>
</tr>
<tr>
<td>5</td>
<td>Respond</td>
<td>Displays a list of corrective actions you can execute when an event occurs, such as shutting down a workstation or blocking an IP address.</td>
</tr>
<tr>
<td>6</td>
<td>Explore</td>
<td>Displays several utilities you can use to research an event, including Whois, Traceroute, and NSlookup.</td>
</tr>
<tr>
<td>7</td>
<td>Time</td>
<td>Provides a drop-down menu to select the time range for your search.</td>
</tr>
<tr>
<td>8</td>
<td>Play</td>
<td>Executes the selected search.</td>
</tr>
<tr>
<td>9</td>
<td>Histogram</td>
<td>Displays the number of events or log messages reported within the selected search time range.</td>
</tr>
<tr>
<td>NUMBER</td>
<td>ITEM</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>Dashboard</td>
<td>Displays the search results in all available widgets. You can change this view by clicking a widget in the nDepth toolbar. The 🗿️ icon indicates you are exploring event data. The 📊 icon indicates you are exploring log messages.</td>
</tr>
<tr>
<td>11</td>
<td>nDepth toolbar</td>
<td>Organizes log data into categories to identify activity in your network. Click a selection to display the category below the histogram.</td>
</tr>
</tbody>
</table>

Open nDepth from another data source

You can open nDepth from an existing data source, such as an event field or another explorer (such as NSLookup, Whois, Traceroute, and Flow) to search for similar events and data.

1. Select the data you want to explore using one of the following methods:
   - In the Monitor view event grid, select the event row or field you want to explore.
   - In the Event Details pane, event map, or event grid, click the item or field you want to explore.
2. From the Explore drop-down list on the Events grid, select nDepth.

The nDepth screen appears, and the nDepth search box contains the event or event field you are exploring.

When you initiate an nDepth search from Monitor view, nDepth automatically searches all hosts and sources for every instance of the selected event field that has occurred within a ten-minute period around the event that you are exploring. This way, you can identify similar events that occurred before and after the event you are exploring.

Search normalized data using nDepth search in LEM

This section describes how to use nDepth to search for normalized event data that passes through a particular LEM Manager.
Create an nDepth query

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. To clear all existing parameters, click x in the search bar.
4. Drag search items to the search box, and then enter a search expression.
5. Modify the default time frame as required.
6. To begin your search, click ➤

Choose an event in Monitor view to send to nDepth for historical search

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. In the nDepth filter sidebar, select a filter.
4. Locate an event in the event grid that you want to research.
5. To stop the event feed, click Pause.
6. Select the event in the grid.
7. From the Explore drop-down list, select nDepth.
   The nDepth screen appears, displaying your results.

In the nDepth screen, you can narrow or widen your search time line using the nDepth histogram. After you establish your search time line, click a tool in the nDepth toolbar to review your results.

Choose a filter in Monitor view to send to nDepth for historical search

You can select a real-time filter in Monitor mode to open in nDepth search. This task requires either the Administrator or Auditor role.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or an auditor.
2. On the LEM toolbar, click Monitor.
3. In the filter sidebar, select the filter you want to send to nDepth.
4. In the Filters pane, click ⚅, and then select Send to nDepth.
The filter opens in the nDepth search engine.

5. Modify the nDepth search Conditions or time frame to fine tune your search (Optional).

   Always click Search, denoted by a play button, after altering an nDepth search to get your new results.

Create an nDepth query for all activities by a single user

Use nDepth to create queries for all activity related to a single user or group of users on your network. This is currently the only method to perform this level of reporting and monitoring in LEM.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

   Log in as an administrator or an auditor.

2. On the LEM toolbar, navigate to Explore > nDepth.

3. To clear all existing parameters, click \( \times \) in the search box.

4. In the Refine Fields list, locate the User Name drop-down list.

5. Drag User Name into the search box at the top. If you choose a different user, change the user next to the pencil icon in the search.

6. Use this selection or change the user name in the Constant text box.

   When you change the user name:
   
   - Use trailing wild card characters (such as *) to search for part of a user name.
   - Avoid using leading wild card characters whenever possible.
   - Use user-defined groups or directory service groups to search for groups of users.

7. Modify the default time frame as required.

8. To begin your search, click .

Delete items from search strings

To delete a search string, click \( \times \) next to a condition in the search bar. You can delete individual conditions, groups of conditions, or the entire string.
Adjust the time frame for your nDepth query

1. In the search bar, click the time selector drop-down list, and then select Custom range.

2. Select the From and To dates and times in the calendars.

   By default, the custom time frame shows the time frame of your last search.

3. Click outside the calendars to close.

   Searches that require several minutes to complete or searching several events can result in the search producing time outs or no results.

Search raw log messages using nDepth search in LEM

If the nDepth log retention option is enabled, you can use nDepth to view and search your original, non-normalized log messages in the LEM console. For details, see About nDepth log retention.

To view and search original log messages using nDepth

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

   Log in as an administrator or an auditor.

2. On the LEM toolbar, navigate to Explore > nDepth.

3. On the far right of the search box, move the switch from Events to Log Messages.

   This switch only appears if LEM is configured to store original log messages.
4. Construct an nDepth search as you would for normalized alerts:
   - Drag Refine Fields components into the search box.
   - Switch the search method from Drag & Drop Mode to Text Input Mode on the left of the search box, and then enter your search conditions in plain text.

   See Search normalized data using nDepth search in LEM for help.

5. Click Search.

Manage nDepth search queries in LEM: Save, schedule, run on-demand, and more

This section explains how to save an nDepth search query, run it on-demand or at a later date, and export the search results. It also describes how to edit or delete saved queries.

Search queries can be saved and scheduled. Save and export your search query for disaster recovery purposes or to share it with another user when they are logged in to the console. A scheduled search can email the results to a defined user.

Save an nDepth search query

1. Create and run an nDepth search query. See Search normalized data using nDepth search in LEM for help.

2. In nDepth, click ![Save As](image) and then select Save As.

   ![Save As](image)

   If you are modifying an existing saved search, click Save.

3. In the Search Name field, enter a report name up to 200 characters in length, and then click OK.

   ![Icon](image)

   SolarWinds recommends that you include the time frame in your search name, as saved searches always run with the saved time frame by default. For example, enter All Firewall Alerts - Last 24 Hours.

4. Click OK.

   Your search appears in the Saved Searches pane appended with an icon.

   - ![Event Data Search](image) indicates an event data search.
   - ![Original Log Message Search](image) indicates an original log message search.
Edit a saved nDepth search query

To edit a saved search query, modify it and save it as a new search.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   - Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. To display the Saved Searches pane (if required), click History in the upper-left corner.
4. In the Saved Searches pane, click the search you want to modify.
5. In the search bar, reconfigure the search.
6. Click 📝, and then select Save.
   - The search is saved with the new configuration.
7. Delete the old search query if you no longer need it. See Delete a saved nDepth search query for help (Optional).

Run a saved nDepth search query on demand

Saved searches are stored and listed alphabetically in the Saved Searches pane.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   - Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. To display the Saved Searches pane (if required), click History in the upper-left corner.
4. In the Saved Searches pane, click the search you want run. Move the pointer over the search for tooltip information.
   - nDepth displays your search data.

Schedule a saved nDepth search query

Schedule a saved search to run automatically at a prescheduled time. You can also share scheduled searches between users.

ℹ️ If the virtual appliance is offline for an extended amount of time (such as more than a day or two), the active schedules may not run at the expected time until the appliance is back online for several hours.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   - Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. To display the Saved Searches pane (if required), click History.

4. From the Saved Searches pane, select a Saved Search.

5. Click \(\text{ Schedule }\), and then select Schedule.

6. Complete the fields as required.

7. Click OK.

Delete a saved nDepth search query

You can permanently delete a search from your Saved Searches pane.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

   Log in as an administrator or an auditor.

2. On the LEM toolbar, navigate to Explore > nDepth.

3. In the Saved Searches pane, move the mouse over a search you want to delete.

4. To delete the search, click \(\text{ }\).

5. When prompted, click Yes to confirm.

   The saved search is deleted.

Export nDepth search results in CSV format

You can only export text results in CSV format. To export charts and graphs, see the PDF export procedure below.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

   Log in as an administrator or an auditor.

2. On the LEM toolbar, navigate to Explore > nDepth.

3. Review all alerts within the last ten minutes.

4. To refine your search parameters, modify the search to extend the time frame, or use the Refine Fields pane.
5. To retrieve your new results, click 🔄.

6. On the nDepth toolbar, click Result Details.

7. In the Result Details pane, click 🔄, and then select Export to CSV.

8. To continue, click Yes.

9. Save the file to the appropriate location.

Export nDepth search results in PDF format

You can export the results of your nDepth search to a printable report and save the report as a PDF file.

PDF reports are limited to 25,000 events or log messages. If you need a larger report, use the Result Details view to export your search results to a spreadsheet in CSV format.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, navigate to Explore > nDepth.

3. Review all alerts within the last ten minutes.

4. Modify the search to extend the time frame or use the Refine Fields pane to refine your search parameters.

5. To retrieve your new results, click 🔄.

6. On the nDepth toolbar, click Result Details.

7. On the nDepth page, click 🔄, and then select Export. Do not click the gear icon in the Result Details pane, click the gear in the upper-right corner above.

8. Customize your report layout:
   a. Replace nDepth Export Report Title with a custom title as required.
   b. Click the page thumbnails and remove page elements (such as charts, graphics, and text) as required.
   c. Adjust the page layout to Portrait or Landscape as required.
   d. Add a new page, click the Items tab, and drag item elements to add additional charts to your report (Optional).

   Some components, such as Result Details, are limited to where they can be dropped.

   e. Click the Saved Layouts tab and click 🔄 to create a new layout or save your layout (Optional).

9. Click Export to PDF.

10. Save the file to the appropriate location.
Visualize search results and take action with nDepth widgets and the Respond menu in LEM

This section documents how to use the Respond menu, and how to work with nDepth widgets.

For details about each nDepth widget type, also see The nDepth view.

About the Explore and Respond menus

The Respond and Explore drop-down menus are located at the top of the nDepth view.

- The Respond menu provides a list of corrective actions you can take in response to an event presented in an explorer, such as shutting down a workstation.
- The Explore menu lists utilities you can use to investigate an event, event detail, or nDepth search result. For more information see Use the explorer utilities in LEM to search or analyze nDepth query results.

Respond to an event with the nDepth Respond menu

Use the actions in the Respond drop-down menu to respond to an issue reported in your nDepth search results. For example, you can block a hostile IP address or send a user account a pop-up message if you see an unusual event.

For more information see About LEM response actions.

1. Run a search in nDepth. See Search normalized data using nDepth search in LEM or Search raw log messages using nDepth search in LEM for help.
2. Select a results entry, and then choose a response from the Respond menu at the top of the nDepth page.
About nDepth widgets

nDepth provides a set of default widgets similar to the widgets in the Ops Center.

Each widget represents a high-level graphical view of the specific network activity associated with your nDepth search results. The widget displays the primary items generating an activity, as well as the count (or number of incidents) for each item.

Use nDepth explorer views to create new widgets, change the look of existing widgets, add widgets to the nDepth Dashboard, and remove widgets you no longer use. Click refresh on the widget toolbar to display the latest data from your network.

View widget details

Click or point to an item in the widget to view details and statistics about the item.
Create a search string from a widget item

You can use items in widgets or any of the nDepth graphical tools to create new search strings, or to append existing search strings.

1. To delete the existing search string, click the delete icon on the search box.
2. Click an item on a widget.
   A new search string associated with the widget item appears in search box.

To append an existing search string with an item from a widget, click an item on the widget. In the search box, a new search string associated with the widget item is appended to the existing search string.

Create a new nDepth widget with nDepth Widget Builder

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. Click a view on the nDepth toolbar, such as bar charts, line charts, pie charts, or bubble charts.
4. To open the nDepth widget builder, click the plus icon on the view title bar.
5. Complete the widget builder selections to configure the new widget.
   The new widget appears at the bottom of the chart view.
   When you configure the widget and choose the Save to Dashboard option, the new widget also appears at the bottom of the nDepth dashboard.

Edit an nDepth widget

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. On the nDepth toolbar, click a view such as bar charts, line charts, pie charts, or bubble charts.
4. Locate the widget you want to edit, and then click the edit icon.
5. Use the nDepth Widget Builder to reconfigure the widget.
   The updated widget appears at the bottom of the view.
   When you configure the widget and choose the Save to Dashboard option, the new widget also appears at the bottom of the nDepth dashboard.
6. To refresh the widget data, click the refresh icon.
Add a chart widget to the nDepth dashboard

You can add an nDepth view (such as word cloud, tree view, or result details) to the nDepth Dashboard. The word cloud, tree view, and result details view display by default. If you remove a view from the dashboard, use this procedure to restore the view.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. To open the chart view you want to see, use the nDepth explorer toolbar.
4. In the view, locate the chart widget you want to add to the dashboard.
5. To add the widget to the dashboard, click 📊 on the widget toolbar.
   The widget is copied to the bottom of the nDepth Dashboard.
6. To minimize the widget in the dashboard, click ⌂. To restore the widget, scroll down and click the widget title bar.

See also:
- The nDepth view for information about each nDepth widget type

Use the explorer utilities in LEM to search or analyze nDepth query results

This section describes how to open the explorer utilities in LEM. The explorer utilities are available from Monitor view, the Explore > nDepth view, and the Explore > Utilities view.

About the Explorer utilities

LEM includes the following Explorer utilities:

- Event
- nDepth
- NSLookup
- Whois
- Traceroute
- Flow

See The Utilities view for documentation about each explorer. For the Flow utility, also see Collect and view NetFlow and sFlow data in LEM.

Use these explorers to investigate event details in your nDepth search results. For example, you can investigate a suspicious IP address with the NSLookup, Traceroute, or Whois explorers to better understand who the IP address is assigned to.
Open the explorer utilities from the nDepth view to investigate event details

1. Run a search in nDepth. See Search normalized data using nDepth search in LEM or Search raw log messages using nDepth search in LEM for help.
2. Select a results entry, and then click the Explore menu to choose an explorer utility.
3. Type the event details into the appropriate explorer field, and then click Search or Analyze (depending on the type of explorer you chose).

Open the explorer utilities from Monitor view or the Utilities view

You can manually explore an IP address, host name, or domain name by opening an explorer in Monitor view or the Utilities view.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Explore > Utilities, or click Monitor.
3. To choose an explorer utility, click the Explore menu in the upper-right corner.
4. Type the event details into the appropriate explorer field, and then click Search or Analyze (depending on the type of explorer you chose).

Collect and view NetFlow and sFlow data in LEM

This section describes how to enable and view NetFlow and sFlow data. The Flow utilities are available from Monitor view, the Explore > nDepth view, and the Explore > Utilities view.

About the Flow explorer

Flow explorer performs flow analysis to determine which IP addresses or ports are generating or receiving the most network traffic. Use this explorer to analyze the volume of data (in bytes or packets) transferring to or from an IP address or port number on your network.

For example, if an unknown IP address displays at the top of the Flow explorer’s activity list, you can select a bar on the graph or a row in the table and choose the Whois explorer from the Explore menu to identify the IP address and why it is transmitting so much data.

LEM supports Flow exports from both NetFlow and sFlow devices. Use the Flow explorer in the LEM console to view graphs, charts, and grids, as well as:

- Top Talkers by Internet Assigned Numbers Authority (IANA)-based Protocol
- Top Talkers by Port
- Top Talkers by Source/Destination Address
- Top Talkers by Total Bytes
- Top Talkers by Total Packets
See the manufacturer specifications to configure your devices to send Flow data to LEM. LEM supports data on the 2100/UDP for NetFlow devices and 6343/UDP for sFlow devices.

Enable Flow collection and analysis in LEM

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. At the cmc> prompt, enter service.
3. At the cmc::service> prompt, enter enableflow.
4. To confirm your entry, enter y.
   The Manager service on LEM automatically restarts.
5. At the prompt, enter n and follow the prompts to select the Flow collector and enable Flow Analysis for Flow data collected on another system.
   Otherwise, enter y.
6. To return to the cmc> prompt, enter exit, and then press Enter.
7. To log out of LEM, enter exit, and then press Enter.

View Flow data in the LEM console

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. From the Explore drop-down list, select Flow.
   The Flow Explorer presents data in graph, chart, or grid formats.
LEM reports: Create reports for regulatory and compliance purposes

About LEM reports

This topic introduces LEM reports and describes how to log in to the LEM reports application.

See "Install the LEM reports application" on page 1 in the LEM Installation Guide if you have not yet installed the reports application.

LEM reports overview

The LEM reports application converts LEM database data into information that can be used to troubleshoot and identify network problems. Run reports on your Log & Event Manager database to view events and trends and make informed decisions about your network activity. You can run over 200 standard and industry-specific reports that can help you make informed decisions about your network security.

About report categories

LEM reports are organized into categories:

- **Standard Reports** ship with LEM. Most standard reports capture specific event data that occurs during a particular period.
- **Industry Reports** support the compliance and auditing needs of certain industries (such as financial services and healthcare), and the accountability requirements of publicly-traded companies.
- **Custom Reports** display reports you created to meet a specific need.
- **Favorite Reports** displays the standard, industry, and custom reports you use most often. You can add and remove reports to this category as needed.

Standard and Custom reports are essentially the same report. The only difference is that Custom reports are undocumented and created specifically by (or for) you.

About report levels

There are three LEM report levels:

- A master report is a standard report that includes a series of subtopics, where each subtopic contains a specific set of details about the higher-level master topic. Together, these topics create the report, similar to chapters in a book. Master reports include a graphical summary page.
- A detail report is a report that includes all events and event details.
- A top report includes the top events for a selected category.
About scheduled and on-demand reports

The reports application can run scheduled or on-demand reports:

- Scheduled reports are reports you configure to automatically run on their own, on a particular schedule, and without intervention.
- On-demand reports are reports you run only when you need them.

SolarWinds recommends identifying who needs to receive performance or status reports, and how often they should receive them.

After you run a report, you can print it or export it to several supported formats, including PDF and Microsoft Word).

Open the LEM reports application

Launch Reports as an administrator the first time you run the application. Depending on your Windows security set up, you may always need to run reports using the Run as administrator option. See To automatically Run as administrator every time you run Reports for help.

1. Log in to a Windows computer that has the LEM reports application.
   - Click Start, and then select All Programs.
2. Choose the SolarWinds folder, and then click the Reports shortcut.
   - The LEM reports application opens.

To automatically Run as administrator every time you run Reports

1. Right-click the Reports application icon.
2. On the Shortcut tab, click Advanced.
3. Select the Run as administrator check box, and then click OK.

Setting up the LEM reports application

Complete the steps in this section after you install the reports application.

See "Install the LEM reports application" on page 1 in the LEM Installation Guide if you have not yet installed the reports application.

Configure the LEM reports application to communicate with the LEM database

SolarWinds recommends that you create a special service account for use with the LEM reports application. See Create a local LEM user account for instructions and specify Reports in the LEM Role field. The Administrator and Auditor roles can also use the LEM reports application.
1. Open the LEM reports application. See Open the LEM reports application for steps.
   - Launch Reports as an administrator the first time you run the application. Depending on your Windows security set up, you may always need to run reports using the Run as administrator option. See Setting up the LEM reports application for help.
   - The first time you open Reports, a pop-up window displays the message A manager list was not found. Please create a list containing at least one manager. This is not an error. Click OK to close the pop-up window.

2. On the Settings tab, click the Configure button (the button with a gear icon).
3. Choose Managers - Credentials and Certificates.
4. Complete the fields as required.
   a. Manager name – Enter the IP address of the LEM Manager.
   b. User name – Enter the service account user you created to log in to the LEM reports application.
   c. Enter the password for the service account user.
   d. Select the green + button to save the credentials.
   e. Close the window.

5. Click Test Connection to verify the connection.
   See Troubleshoot the LEM reports application database connection if the connection failed.
6. Click OK.
   The reports application is connected to the LEM database server.

Secure the LEM reports application

To secure the LEM reports application, see the following topics in the "Securing LEM" section of the LEM Administrator Guide:

- Restrict access to the LEM reports application
- Enable transport layer security (TLS) in the LEM reports application
Select a default primary data source

Select the primary data source connection for running reports when you open the LEM reports application. The connection settings display as the default setting in the Data Source drop-down menu.

You can select a different data source when you open the LEM reports application. The next time you open the application, the setting defaults to the primary data source.

1. Open the LEM reports application. See Open the LEM reports application for steps.
2. On the Settings tab, click Configure, and then select Primary Data Source.
3. In the Primary Data Source list, select the default data source.

![Select Primary Data Source](image)

4. To verify your connection to the data source, click Test Connection.
   - If the test succeeds, Ping Test success appears in the dialog box. If the test fails, an error message appears. See Troubleshoot the LEM reports application database connection.
5. Click OK.
   - The default primary data source is configured.

Configure a syslog server (optional)

You can enable a LEM Manager to send report log information to a syslog server to record all report-related events and application messages. The server logs basic report activity, such as the user name, report type, targeted database, report time, and any error messages that occur while generating the report.

The syslog server is set to the Primary Manager by default, but can be set to any server running a standard syslog service. The server must have an Agent installed to communicate with the LEM Manager.

1. Open the LEM reports application. See Open the LEM reports application for steps.
2. On the Settings tab, click Configure, and then select Syslog Server.
   - The Set Syslog Server form appears.
3. In the Syslog Server (Host Name) box, enter the server host name.
4. Click Test.

The system tests the connection.

You must test the connection before the server can be accepted. A successful test does not confirm that the host is a syslog server.

- If the ping test succeeds, The Ping Test succeeded notification appears in the dialog box with the host IP address.
- If the ping test fails, an error message appears. Verify that you entered a host name that matches a valid DNS entry, and then click Test.

5. Click OK.

The syslog server is configured.

The LEM reports application interface

This section describes the LEM reports application interface. See About LEM reports for a LEM reports overview and steps to log in to the reports application.
The Reports application features

This topic describes the Reports application interface and its key features.

![Reports application interface](image)

The following table describes the reports application.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Menu button</td>
<td>Opens, saves, or prints a report. Also provides additional options for your report.</td>
</tr>
<tr>
<td>2</td>
<td>Quick Access Toolbar</td>
<td>Contains a set of commands independent of the currently-selected tab. You can customize the toolbar by adding buttons for the commands you use most often and move the toolbar to two different locations. See the <a href="#">Quick Access toolbar</a> for more information.</td>
</tr>
<tr>
<td>3</td>
<td>Ribbon</td>
<td>Locates the commands you need to complete a task. Commands are organized in logical groups under tabs. Each tab relates to a type of activity, such as running and scheduling reports, or viewing and printing reports. To save space, you can minimize the Ribbon, displaying only the tabs. See <a href="#">Minimize the ribbon</a> for more information.</td>
</tr>
<tr>
<td>4</td>
<td>Settings tab</td>
<td>Helps you select the reports you want to run, open, and schedule. You can also configure reports and the report data source settings.</td>
</tr>
</tbody>
</table>
### Item Name | Description
---|---
5 | View tab
| Provides options to print, export, resize and view a report.
| Click this tab after you run a report to view the report contents.
6 | Grouping bar
| Provides options to group, sort, and organize the reports list.
7 | Report list/Preview pane
| Displays a list of standard reports by default. When you select a new report category, the grid displays the reports for your selected category. Use this grid to select report that you want to run or schedule.
| You can also filter and sort the grid to quickly find the reports you want to work with.
| When you open or run a report, this section changed into a report preview pane that displays the report. The ribbon automatically switches to the View tab with a toolbar to print, export, resize, or view the report.

### Menu button

Click the menu button to open a drop-down menu and execute the most common report commands. In Reports, the menu button opens a menu that lets you execute the most common report commands, as described below.

### Menu Option | Description
---|---
Open Report | Opens a report saved in RPT format. The report opens in the Reports Preview pane in the View tab where you can view, search, print, and export the report. You can also view and execute recently-opened report files.
Export Report | Exports the selected report.
Schedule Report | Configures a schedule to automatically run the selected report in the report list.
Print Report | Prints your selected report to your default printer.
**Quick Access toolbar**

The Quick Access toolbar contains a set of commands that are independent of the active tab. You can customize the toolbar by adding buttons for the commands you use most often, and you can move the toolbar to two different locations.

**Default commands**

By default, the Quick Access Toolbar shows the commands listed in the following table.

<table>
<thead>
<tr>
<th>BUTTON</th>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Open</td>
<td>Opens a report saved in RPT format. The report opens in the Reports Preview pane in the View tab where you can view, search, print, and export it.</td>
</tr>
<tr>
<td></td>
<td>Run</td>
<td>Runs the report currently selected in the report list. If the report requires any parameters, the Enter Parameter Values form appears. See Run and schedule reports to run a report.</td>
</tr>
<tr>
<td></td>
<td>Refresh Report List</td>
<td>Refreshes the report list for each report category. Use this command if you added new report files (such as new custom reports) and they do not appear in the report list. This command accesses the Reports directory on your computer, retrieves information about all of the reports, and rebuilds the lists for each report category.</td>
</tr>
<tr>
<td></td>
<td>Exit</td>
<td>Exits the Reports application.</td>
</tr>
</tbody>
</table>
Customize the Quick Access Toolbar

You can customize the toolbar by adding or removing any command displayed on the ribbon, customizing the toolbar with the commands you use most often.

1. Next to the Quick Access Toolbar, click the drop-down list.
2. In the Customize Quick Access Toolbar form, add or remove commands from the toolbar.
   - To add a button to the toolbar, select the corresponding command check box.
   - To remove a button from the toolbar, clear the corresponding command check box.
   - To choose from a list of additional commands, click More Commands, and then use the Customize view to add or remove commands to the toolbar.

Add commands from the ribbon

1. On the ribbon, click the appropriate tab or group to display the command you want to add to the toolbar.
2. Right-click the command, and then click Add to Quick Access Toolbar on the shortcut menu.
   - The command appears in the toolbar.

Move the Quick Access Toolbar

The Quick Access Toolbar is in the upper-left corner of the window next to the Reports Button (default) or below the ribbon. You can move the toolbar to another location.

1. Next to the Quick Access Toolbar, click the drop-down list.
   - The Customize Quick Access Toolbar form appears.
2. In the Customize Quick Access Toolbar form, move the toolbar below or above the ribbon.
   - To move the toolbar below the Ribbon, click Show Quick Access Toolbar Below the Ribbon.
To move the toolbar above the Ribbon, click Show Quick Access Toolbar Above the Ribbon.

Minimize the ribbon

You can minimize the ribbon to make more space available on your screen. When the Ribbon is minimized, only the tabs display.

To keep the ribbon minimized, click the drop-down list next to the Quick Access toolbar and select Minimize the Ribbon. To use the ribbon while it is minimized, click the tab you want to use and select the option or command you want to use. After you click the command, the ribbon returns to a minimized view.

To restore the Ribbon, click the drop-down list next to the Quick Access Toolbar and clear the Minimize the Ribbon check box.

To toggle between full and minimized view, double-click the name of the active tab or press Ctrl+F1.

The Preferences group

In the Preferences group, use the Configure drop-down menu to link the LEM reports application to a data source (such as a LEM Manager). You can select a primary data source, a syslog server, or a data warehouse.

The following table describes each option in the Preferences group.

<table>
<thead>
<tr>
<th>PREFERENCE / OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure</td>
<td></td>
</tr>
</tbody>
</table>
### Find, filter, and group LEM reports

This section describes how to find and work with LEM reports.

#### Find a LEM report by title

1. Open the LEM reports application. See [Open the LEM reports application](#) for steps.
2. Click the Settings tab.
3. From the Category drop-down list, select the category that contains your targeted report.
4. Click a report title and begin entering your report name.

   The console highlights the first report that matches your text. For example, if you click Standard Reports and enter *Event*, the system highlights Event Summary, which is the first matching report title.
Find reports for specific industries

Use the Industry Setup tab to select the industries and areas of regulatory compliance related to your company. This helps you reduce the number of reports that display in the Industry Reports list.

1. Open the LEM reports application. See [Open the LEM reports application](#) for steps.
2. On the Settings tab, click Manage, and then select Manage Categories.
3. In the Manage Categories form, click the Industry Setup tab.
   The Classifications section lists industries and regulatory areas supported by standard Reports. The Reports for section displays the standard reports that support your classification selections.
4. Select the check box for each industry related to your company.
   The Reports for section displays all standard reports that support your selected industry.
5. Select the check box for each regulatory area related to your company.
   See [Industry options](#) for more information.
6. Click OK.

Industry Options

Industry reports are standard reports designed to support the compliance and auditing needs of certain industries. SolarWinds provides reports that support the financial services and health care industries, as well as the accountability reporting needs of publicly traded companies. The following table describes the compliance and auditing areas supported in the reports.

<table>
<thead>
<tr>
<th>Supported Industry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Education</strong></td>
<td></td>
</tr>
<tr>
<td>FERPA</td>
<td>Federal Educational Rights and Privacy Act (FERPA), which gives parents and eligible students certain rights with respect to their children’s education records.</td>
</tr>
<tr>
<td><strong>Federal</strong></td>
<td></td>
</tr>
<tr>
<td>CoCo</td>
<td>UK Code of Connection regulations.</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Management Act (FISMA).</td>
</tr>
<tr>
<td>NERC-CIP</td>
<td>North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) reliability standards.</td>
</tr>
<tr>
<td><strong>Finance</strong></td>
<td></td>
</tr>
<tr>
<td>SUPPORTED INDUSTRY</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CISP</td>
<td>Cardholder Information Security Program, which helps safeguard credit card and bank card transactions at the point of sale, over the Internet, on the phone, or through the mail. CISP helps protect cardholder data for cardholders, merchants, and service providers.</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information and related Technology (COBIT™). COBIT is an open standard for IT security and control practices. It includes more than 320 control objectives and includes audit guides for more than 30 IT processes.</td>
</tr>
<tr>
<td>GLBA</td>
<td>Gramm Leach Bliley Act (GLBA). GLBA requires financial institutions to protect the security, integrity, and confidentiality of consumer information. It affects banking institutions, insurance companies, securities firms, tax preparation services, all credit card companies, and all federally insured financial institutions. Security information and event management (SIEM) plays a vital role in GLBA.</td>
</tr>
<tr>
<td>NCUA</td>
<td>National Credit Union Administration (NCUA). NCUA is the federal agency that charters and supervises federal credit unions and insures savings in federal and most state-chartered credit unions across the country through the National Credit Union Share Insurance Fund (NCUSIF), a federal fund backed by the United States government.</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry (PCI) Data Security Standard requirements of VISA CISP and AIS, MasterCard SDP, American Express and DiscoverCard.</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley (SOX) Act of 2002. Sarbanes-Oxley protects company investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws. Provisions within Sarbanes-Oxley hold executive management and the board of directors liable for criminal and civil penalties. Specifically, under Section 404 of the Sarbanes-Oxley Act, executives must certify and demonstrate that they have established and are maintaining an adequate internal control structure and procedures for financial reporting.</td>
</tr>
<tr>
<td>General</td>
<td>ISO 17799, ISO 27001, and ISO 27002 international security standards.</td>
</tr>
<tr>
<td>GPG13</td>
<td>Good Practice Guide 13 (GPG13), a mandatory aspect of CoCo compliance.</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Health Insurance Portability and Accountability Act (HIPAA), which requires national standards for electronic health care transactions.</td>
</tr>
</tbody>
</table>
View LEM report properties

In the reports grid, select a report, and then click Report Properties. A dialog box appears with information about your report.

Filter and sort LEM report lists in the reports application

Use the Reports window to filter your report list and display only those reports associated with a particular report title, category, level, or type. You can also apply more than one filter at a time to display a very small subset of the report list. If required, you can create your own custom filter, and save them for later use.

Each report list column header includes a drop-down list that displays column filter options, as shown below.

For example, selecting Audit reduces the list to show only the reports associated with the Audit category.
When you apply a filter, a yellow status bar appears below the reports list. The status bar lists which filters are currently applied. You can use this list to remove each filter individually, or to remove them all at once.

Filter the report list to reduce the number of listed reports

1. Decide which column you want to use for the filter.
2. Click \(\checkmark\), and then select a filter option.
   
The report list refreshes to display the filtered list.
3. Repeat the previous step for each additional filter you want to apply.

Change a filter setting

In the status bar below the report list, click \(\downarrow\) and select a different filter option from your list of most commonly-used filters.

Sort the report list

You can sort the report list by clicking the column headers. This sorts the entire report list by the contents of your selected column in either ascending or descending order.

- The column header appears \(\uparrow\) indicating the report list is sorted by this column in ascending order.
- Click the column header again to reverse-sort the report list in descending order. The column header appears \(\downarrow\) indicating the report list is sorted by this column in descending order.
Turn off report filters

In the Reports window, when you are finished with a report filter, you can turn it off. Turning off a filter refreshes the report list so that it displays the list without that column filter. You can turn off a single filter or all of the filters at once.

To turn off a filter, clear the check box next to the filter in the status bar.

To turn off all of the filters, click ✗ in the status bar. The report list refreshes to display the list without any filters.

Manage report categories

Use the Manage Categories form to select reports from several industries, including Federal, Education, and Healthcare. You can search for specific reports and add reports to your Favorite Reports list.

Using the Industry Setup tab, you can select the industries and areas of regulatory compliance related to your company. Reports related to the options you select display in the Industry Reports list.

The Favorites Setup tab includes a search option to list, sort, and group the report list by industry and regulatory area. It highlights reports currently listed in your Favorite Reports list and allows you to add new reports to the list.

The tab also includes a Favorites tab that displays your current list of favorite reports. You can use this view to sort and group your favorite reports to locate a specific report. When needed, this view is also used to remove a report from your list of favorites.
Create a favorite LEM reports list

You can access frequently-used reports by adding them to the Favorite Reports list. This list can include both standard and custom reports. To create a favorite reports list, search the reports and then add your selections to your Favorites list.

Each authorized reports application user can set up a list of favorite reports. Each list is unique to the user logged in to the console. A reports application user is determined by the user's Windows account. If two users on the same computer log in to the same account, they will share a list of favorites.

Step 1: Search the reports

1. Open the LEM reports application. See Open the LEM reports application for steps.
2. On the Settings tab, click Manage, and then select Manage Categories.
3. Click the Favorites Setup tab.
4. Click the Search tab.

The Classifications section lists industries and regulatory areas supported by standard Reports. The Reports Matching Search Criteria box lists all standard SolarWinds report. If a report appears highlighted in green, the report is in your Favorite Reports tab.

5. In the Classifications section, select each industry or regulatory area related to your company.
6. Click Search.

The Reports Matching Search Criteria section displays all standard reports that support your options.

For example, if you select Finance, Search lists reports associated with Finance. If you selected Finance and PCI, Search lists every report that is associated with either Finance or PCI.

You can organize the report list by sorting, filtering, and grouping the report list.
Step 2: Add a report to your Favorites tab

1. In the report list, locate a report to save to the Favorite Reports list.
2. Right-click the report, and then select Add to Favorites.
3. Click Apply.

The report is saved to your Favorites list.

Remove a report from the Favorites tab

When you remove a report from the Favorite Reports list, the report remains in its original category. It is not deleted from the reports application.

1. Open the LEM reports application. See Open the LEM reports application for steps.
2. On the Settings tab, click Manage, and then select Manage Categories.
3. Click the Favorites tab.
4. Select a report, and then click Remove From Favorites.
5. Click Apply.

The report is removed from the Favorites tab.

Search LEM reports for specific text

The Reports window includes a search tool in the View tab to search for key words or phrases in text-based reports.
This tool only works when you are viewing a text-based view of a report in the Preview pane. You cannot use this tool with graphical-only reports, or the default graphical view that is displayed when you first run the report.

View the text-based details of a report

In the View tab, click the tree button to open the subtopics in the reports list. Click the content-based subtopic to jump to that section of the report.

Use the Search tool

1. In the Reports window, open or run the report you want to view.
   The report appears in the Preview pane.
2. Display the text-based details you want to search in the Preview pane.
3. In the View tab, click Search.
   The Find form appears.
4. In the Find what box, type the text you want to search for.
5. Select Match whole word only to search for entire words that match, omitting matching letters within words.
6. Select Match case to make the search sensitive to uppercase or lowercase letters.
7. In the Direction area, select Up to search from where you are now to the start of the document.
   Select Down to search from where you are now to the end of the document.
8. Click Find Next.
   The tool locates the next instance of the text in the report and highlights it for easy viewing.
9. Continue clicking Find Next for each remaining instance of the text you want to find.
10. To close the Search form, click Cancel.

Customize and share report filters in the LEM reports application

This section describes how to create custom reports using multi-column filters, and share your custom reports with other users.
Create a custom report filter in the LEM reports application

1. In the Reports window, click the report filter you want to use as a starting point.
2. At the bottom of the filter, click Customize.
   The Filter Builder form displays.
   In this example, the filter displays reports where the Category column equals Audit and the Type column equals Authentication.

   ![Filter Builder Form](image)

3. Click the options in the form to select the column, column option, and specific conditions that define the filter.
4. To apply the filter, click OK or Apply.

Save a custom report filter in the LEM reports application

1. Create a custom report filter. See [Create a custom report filter in the LEM reports application](#) for details.
2. Click Save As, and then select the folder where you want to store the file.
3. In the File name box, enter a filter name.
4. Click Save.

The filter is now saved and available for later use.

Open a saved custom report filter in the LEM reports application

1. Click Customize.
2. In in the Filter builder form, click Open.
3. From the Look in drop-down list, locate and open the filter.

4. In the Filter Builder form, click OK or Apply.

The custom filter is applied to the report list.
Categorize and display LEM reports by group

You can sort the report list into groups of reports by dragging one or more column headers into the grouping box. This allows you to quickly organize and display groups of reports that fall into very specific categories. For example, to group reports by category, drag the Category column header from the report list into the grouping box.

You can rearrange the report list into groups defined by items from the Category column, as shown below.

Groups change the report list into a series of nodes. There is a separate node for each unique item or category from the column that defines the grouping. The nodes are alphabetized, and each node is named by the column and category that defines the grouping.

For example, the Category column that defines the grouping in the example above includes three unique categories: Audit, Security, and Support. Grouping by the Category column creates three nodes: Category: Audit, Category: Security, and Category: Support. Opening a particular node displays only the reports associated with the particular grouping configuration.

You can group reports by any column header in the report list (such as Title, Category, Level, and Type). You can also create sub-groups to create parent-child hierarchies. For example, you could create a Category group and a Type sub-group.

Create a report group in the LEM reports application

To create a report group, decide which column defines the report groupings.
Next, drag the column header into the area above the Reports Title column. In this example, the Category header was dragged to the area above the Reports Title column. The report list now displays a separate node for each unique item that is in the column that is defining the grouping. The nodes are alphabetized and labeled for easy reference.

View the reports within a group in the LEM reports application

Click a node to display a list of reports that fall within that grouping. To close the node, click it again.

Create a sub-group in the LEM reports application

1. Drag another column header into the Drag a column header here to group by that column area.

2. Perform one of the following steps:
   - Place the new column header above the existing header to have the new header act as the primary grouping. In the example shown above, the report list would be grouped by Level and then Type.
   - Place the new column header below the existing header to have the new header act as the secondary grouping. In the example shown above, the report list would be grouped by Type and then Level.

The report list refreshes to display two levels of nodes—one level of nodes for the primary group, and one set of nodes for the secondary group.
3. To view the reports within a particular grouping, click a higher-level group node, and then a sub-group node.

   The report list displays only those reports that apply to both groupings.

4. Repeat Steps 1 and 2 for each additional grouping you require.

## Run a LEM report on-demand or schedule a LEM report to run later

This section describes how to run a LEM report on-demand, as well as schedule reports to run automatically. This section also documents how to run the default LEM Batch Reports using Windows Task Scheduler.

### Run an on-demand report in the LEM reports application

1. Open the LEM reports application. See [Open the LEM reports application](#) for steps.

2. On the Settings tab, click the Data Source drop-down menu and select a LEM Manager instance (the IP address or hostname of your LEM VM).

3. From the Category drop-down list, select a report category filter—for example, Audit (Optional).

4. Select a report title, and then click Run in the toolbar.
5. Select your start and end date and time parameters, and then click OK.

![Parameter Fields: Start Date/Time and End Date/Time]

The report appears in the View tab.

ℹ️ This process may take several minutes to complete.

![Graph showing number of events]

6. To send the report to a local or network printer, click Print.

7. To export the report to the appropriate format (such as a PDF or a Microsoft Word document), click Export.
Create a scheduled report in the LEM reports application

The following list provide an overview of the report scheduling process. Each step is described in greater detail in the subsections that follow.

1. Open the LEM reports application. See Open the LEM reports application for steps.
2. Select the report that you want to schedule, and then click Schedule.
3. Name the scheduled task to distinguish it from other similar tasks.
4. Set the schedule parameters.
   This states when the scheduled report runs.
5. Apply any advanced scheduling options.
6. Define when the system can and cannot run the task.
7. Apply the scheduled report to the data source (Manager) for which you want a report. Then define the scope, which is the period you want to the report to cover.
   When the system runs the report, it retrieves any pertinent events that occurred within the period defined by the scope.
8. Select any export options for the report.
   This allows you to export to the folder of your choice, and in a format that is easy to read and print. If you do not export the report, it will automatically print to your default printer.

Repeat this process for each report you want to schedule.

You can create more than one schedule for the same report. This allows you to run the same report on different LEM Managers or run the same report in different intervals (such as daily, weekly, or monthly), each with a different scope.

Step 1: Selecting the report you want to schedule

In this step, you will select the report you want to schedule, and then open the Report Scheduler Tasks window.

1. Open the LEM reports application. See Open the LEM reports application for steps.
2. On the Settings tab, click the Category drop-down menu and select a report category
   The report list displays all saved reports in the category.
3. In the Report Title column, locate the report you want to schedule.
4. Right-click the report, and then select Schedule Report.
   The Report Scheduler Tasks window appears.
5. Add, edit, and delete your scheduled report tasks.

**Step 2: Add a new scheduled report task**

Name and configure the new scheduled task associated with this report.

1. In the Reports Scheduler Tasks window, click Add.
2. Enter a name for the report, and then click OK.
3. Verify that the path in the Run field is correct. Click Browse and select the correct path, if required.
4. Verify that the user name in the Run as field is correct.
   To change the user path, use the following format:
   [Domain]\[UserName].
5. To set up a password for the current user to run the report, click Set password.
6. To run the scheduled task using the schedule you select in the Schedule tab, select the Enabled check box.
   To disable the schedule, clear the check box.
7. To save your changes, click Apply.
8. Complete the Task tab as described in the table.
9. To save your changes, click Apply.

**Step 3: Schedule the report**

Create the report schedule. The settings on the Schedule tab tell the system when to run the report.

You can create multiple schedules for each report that is within the same scope. For example, you can run an event summary report for the current week and display the running total for the week at each hour. When completed, you can set the report to Week: Current and have multiple schedules that run on an hourly schedule and on a twice-daily schedule.

1. Click the Schedule tab.

   - For new tasks, the tab states that the task is not scheduled.
2. To create a new report schedule, click New.

3. Complete the Schedule tab selections.

4. To save your changes, click Apply.

   The new report schedule appears in the list box near the top of the tab.

Step 4: Select the advanced scheduling options

If you clicked Advanced in the Schedule tab, the Advanced Schedule Options dialog box appears. You can schedule start and end dates for the report, or set a task to repeat for a set period of time.

1. In the Schedule tab, click Advanced.

2. Select the start and end dates.

3. To start running repeated tasks, select the Repeat task check box.
4. In the Until section, select the time or how long you want the task to run.

By limiting the task run time, you can prevent the task from running continuously if a problem should occur.

5. Select if the task is still running, stop it at this time to stop the system from running a report when the Time or Duration setting occurs. Clear this check box to have the system finish running a report that overlaps the Time or Duration setting.

The following illustration displays the valid and invalid date formats for reports.

<table>
<thead>
<tr>
<th>Valid</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>d/M/yy</td>
<td>d-M-yy</td>
</tr>
<tr>
<td>dd/M/yy</td>
<td>d-M-yy</td>
</tr>
<tr>
<td>d/MM/yy</td>
<td>d-MM-yy</td>
</tr>
<tr>
<td>d/M/yyyy</td>
<td>d-M-yyyy</td>
</tr>
<tr>
<td>dd/M/yyyy</td>
<td>d-M-yyyy</td>
</tr>
<tr>
<td>d/MM/yyyy</td>
<td>d-MM-yyyy</td>
</tr>
<tr>
<td>N/d/yy</td>
<td>M-d-yy</td>
</tr>
<tr>
<td>MM/d/yy</td>
<td>MM-d-yy</td>
</tr>
<tr>
<td>N/dd/yy</td>
<td>M-dd-yy</td>
</tr>
<tr>
<td>N/d/yyyy</td>
<td>M-d-yyyy</td>
</tr>
<tr>
<td>MM/d/yyyy</td>
<td>MM-d-yyyy</td>
</tr>
<tr>
<td>N/dd/yyyy</td>
<td>M-dd-yyyy</td>
</tr>
<tr>
<td>dd/MM/yy</td>
<td>dd-MM-yy</td>
</tr>
<tr>
<td>MM/dd/yy</td>
<td>MM-dd-yy</td>
</tr>
<tr>
<td>dd/MM/yyyy</td>
<td>dd-MM-yyyy</td>
</tr>
<tr>
<td>MM/dd/yyyy</td>
<td>MM-dd-yyyy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Invalid</th>
<th>Invalid</th>
</tr>
</thead>
<tbody>
<tr>
<td>ddd/M/yy</td>
<td>ddd-M-yy</td>
</tr>
<tr>
<td>ddd/MM/yy</td>
<td>ddd-MM-yy</td>
</tr>
<tr>
<td>ddd/MMM/yyyy</td>
<td>ddd-MM-yyy</td>
</tr>
<tr>
<td>ddd/MM/yyyy</td>
<td>ddd-MM-yyyy</td>
</tr>
<tr>
<td>MMM/d/yy</td>
<td>MMM-d-yy</td>
</tr>
<tr>
<td>MMM/dd/yy</td>
<td>MMM-dd-yy</td>
</tr>
<tr>
<td>MMM/dd/dd/yy</td>
<td>MMM-dd-dd-yyyy</td>
</tr>
<tr>
<td>MMM/dd/yyyy</td>
<td>MMM-dd-yyyy</td>
</tr>
</tbody>
</table>

In this example, the configured report runs every four hours, starting on Monday, August 18, and running through Sunday, August 30. Each time the task runs, the system will stop it if it continues to run for more than one hour.

6. To save your changes and exit the form, click OK.

You return to the task scheduler form.
Step 5: Stating when the system can or cannot run the task

Use the Settings tab to select when the system can and cannot run the task.

1. Click the Settings tab.
2. Complete the selections as required.

3. To save your changes, click Apply.
4. To close the task scheduler form and return to the Report Scheduler Tasks window, click OK.
Step 6: Assign the data source and scope

Assign the task to a particular data source (or Manager) and define the task scope (the period you want the report to cover). When the system runs the report, it retrieves any relevant events that occurred within the period defined by the scope.

1. Select the report schedule you want to assign.

![Report Scheduler Tasks](image)
![Report Execution Settings For Selected Task](image)

2. Click Load to View or Edit.
   
   *The Report Execution Settings For Selected Task section is enabled.*

3. Use this section to configure the report execution settings for the task (report schedule) you selected above.

4. Use the Select the report data source list to select the Manager or to which you want to assign this task.

   > You can only assign a task to a single Manager. If you need to assign a similar or identical task to a second Manager, create a new task.
Assign the task scope

In the Report Scope section, set up the task scope for this data source. The scope is the event period (or time frame) for the events you want the report to cover.

1. From the Date Range drop-down list, select the date range you want the report to cover for this task and data source.
   
   In this example, the date range is Day: Today. The report will cover the period from 12:00:00 AM to 11:59:59 PM of the current date.

   If you select Week: Previous, the scheduled report will contain information from the last full week—from 12:00:00 AM the last Monday to 11:59:59 PM the last Sunday. For example, if today is Wednesday the 11th, the task runs from 12:00:00 AM on the 2nd to 11:59:59 PM on the 8th.

   Select one of the following date ranges:

   - Day: Today: Run for the specified time frame on the current (today's) date.
   - Day: Yesterday: Run for the specified time frame on the previous (yesterday's) date.
   - Week: Current: Run from one week ago to the current time.
   - Week: Previous: Run from 12:00:00 AM last Monday to at most 11:59:59 Sunday. This report will capture the last full week of data.
   - Month: Current: Run from one month ago to the current time.
   - Month: Previous: Run from 12:00:00 AM on the first of the month until 11:59:59 PM on the last day of the month. This will report will capture the last full month of data.
   - User Defined: Run another report scope. Use this option to schedule reports for arbitrary periods or periods that are outside of the conventional scope of a day, week, or month.

2. Enter or select a start time and end time for reporting events that occurred on this Manager. The report will only show those events that occurred on the Manager within this period.

   If you select a week or month scope, you cannot edit the Start and End date and time fields.

3. To configure the report so it automatically exports to a file, go to the next step. Otherwise, click Save.
   
   The Count Settings area only applies to count-based reports, such as Top 20 reports.

4. In the Number of Items box, type or select the number of items you want the report to track.
Step 7: Export a scheduled report

You can enable the report utility to automatically export a scheduled report in PDF format to a specific folder. Otherwise, the system will send the report to your default printer.

1. Open the Report Scheduler Tasks window.
2. Select the scheduled report task you want to export in the Task Description box.
3. Select the Export check box in the Report Settings tab to name and export this report when the task scheduler runs this report.

![Image of Export settings]

4. From the Format drop-down list, select a file format for the exported report.
5. Click the folder icon, locate the folder where you want to save the report, and a unique file name for the report.
   
   If the report has multiple schedules, give each scheduled report a different name. Otherwise, the exported file names files will overwrite each other or increment according to the If File Exists setting.
6. In the If File Exists list, choose one of the following options:
   - Select Increment to store the new report along with any previous versions of the report in the folder. The reports application increments each report by appending the report file name with an underscore and a digit. For example, [FileName]_1.pdf.
   - Select Overwrite to have each new version of the report overwrite the previous version of the report in the folder.
7. Click Save.
8. Click Close to close the Report Scheduler Tasks window and return to the Reports window.
9. Repeat Step 2: Adding a new scheduled report task through Step 7: Export a scheduled report for each report you want to schedule and assign to a particular data source.

Remove a report from the report scheduler

1. Open the LEM reports application. See Open the LEM reports application for steps.
2. Click the Settings tab.
3. From the Category drop-down list, select Standard Reports or Custom Reports.
   
   The grid displays all reports in your selected category.
4. In the Report Title column, click the name of the scheduled report for which you want to delete the task schedule.
5. Click Schedule.
6. In the Report Scheduler Tasks window, select the scheduled report in the Task Description list that
includes the schedule you want to delete.

7. Click Modify.
   The task schedule form appears.

8. In the Task Schedule window, click the Schedule tab and select the Show Multiple Schedules check box.

9. In the schedule list, select the schedule you want to delete, and then click Delete.

10. To close the Report Scheduler Tasks form, click Close.

## Configure Windows Task Scheduler to run the default LEM Batch Reports

The LEM reports application includes a default batch set of .ini files used to schedule reports. These files contain the configurations necessary to schedule several best-practice reports on either a daily or weekly basis, depending on the scope.

### Prepare the INI file

Modify the default .ini files in the LEM reports installation directory to specify the hostname of the LEM Manager or LEM database in your environment, and the export destination for your scheduled reports.

To modify the default INI files:

1. Navigate to the LEM Reports installation directory and open the SchedINI folder:
   - **On 32-bit computers**: C:\Program Files\SolarWinds Log and Event Manager Reports
   - **On 64-bit computers**: C:\Program Files (x86)\SolarWinds Log and Event Manager Reports

2. Open each of the BRPT*.ini files and make the following changes in a text editor:
   - Replace the default value next to Manager1 with the hostname of the LEM Manager or database appliance in your environment. Use the hostname of your LEM database appliance if you have a dedicated appliance to store your normalized LEM alert data.
   - Modify the ExportDest file path if you want to customize the location to which LEM Reports saves the exported reports. The default file path is %ProgramFiles%\SolarWinds Log and Event Manager Reports\Export.

3. Save your changes and close the files.

### Schedule the Reports to Run using Windows Task Scheduler

Schedule your batch reports to run using Windows Task Scheduler. Complete the following procedure twice: once for the daily reports and once for the weekly reports.

1. Create a new scheduled task by opening Control Panel > Administrative Tools > Task Scheduler.
2. Select Task Scheduler Library.
3. In the Actions pane, click Create Basic Task.
4. Enter a name for your task that reflects the frequency of the scheduled task. For example, enter LEM Reports - Weekly for the weekly task, and then click Next.

5. Select Daily or Weekly, depending on what batch of reports you are scheduling, and then click Next.

6. Set the start time and frequency for your scheduled reports, and then click Next.
   - For the daily task: 1 AM, Recur every 1 Day
   - For the weekly task: 3 AM, Recur every 1 week, Monday

7. Select Start a program, and then click Next.

8. For the Program/script field, click Browse to browse for SWLEMReports.exe. See Step 1 in Prepare the INI file for the default installation paths.

9. In the Add arguments (optional) field, enter the following, according to the task being created:
   - Use the %ProgramFiles(x86)% environment variable on 64-bit computers.
   - The /l at the beginning of the additional argument is optional. This generates a log file called SWLEMReports.log when Task Scheduler runs your task. The file is saved in %ProgramFiles%\SolarWinds Log and Event Manager Reports.

10. For the daily task: /l "%ProgramFiles%\SchedINI\BATCHDay.ini"

11. For the weekly task: /l "%ProgramFiles%\SchedINI\BATCHWeek.ini"

12. Click Next.

13. To verify the task details on the Summary dialog, select Open the Properties dialog for this task when I click Finish, and then click Finish.

14. To change the user account the task scheduler should use to complete the task, click Change User or Group.

   - Provide a user with administrator level permissions.
   - If you specified a network location in Step 2 in Prepare the INI file, provide a user with write permissions to that folder.
   - Use a service account to avoid having to maintain the task according to your password change policy.

15. On the Properties window, select Run whether user is logged on or not.

16. Select Run with highest privileges.

17. Select the appropriate operating systems in the Configure menu, and then click OK to save your changes and exit the Properties window.

18. Enter the Windows password for the user specified for this task, and then click OK.

**Default Report Schedules**

Once configured, the scheduled tasks run and export the following reports:

**Daily Reports**

- EventSummary.pdf
- SubscriptionsByUser.pdf
Weekly Reports

- MaliciousCode.rpt
- NetSuspicious.rpt
- NetAttackAccess.rpt
- NetAttackDenial.rpt
- Authentication.rpt
- FileAudit.rpt
- MachineAudit.rpt
- ResourceConfiguration.rpt

You can open reports with the .rpt extension in the LEM reports application for filtering and exporting. If you have a program like Crystal Reports associated with this file format, you can access these reports with the LEM reports application by opening LEM Reports first and then clicking Open on the Settings tab.

If you create a scheduled report, you can remove the task from Windows task scheduler, and the .ini file will still be under the SchedINI directory. You can change the name of the RPTxxxxx-x.ini to BRPTxxxxx-x.ini, and add the file to the BatchDay.INI or the BatchWeek.INI.

Edit a scheduled report in the Task Scheduler

When you create custom and scheduled reports, SolarWinds recommends that you document your procedures for disaster recovery.

The scheduled Report INI files are located in: Program Files\SolarWinds Log and Event Manager Reports\SchedINI. These report INI files are generated automatically when you schedule a report in the LEM console. If you need to edit an INI file or change a report format, add the corresponding report format after the equal sign to the line containing "ExportFormat= ".

The following table identifies the number assigned to each possible format for a LEM report.

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>REPORT FORMAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Excel: MS Excel 97-2000, with headings format</td>
</tr>
<tr>
<td>2</td>
<td>Exceldata: MS Excel 97-2000, data only format</td>
</tr>
<tr>
<td>3</td>
<td>HTML32: HTML version 3.2 format</td>
</tr>
<tr>
<td>4</td>
<td>HTML40: HTML version 4.0 format</td>
</tr>
<tr>
<td>5</td>
<td>PDF: Adobe Portable Document format</td>
</tr>
<tr>
<td>6</td>
<td>RTF: Rich Text Format</td>
</tr>
<tr>
<td>7</td>
<td>CSV: Separated Values Text format</td>
</tr>
</tbody>
</table>
Below is an example of a LEM scheduled report INI file:

```
[TaskSetup]
Keyword=2009331
Filename=C:\Program Files\SolarWinds Log and Event Manager Reports\Reports\RPT2009-33-1.rpt
[DSNManager]
Manager1=sherman
[RptParams]
RptDateRangeDesc=DAY_P
RptDateRange=2
RptStartTime=12:00:00 AM
RptStopTime=11:59:59 PM
TopN=20
[Export]
DoExport=T
ExportDesc=EXCEL
ExportFormat=1
ExportDest=C:\Program Files\SolarWinds Log and Event Manager Reports\Export
ExportFileName=format1.xls
ExportOverWrite=INCREMENT
```

Create a custom LEM report

This section describes how to customize a LEM report.

💡 To view a tutorial about filtering and exporting LEM Reports, see: [http://video.solarwinds.com/watch/pMuk9eqsTPtja99u4EUvrx](http://video.solarwinds.com/watch/pMuk9eqsTPtja99u4EUvrx)
Create a custom report in the LEM reports application

If you want to report about a specific event (such as a user logon failure), you can create a custom report that reports on a specific field. Using the left menu in the reports application to select the field for your report.

1. Run a report. See Run an on-demand report in the LEM reports application for help.
   The report opens on the View tab.

2. In the left column of the report, select the field you want to query.

3. On the View tab, examine the report to identify the value you want to use in your filter.

4. Click Select Expert.
   The Select Expert dialog box opens.

5. Click New.
   The Fields dialog box opens.

6. Select a field to report on, and then click OK.
7. From the Boolean drop-down list, select your comparison value.

8. Select or enter a second value. Click New to select or enter additional fields and expand your query.

9. Click OK.

Select Expert filters out only the information in your query.

All fields are listed as column labels across the top. You can also mouse over data to display the reported field.

10. To print your report, click Print.

11. To export your report to a PDF, Word Document, or other format, click Export.

Export and save a copy of the filtered LEM report with a new name

1. Create and run the custom report. See Create a custom report in the LEM reports application for help.
2. On the View tab, click Export.
   The Export dialog box opens.

3. Select Crystal Reports (RPT) from the Format menu.
   Leave Destination set to Disk file, and then click OK.

4. In the Save File window, navigate to the following folder:
   C:\Program Files (x86)\SolarWinds Log and Event Manager Reports\CustomReports
   This is the default location for 64-bit operating systems. If you are using a 32-bit operating system, the default folder would be C:\Program Files\SolarWinds Log and Event Manager Reports\CustomReports.

5. In the File name field, type a name for your filtered report to identify the report by the file name under Custom Reports

6. Click Save.

Open a custom report in the LEM reports application

1. Open the LEM reports application. See Open the LEM reports application for steps.

2. In the Reports window, click the Settings tab.

3. In the Category list, select Custom Reports.

4. On the Quick Access toolbar, click the Refresh Report List icon or press F5.
   When the refresh completes, the new custom report appears in the list, and displays any changes made to its Properties.

5. Launch your custom report for any time frame.

Use the Select Expert tool to create a more focused LEM report

The Select Expert tool lets you execute queries to create a smaller, more focused report from a larger text-based report.

You can use this tool when you are viewing the text-based view of a report in the Preview frame. You cannot use this tool with the default graphical view displayed when you first run the report.

To View the text-based details of a report, check that the View tab is open and click the tree button to open the subtopics in the reports list. Click the content-based subtopic to jump to that section of the report.

If using the Select Expert to filter report data by date or time fields (such as InsertionTime or DetectionTime) results in an error, clear the error prompt, return to the Select Expert, and delete the time-based filter. To filter by time and date, you must run the report with the specified range.
View the text-based details of a report

In the View tab, click the tree button to open the subtopics in the reports list. Click the content-based subtopic to jump to that section of the report.

Run a report query using the Select Expert tool

1. Run a report. See Run an on-demand report in the LEM reports application for help.
   The report opens on the View tab.
2. On the View tab, locate the View group, and then click Select Expert.
3. Click either the New button or the <New> tab.

![Select Expert dialog box with New button and <New> tab]

The Fields form appears with the various report fields you can query on this report.

![Fields form with list of available fields]

Click Browse to display a list of available fields you can select with the tool.

4. Select the field you want to query, and then click OK.
   The Select Expert form appears.
The first tab displays your selected field name. It lists the query options for that field and includes an adjacent list where you can select a specific value.

5. From the left drop-down list, select a query option for the field.
6. From the adjacent drop-down list, select a specific value for the field.

You can click Browse Data to view a complete list of values in the report for that field. From the Browse Data box, you can select a value, and then click Close to apply that value to the query.

7. Repeat Steps 3 – 6 for each field you want to add to the query.
8. To close the form and apply the query, click OK.

The new report appears in the Preview frame.

You can use the Preview frame's toolbar to save or export the report.

**Restore the original report after using the Select Expert tool**

When you are through querying a report with the Select Expert tool, you can restore the report to its original state.

To turn off the Select Expert settings:

1. On the View tab in the View group, click Select Expert.

   The Select Expert form appears.
2. To remove the query options, click Delete.
3. Click OK.
   The original report appears in the Preview frame.

Manage LEM reports: Open, print, and more

This section describes how to manage LEM reports in the reports application.

Open your saved reports

Whenever a report is saved or exported to RPT format, you can use the Open command to reopen and view the report contents. This applies to scheduled reports that the system ran and saved, as well as on-demand reports that you ran and exported for later viewing.

1. Open the LEM reports application. See Open the LEM reports application for steps.
2. Click the Menu button, and then select Open Report.
   The Open Report File form appears.
3. Use the Open Report File form to locate the report file you want to view.
   If you cannot locate the report, be sure you selected Crystal Reports (*.rpt) in the File type list.
4. Select the file and click Open.
   The report opens in the Reports Preview pane.
View the master report sections

Some standard reports are master reports. A master report is a report that includes a series of subtopics, where each subtopic contains a specific set of details about the higher-level master topic. Together, these topics create the report, similar to chapters in a book.

When a report includes more than one subtopic, a subtopic pane appears in the Preview pane. The subtopic pane lists the subtopics found in the report. If you click a subtopic, the Preview pane displays the first page of that section of the report.

To view a section of a master report, select the subtopic you want to review. The Preview pane displays the first page of that section in the report.

Hide and show a master report subtopic pane

When you preview a master report, Tree is enabled in the View tab. Click Tree to toggle between hiding and revealing the report’s subtopic pane.
You can hide the subtopic pane in the View group by clicking Tree. The subtopic pane is hidden, as shown below.

To restore the subtopic pane, click Tree again. The subtopic pane appears again.
View the report pages

In the reports application, the Navigate group provides tools to browse through the pages of a multi-page report. If the report includes only one page, the toolbar is disabled.

Click \( \text{Previous} \) or \( \text{Next} \) to move to the first or last page of the report. Click \( \text{Previous} \) or \( \text{Next} \) to move to the previous or next page of the report.

The Page field displays the page number currently active in the Preview frame, as well as the total number of pages in the report. A plus (+) next to a page number indicates additional pages in the report.

To determine how many pages are in the report, click \( \text{Last Page} \) in the toolbar. This takes you to the last page of the report, forcing the console to determine how many pages there are. It also causes the + to display the actual number of pages.

You can also use this feature to display a particular page of the report. In the Page box, enter a page number you want to view and press Enter. The Preview frame displays your selected page.

Magnify and reducing report pages

Use the Zoom feature to resize a report. You can select a percentage or have the report expand or reduce to fit the Preview pane. Click the Zoom drop-down menu and select an option to resize your report in the Preview pane.
Stop a report in progress

To stop running or loading a report that is progress, click Stop on the status bar.

Edit a scheduled report task

When required, you can edit a scheduled report task or task schedule by editing the task settings. This process allows you to modify your report scheduling when conditions change within your organization.

1. Open the Reports application. See Open the LEM reports application for steps.
2. Click the Settings tab.
3. From the Category drop-down list, select Standard Reports or Custom Reports.
4. In the Report Title column, select the report that requires a schedule change, and then click Schedule.
5. In the Report Scheduler Tasks window, select the report schedule you want to edit, and then click Modify.
6. In the Scheduler window, edit the Task, Schedule, and Settings tabs as required.
   To change the settings for a particular schedule, click the Schedule tab and select the schedule you want to change. Use the boxes to change the settings, and then click Apply.
7. To close the window, click OK.
8. Make any additional changes to the Report Settings as required in the Report Schedule Tasks window.
9. Click Save.
10. To close the Report Scheduler Tasks window, click Close.
Export a report

You can export a report from the Preview pane into several formats, including:

- Adobe Portable Document File (PDF)
- Crystal Reports RPT file
- HTML
- Microsoft Excel file

LEM officially supports PDF and RPT formats.

1. In the Reports window, open or run the report you want to export.
   The report appears in the Preview pane.
2. On the View tab in the Output group, click Export.
   The Export form appears.

3. In the Format list, select the fine type to save the report.
   The Description box at the bottom of the form describes your selected file format.
4. Use the Destination list to browse to the folder and save the file.
5. Click OK.
   The system saves the file in your selected format to your destination folder.
Print reports

You can print any report displayed in the Preview pane.

1. In the Reports window, open or run the report you want to print.
   The report appears in the Preview pane.
2. On the View tab, click Print in the Output group.
3. In the Print form, select the printer and any print options.
4. Click Print.
   The report is sent to your printer based on your print options.

Set up your printer preferences

Use the Printer Setup command to define the default print settings (such as Portrait or Landscape) for printing your reports.

1. In the Reports window, open or run the report you want to print.
   The report appears in the Preview pane.
2. On the View tab, click Printer Setup in the Preferences group.
3. In the Page Setup dialog box, select the appropriate options.
4. Click OK.
   The report is printed according to your selected print options.
Default reports included with LEM

This section describes the reports included with LEM and suggests how often to run each report.

Scheduling terminology used in this topic

This section describes the scheduling terminology used in the reports table.

<table>
<thead>
<tr>
<th>SCHEDULE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>Run and review this report once each day.</td>
</tr>
<tr>
<td>Weekly</td>
<td>Run and review this report once each week.</td>
</tr>
<tr>
<td>As needed</td>
<td>SolarWinds suggests that you run these reports only when needed for specific auditing purposes, or when you need the details surrounding a Priority event or a suspicious event.</td>
</tr>
<tr>
<td>As requested</td>
<td>These reports are diagnostic tools and should only be run at the request of SolarWinds' technical support personnel.</td>
</tr>
</tbody>
</table>

Audit reports included with LEM

The following table lists and describes each audit report, listed alphabetically by title.

<table>
<thead>
<tr>
<th>TITLE</th>
<th>DESCRIPTION</th>
<th>FILE NAME</th>
<th>SCHEDULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Report</td>
<td>This report lists all authentications tracked by the SolarWinds system, including user logon, logoff, failed logon attempts, guest logons, and so on.</td>
<td>RPT2003-02.rpt</td>
<td>Weekly</td>
</tr>
<tr>
<td>Authentication Report - Authentication Audit</td>
<td>This report lists event events that are related to authentication and authorization of accounts and account “containers” such as groups or domains. These events can be produced from any network node including firewalls, routers, servers, and clients.</td>
<td>RPT2003-02-10.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - Suspicious Authentication</td>
<td>This report lists event events that are related to suspicious authentication and authorization events. These events include excessive failed authentication or authorization attempts, suspicious access to unauthenticated users, and suspicious access to unauthorized services or information.</td>
<td>RPT2003-02-9.rpt</td>
<td>As Needed</td>
</tr>
<tr>
<td><strong>TITLE</strong></td>
<td><strong>DESCRIPTION</strong></td>
<td><strong>FILE NAME</strong></td>
<td><strong>SCHEDULE</strong></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Authentication Report - Top User Log On by User</td>
<td>This report lists the Top User Log On events grouped by user name.</td>
<td>RPT2003-02-6-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - Top User Log On Failure by User</td>
<td>This report lists the Top User Log On Failure events grouped by user name.</td>
<td>RPT2003-02-7-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - SolarWinds Authentication</td>
<td>This report shows logon, logoff, and logon failure activity to the SolarWinds Console.</td>
<td>RPT2003-02-8.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - User Log Off</td>
<td>User Logoff events reflect account logoff events from network devices (including network infrastructure devices). Each event will reflect the type of device from which the user was logging off. These events are usually normal events but are tracked for consistency and auditing purposes.</td>
<td>RPT2003-02-5.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - User Log On</td>
<td>User Logon events reflect user account logon events from network devices monitored by SolarWinds (including network infrastructure devices). Each event will reflect the type of device that the logon was intended for along with all other relevant fields.</td>
<td>RPT2003-02-6.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - User Log On by User</td>
<td>This report lists all account logon events, grouped by user name.</td>
<td>RPT2003-02-6-1.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - User Log On Failure</td>
<td>User Logon Failure events reflect failed account logon events from network devices (including network infrastructure devices). Each event will reflect the point on the network where the user was attempting logon. In larger quantities, these events may reflect a potential issue with a user or set of users, but as individual events they are generally not a problem.</td>
<td>RPT2003-02-7.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - User Log On Failure by User</td>
<td>This report lists all account logon failure events, grouped by user name.</td>
<td>RPT2003-02-7-1.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td><strong>Description</strong></td>
<td><strong>File Name</strong></td>
<td><strong>Schedule</strong></td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Change Management - General Authentication Related Events</td>
<td>This report includes changes to domains, groups, machine accounts, and user accounts.</td>
<td>RPT2006-20.rp</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Domain Events</td>
<td>This report includes changes to domains, including new domains, new members, and modifications to domain settings.</td>
<td>RPT2006-20-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Domain Events - Change Domain Attribute</td>
<td>This report lists changes to domain type. These events are uncommon and usually provided by the operating system. Usually, these changes are made by a user account with administrative privileges, but occasionally a change will happen when local system maintenance activity takes place.</td>
<td>RPT2006-20-01-7.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Domain Events - Change Domain Member</td>
<td>This report lists event events that occur when an account or account container within a domain is modified. Usually, these changes are made by a user account with administrative privileges, but occasionally an event occurs when local system maintenance activity takes place. Events of this nature mean a user, machine, or service account within the domain has been modified.</td>
<td>RPT2006-20-01-4.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Domain Events - Delete Domain</td>
<td>This report lists event events that occur upon removal of a trust relationship between domains, deletion of a subdomain, or deletion of account containers within a domain. Usually, these changes are made by a user account with administrative privileges.</td>
<td>RPT2006-20-01-8.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Domain Events - Delete Domain Member</td>
<td>This report lists event events that occur when an account or account container has been removed from a domain. Usually, these changes are made by a user account with administrative privileges, but occasionally they occur when local system maintenance activity takes place.</td>
<td>RPT2006-20-01-3.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Change Management - General Authentication: Domain Events - Domain Member Alias</td>
<td>This report lists event events that happen when the alias for a domain member has been changed. This means an account or account container within a domain has an alias created, deleted, or otherwise modified. This event is uncommon and is used to track links between domain members and other locations in the domain where the member may appear.</td>
<td>RPT2006-20-01-5.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Domain Events - DomainAuthAudit</td>
<td>This report lists authentication, authorization, and modification events that are related only to domains, subdomains, and account containers. These events are normally related to operating systems. However, they can be produced by any network device.</td>
<td>RPT2006-20-01-1.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Domain Events - New Domain</td>
<td>This report lists event events that occur upon creation of a new trust relationship between domains, creation of a new subdomain, or creation of new account containers within a domain. Usually, these creations are done by a user account with administrative privileges.</td>
<td>RPT2006-20-01-6.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Domain Events - New Domain Member</td>
<td>This report lists event events that occur when an account or an account container (a new user, machine, or service account) has been added to the domain. Usually, these additions are made by a user account with administrative privileges, but occasionally they occur when local system maintenance activity takes place.</td>
<td>RPT2006-20-01-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Group Events</td>
<td>This report lists changes to groups, including new groups, members added/removed to/from groups, and modifications to group settings.</td>
<td>RPT2006-20-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Group Events - Change Group Attribute</td>
<td>This report lists event events that occur when a group type is modified. Usually, these changes are made by a user account with administrative privileges, but occasionally they occur when local system maintenance activity takes place.</td>
<td>RPT2006-20-02-6.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>TITLE</td>
<td>DESCRIPTION</td>
<td>FILE NAME</td>
<td>SCHEDULE</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Change Management - General Authentication: Group Events - Delete Group</td>
<td>This report lists event events that occur upon deletion of a new group of any type. Usually, these additions are made by a user account with administrative privileges.</td>
<td>RPT2006-20-02-5.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Group Events - Delete Group Member</td>
<td>This report lists event events that occur when an account or group has been removed from a group. Usually, these changes are made by a user account with administrative privileges, but occasionally they occur when local system maintenance activity takes place.</td>
<td>RPT2006-20-02-3.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Group Events - Group Audit</td>
<td>This report lists authentication, authorization, and modification events related only to account groups. These events are normally operating system related, however could be produced by any network device.</td>
<td>RPT2006-20-02-1.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Group Events - New Group</td>
<td>This report lists NewGroup events. These events occur upon creation of a new group of any type. Usually, these additions are made by a user account with administrative privileges.</td>
<td>RPT2006-20-02-4.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Group Events - New Group Member</td>
<td>This report lists NewGroupMember events. These events occur when an account (or other group) has been added to a group. Usually, these additions are made by a user account with administrative privileges, but occasionally an event will occur when local system maintenance activity takes place. A new user, machine, or service account has been added to the group.</td>
<td>RPT2006-20-02-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td></td>
<td>This report includes changes to machine accounts, including enabling/disabling machine accounts and modifications to machine account settings.</td>
<td>RPT2006-20-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Change Management - General Authentication: Machine Account Events - Machine Disabled</td>
<td>This report lists MachineDisable events. These events occur when a machine account is actively disabled and/or when an account is forcibly locked out by the operating system or other authentication tool. These events are usually operating system related and could reflect a potential issue with a computer or set of computers.</td>
<td>RPT2006-20-03-3.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Machine Account Events - Machine Enabled</td>
<td>This report lists MachineEnable events, which reflect the action of enabling a computer or machine account. These events are normally related to the operating system, and will trigger when a machine is “enabled,” normally by a user with administrative privileges.</td>
<td>RPT2006-20-03-1.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: Machine Account Events - Machine Modify Attribute</td>
<td>This report lists MachineModifyAttribute events, which occur when a computer or machine type is changed. These events are uncommon and usually provided by the operating system.</td>
<td>RPT2006-20-03-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: User Account Events</td>
<td>This report includes changes to user accounts, including enabling/disabling user accounts and modifications to user account settings.</td>
<td>RPT2006-20-04.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: User Account Events - User Disabled</td>
<td>This report lists UserDisable events. These events occur when a user account is actively disabled and/or when a user is forcibly locked out by the operating system or other authentication tool. These events are usually related to the operating system and can reflect a potential issue with a user or set of users.</td>
<td>RPT2006-20-04-3.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - General Authentication: User Account Events - User Enabled</td>
<td>This report lists UserEnable events, which reflect the action of enabling a user account. These events are normally related to the operating system. They occur both when an account is unlocked after lockout due to unsuccessful logons, and when an account is “enabled” in the traditional sense.</td>
<td>RPT2006-20-04-1.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>TITLE</td>
<td>DESCRIPTION</td>
<td>FILE NAME</td>
<td>SCHEDULE</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Change Management - General Authentication: User Account Events - User Modify Attributes</td>
<td>This report lists UserModifyAttribute events that occur when a user type is changed. These events are uncommon and usually provided by the operating system.</td>
<td>RPT2006-20-04-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Network Infrastructure: Policy/View Change</td>
<td>This report includes accesses to network infrastructure device policy, including viewing or changing device policy.</td>
<td>RPT2006-21.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Group Created</td>
<td>This report includes creations of Windows/Active Directory groups.</td>
<td>RPT2006-22-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Group Deleted</td>
<td>This report includes deletions of Windows/Active Directory groups.</td>
<td>RPT2006-22-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Group Events</td>
<td>This report includes Windows/Active Directory group-related events.</td>
<td>RPT2006-22.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Group Property Updated</td>
<td>This report includes changes to Windows/Active Directory group properties, such as the display name.</td>
<td>RPT2006-22-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td><strong>Description</strong></td>
<td><strong>File Name</strong></td>
<td><strong>Schedule</strong></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Machine Events</td>
<td>This report includes Windows/Active Directory machine-related events.</td>
<td>RPT2006-23.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Machine Events - Account Created</td>
<td>This report includes creations of Windows/Active Directory machine accounts.</td>
<td>RPT2006-23-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Machine Events - Account Deleted</td>
<td>This report includes deletions of Windows/Active Directory machine accounts.</td>
<td>RPT2006-23-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Machine Events - Account Disabled</td>
<td>This report includes disables of Windows/Active Directory machine accounts.</td>
<td>RPT2006-23-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Machine Events - Account Enabled</td>
<td>This report includes enables of Windows/Active Directory machine accounts.</td>
<td>RPT2006-23-04.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td><strong>Description</strong></td>
<td><strong>File Name</strong></td>
<td><strong>Schedule</strong></td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Machine Events - Account Properties Update</td>
<td>This report includes changes to Windows/Active Directory machine account properties, such as the display name.</td>
<td>RPT2006-23-05.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Machine Events - Added To Group</td>
<td>This report includes additions of Windows/Active Directory machine accounts to groups.</td>
<td>RPT2006-23-06.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Machine Events - Added To OU</td>
<td>This report includes additions of Windows/Active Directory machine accounts to Organizational Units.</td>
<td>RPT2006-23-07.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Machine Events - Removed From Group</td>
<td>This report includes removals of Windows/Active Directory machine accounts from groups.</td>
<td>RPT2006-23-08.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: Machine Events - Removed From OU</td>
<td>This report includes removals of Windows/Active Directory machine accounts from Organizational Units.</td>
<td>RPT2006-23-09.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td><strong>Description</strong></td>
<td><strong>File Name</strong></td>
<td><strong>Schedule</strong></td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: New Critical Group Members</td>
<td>This report includes additions of Windows/Active Directory user accounts to critical groups, such as Domain or Enterprise Admins.</td>
<td>RPT2006-22-04.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: OU Events</td>
<td>This report includes Windows/Active Directory Organizational Unit-related events.</td>
<td>RPT2006-24.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: OU Events - OU Created</td>
<td>This report includes creation of Windows/Active Directory Organizational Units.</td>
<td>RPT2006-24-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: OU Events - OU Deleted</td>
<td>This report includes deletion of Windows/Active Directory Organizational Units.</td>
<td>RPT2006-24-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: OU Events - OU Properties Update</td>
<td>This report includes updates to Windows/Active Directory Organizational Unit properties, such as the display name.</td>
<td>RPT2006-24-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events</td>
<td>This report includes Windows/Active Directory user-related events.</td>
<td>RPT2006-25.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events - Account Created</td>
<td>This report includes creations of Windows/Active Directory user accounts.</td>
<td>RPT2006-25-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events - Account Deleted</td>
<td>This report includes deletions of Windows/Active Directory user accounts.</td>
<td>RPT2006-25-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events - Account Disabled</td>
<td>This report includes disables of Windows/Active Directory user accounts.</td>
<td>RPT2006-25-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events - Account Enabled</td>
<td>This report includes enables of Windows/Active Directory user accounts.</td>
<td>RPT2006-25-04.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events - Account Lockout</td>
<td>This report includes user-driven disables of Windows/Active Directory user accounts, such as a user triggering an excessive failed password limit.</td>
<td>RPT2006-25-05.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td><strong>Description</strong></td>
<td><strong>File Name</strong></td>
<td><strong>Schedule</strong></td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events - Account Properties Updated</td>
<td>This report includes changes to Windows/Active Directory user account properties, such as the display name.</td>
<td>RPT2006-25-06.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events - Added To Group</td>
<td>This report includes additions of Windows/Active Directory user accounts to groups.</td>
<td>RPT2006-25-07.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events - Added To OU</td>
<td>This report includes additions of Windows/Active Directory user accounts to Organizational Units.</td>
<td>RPT2006-25-08.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events - Removed From Group</td>
<td>This report includes removals of Windows/Active Directory user accounts from groups.</td>
<td>RPT2006-25-09.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Change Management - Windows/Active Directory Domains: User Events - Removed From OU</td>
<td>This report includes removals of Windows/Active Directory user accounts from Organizational Units.</td>
<td>RPT2006-25-10.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events</td>
<td>This report tracks file system activity associated with audited files and system objects, such as file access successes and failures.</td>
<td>RPT2003-05.rpt</td>
<td>Weekly</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>File Audit Events - File Attribute Change</td>
<td>File Attribute Change is a specific File Write event generated for the modification of file attributes (including properties such as read-only status). These events may be produced by any tool that is used to monitor the activity of file usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-41.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Audit</td>
<td>File Audit events are used to track file activity on monitored network devices, usually through the Operating System or a Host-Based IDS. These events will note success or failure of the requested operation.</td>
<td>RPT2003-05-11.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Audit Failure</td>
<td>File Audit Failure events are used to track failed file activity on monitored network devices, usually through the Operating System or a Host-Based IDS. These events will note what requested operation failed.</td>
<td>RPT2003-05-12.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Create</td>
<td>File Create is a specific File Write event generated for the initial creation of a file. These events may be produced by any tool that is used to monitor the activity of file usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-42.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Data Read</td>
<td>File Data Read is a specific File Read event generated for the operation of reading data from a file (not just properties or status of a file). These events may be produced by any tool that is used to monitor the activity of file usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-31.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Data Write</td>
<td>File Data Write is a specific File Write event generated for the operation of writing data to a file (not just properties or status of a file). These events may be produced by any tool that is used to monitor the activity of file usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-43.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>File Audit Events - File Delete</td>
<td>File Delete is a specific File Write event generated for the deletion of an existing file. These events may be produced by any tool that is used to monitor the activity of file usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-44.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Execute</td>
<td>File Execute is a specific File Read event generated for the operation of executing files. These events may be produced by any tool that is used to monitor the activity of file usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-32.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Handle Audit</td>
<td>File Handle Audit events are used to track file handle activity on monitored network devices, usually through low level access to the Operating System, either natively or with or a Host-Based IDS. These events will note success or failure of the requested operation.</td>
<td>RPT2003-05-21.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Handle Close</td>
<td>File Handle Close is a specific File Handle Audit event generated for the closing of file handles. These events may be generated by a tool that has low-level file access, such as an Operating System or some Host-Based IDS'.</td>
<td>RPT2003-05-22.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Handle Copy</td>
<td>File Handle Copy is a specific File Handle Audit event generated for the copying of file handles. These events may be generated by a tool that has low-level file access, such as an Operating System or some Host-Based IDS'.</td>
<td>RPT2003-05-23.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Handle Open</td>
<td>File Handle Open is a specific File Handle Audit event generated for the opening of file handles. These events may be generated by a tool that has low-level file access, such as an Operating System or some Host-Based IDS'.</td>
<td>RPT2003-05-24.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Link</td>
<td>File Link is a specific File Write event generated for the creation, deletion, or modification of links to other files. These events may be produced by any tool that is used to monitor the activity of file usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-45.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>File Audit Events - File Move</td>
<td>File Move is a specific File Write event generated for the operation of moving a file that already exists. These events may be produced by any tool that is used to monitor the activity of file usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-46.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Read</td>
<td>File Read is a specific File Audit event generated for the operation of reading files (including reading properties of a file or the status of a file). These events may be produced by any tool that is used to monitor the activity of file usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-33.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - File Write</td>
<td>File Write is a specific File Audit event generated for the operation of writing to a file (including writing properties of a file or changing the status of a file). These events may be produced by any tool that is used to monitor the activity of file usage, including a Host-Based IDS and some operating systems.</td>
<td>RPT2003-05-47.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - Object Audit</td>
<td>Object Audit events are used to track special object activity on monitored network devices, usually through the Operating System or a Host-Based IDS. Generally, Objects are special types of system resources, such as registry items or user account databases. These objects may be actual 'files' on the system, but are not necessarily human readable. These events will note success or failure of the requested operation.</td>
<td>RPT2003-05-51.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - Object Audit Failure</td>
<td>Object Audit Failure events are used to track special object activity on monitored network devices, usually through the Operating System or a Host-Based IDS. Generally, Objects are special types of system resources, such as registry items or user account databases. These objects may be actual 'files' on the system, but are not necessarily human readable. These events will note a failure of the requested operation.</td>
<td>RPT2003-05-52.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>File Audit Events - Object Delete</td>
<td>Object Delete is a specific Object Audit event generated for the deletion of an existing object. These events may be produced by any tool that is used to monitor the activity of file and object usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-53.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>File Audit Events - Object Link</td>
<td>Object Link is a specific Object Audit event generated for the creation, deletion, or modification of links to other objects. These events may be produced by any tool that is used to monitor the activity of file and object usage, including a Host-Based IDS and some Operating Systems.</td>
<td>RPT2003-05-54.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Incident Events</td>
<td>This report tracks the Incident, HostIncident, HybridIncident and NetworkIncident events that have been generated to reflect enterprise-wide issues.</td>
<td>RPT2006-19.rpt</td>
<td>Daily</td>
</tr>
<tr>
<td>Inferred Events</td>
<td>This report tracks events that are triggered by correlations built in the SolarWinds Rule Builder.</td>
<td>RPT2006-27.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Inferred Events by Inference Rule</td>
<td>This report tracks events that are triggered by correlations, and orders them by the correlation rule name.</td>
<td>RPT2006-27-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Log On/Off/Failure</td>
<td>Track activity associated with account events such as log on, log off and log on failures. This is a refined version of the Authentication Report that does not include SolarWinds authentication events. It is more appropriate for management reports or audit reviews than regular use.</td>
<td>RPT2003-03.rpt</td>
<td>Weekly</td>
</tr>
<tr>
<td>Network Traffic Audit</td>
<td>Track activity associated with network traffic audit events such as TCP, IP and UDP events. Specifically, this report tracks regular network traffic activity, such as encrypted traffic, web traffic, and other forms of UDP, TCP and ICMP traffic. It gives you both an overview and some details of exactly what is flowing through your network. This report can be quite large.</td>
<td>RPT2003-06.rpt</td>
<td>Daily, if needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Network Traffic Audit - Application Traffic</td>
<td>ApplicationTrafficAudit events reflect network traffic that is mostly or all application-layer data. Events that are children of ApplicationTrafficAudit are also related to application-layer resources. Events placed in the parent ApplicationTrafficAudit event itself are known to be application-related, but are not able to be further categorized based on the message provided by the tool or because they are uncommon and rarely, if ever, imply network attack potential.</td>
<td>RPT2003-06-11.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Application Traffic by Destination Machine</td>
<td>This report lists all Application Traffic events (such as WebTrafficAudit), grouped by destination machine/IP.</td>
<td>RPT2003-06-11-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Application Traffic by Provider SID</td>
<td>This report lists all Application Traffic events (such as WebTrafficAudit), grouped by provider SID.</td>
<td>RPT2003-06-11-3.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Application Traffic by Source Machine</td>
<td>This report lists all Application Traffic events (such as WebTrafficAudit), grouped by source machine/IP.</td>
<td>RPT2003-06-11-1.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Application Traffic by Tool Alias</td>
<td>This report lists all Application Traffic events (such as WebTrafficAudit), grouped by the SolarWinds sensor tool alias that reported each event.</td>
<td>RPT2003-06-11-0.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Network Traffic Audit - Configuration Traffic</td>
<td>Configuration Traffic Audit events reflect application-layer data related to configuration of network resources. Included in ConfigurationTrafficAudit are protocols such as DHCP, BootP, and SNMP. ConfigurationTrafficAudit events generally indicate normal traffic, however, events of this type could also be symptoms of misconfiguration, inappropriate usage, attempts to enumerate or access network devices or services, attempts to access devices that are configured via these services, or other abnormal traffic.</td>
<td>RPT2003-06-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Core Traffic</td>
<td>CoreTrafficAudit events reflect network traffic sent over core protocols. Events that are children of CoreTrafficAudit are all related to the TCP, IP, UDP, and ICMP protocols. Events of this type and its children do not have any application-layer data. Events placed in the parent CoreTrafficAudit event itself are known to be a core protocol, but are not able to be further categorized based on the message provided by the tool.</td>
<td>RPT2003-06-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Core Traffic by Destination Machine</td>
<td>This report lists all Core Traffic events (such as TCPTrafficAudit), grouped by destination machine/IP.</td>
<td>RPT2003-06-03-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Core Traffic by Provider SID</td>
<td>This report lists all Core Traffic events (such as TCPTrafficAudit), grouped by provider SiD.</td>
<td>RPT2003-06-03-3.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Core Traffic by Source</td>
<td>This report lists all Core Traffic events (such as TCPTrafficAudit), grouped by source machine/IP.</td>
<td>RPT2003-06-03-1.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Core Traffic by Tool Alias</td>
<td>This report lists all Core Traffic events (such as TCPTrafficAudit), grouped by the SolarWinds tool sensor alias that reported the event.</td>
<td>RPT2003-06-03-0.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Network Traffic Audit - Encrypted Traffic</td>
<td>Encrypted Traffic Audit events reflect application-layer traffic that has been encrypted and is intended for a secure host. Included in Encrypted Traffic Audit are client and server side application events, such as key exchanges, that normally occur after the low-level session creation and handshaking have completed.</td>
<td>RPT2003-06-04.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Link Control Traffic</td>
<td>Link Control Traffic Audit events are generated for network events related to link level configuration. Link Control Traffic Audit events generally indicate normal traffic, however, events of this type could also be symptoms of misconfiguration at the link level, inappropriate usage, or other abnormal traffic.</td>
<td>RPT2003-06-05.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Network Traffic</td>
<td>Members of the Network Audit tree are used to define events centered on usage of network resources/bandwidth.</td>
<td>RPT2003-06-06.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Point to Point Traffic</td>
<td>Point To Point Traffic Audit events reflect application-layer data related to point-to-point connections between hosts. Included in Point To Point Traffic Audit are encrypted and unencrypted point-to-point traffic.</td>
<td>RPT2003-06-07.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Remote Procedure Traffic</td>
<td>Remote Procedure Traffic Audit events reflect application-layer data related to remote procedure services. Included in Remote Procedure Traffic Audit are the traditional RPC services used to service remote logons and file shares, and other services which require remote procedure access to complete authentication, pass data, or otherwise communicate. RemoteProcedureTrafficAudit events generally indicate normal traffic for networks that have remote procedure services on their network; however, events of this type could also be symptoms of inappropriate access, misconfiguration of the remote procedure services, errors in the remote procedure calls, or other abnormal traffic.</td>
<td>RPT2003-06-08.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Network Traffic Audit - Routing Traffic</td>
<td>Routing Traffic Audit events are generated for network events related to configuration of network routes, using protocols such as IGMP, IGRP, and RIP. RoutingTrafficAudit events generally indicate normal traffic, however, events of this type could also be symptoms of misconfigured routing, unintended route configuration, or other abnormal traffic.</td>
<td>RPT2003-06-09.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Time Traffic</td>
<td>Time Traffic Audit events reflect application-layer data related to network time configuration. Included in TimeTrafficAudit are protocols such as NTP and activities, such as detection of client-side network time updates.</td>
<td>RPT2003-06-10.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Top Application Traffic by Source</td>
<td>This report lists the Top Application Traffic events (such as WebTrafficAudit), grouped by source machine/IP.</td>
<td>RPT2003-06-01-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Top Core Traffic by Source</td>
<td>This report lists the Top Core Traffic events (such as TCPTrafficAudit), grouped by source machine/IP.</td>
<td>RPT2003-06-03-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Web Traffic</td>
<td>WebTrafficAudit events reflect application-layer data related to web services. Included in WebTrafficAudit are client and server web events from web servers, web applications, content filter related events, and other web services. WebTrafficAudit events generally indicate normal traffic, however, events of this type could also be symptoms of inappropriate web usage, potential abuse of web services, or other abnormal traffic.</td>
<td>RPT2003-06-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Web Traffic by Destination Machine</td>
<td>This report lists all WebTrafficAudit events grouped by destination machine/IP.</td>
<td>RPT2003-06-01-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Web Traffic by Provider SID</td>
<td>This report lists Web Traffic Audit events grouped by provider SID.</td>
<td>RPT2003-06-01-3.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td><strong>Description</strong></td>
<td><strong>File Name</strong></td>
<td><strong>Schedule</strong></td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Network Traffic Audit - Web Traffic by Source Machine</td>
<td>This report lists all WebTrafficAudit events grouped by source machine/IP.</td>
<td>RPT2003-06-01-1.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Web Traffic by Tool Alias</td>
<td>This report lists Web Traffic Audit events grouped by tool alias.</td>
<td>RPT2003-06-01-0.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Web URL Requests by Source Machine</td>
<td>This report lists the most frequently visited URLs grouped by the requesting client source machine.</td>
<td>RPT2003-06-01-5.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Traffic Audit - Web URL Requests by Source Machine - Graphs</td>
<td>This report shows graphs of the most frequently visited URLs for each client source machine.</td>
<td>RPT2003-06-01-4.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Resource Configuration</td>
<td>The Resource Configuration report details events that relate to configuration of user accounts, machine accounts, groups, policies and their relationships. Items such as domain or group modification, policy changes, and creation of new network resources.</td>
<td>RPT2003-08.rpt</td>
<td>Weekly</td>
</tr>
<tr>
<td>Resource Configuration - Authorization Audit</td>
<td>Events that are part of the Auth Audit tree are related to authentication and authorization of accounts and account containers such as groups or domains. These events can be produced from any network node including firewalls, routers, servers, and clients.</td>
<td>RPT2003-08-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Resource Configuration - Domain Authorization Audit</td>
<td>Domain Auth Audit events are authentication, authorization, and modification events related only to domains, subdomains, and account containers. These events are normally operating system related, however could be produced by any network device.</td>
<td>RPT2003-08-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Resource Configuration - Group Audit</td>
<td>Group Audit events are authentication, authorization, and modification events related only to account groups. These events are normally operating system related, however could be produced by any network device.</td>
<td>RPT2003-08-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Resource Configuration - Machine Authorization Audit</td>
<td>Machine Auth Audit events are authentication, authorization, and modification events related only to computer or machine accounts. These events can be produced from any network node including firewalls, routers, servers, and clients, but are normally operating system related.</td>
<td>RPT2003-08-04.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Resource Configuration - Policy Audit</td>
<td>Policy Audit events are used to track access, modification, scope change, and creation of authentication, domain, account, and account container policies. Many of these events reflect normal system traffic. Most PolicyAudit events are provided by the Operating System.</td>
<td>RPT2003-08-06.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Resource Configuration - User Authorization Audit</td>
<td>User Auth Audit events are authentication, authorization, and modification events related only to user accounts. These events can be produced from any network node including firewalls, routers, servers, and clients.</td>
<td>RPT2003-08-05.rpt</td>
<td>As needed</td>
</tr>
</tbody>
</table>
## Security reports included with LEM

The following table lists and describes each of the security reports, listed alphabetically by title.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>File Name</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Report - Failed Authentication</td>
<td>Failed Authentication events occur when a user has made several attempts to authenticate themselves which has continuously failed, or when a logon failure is serious enough to merit a security event on a single failure.</td>
<td>RPT2003-02-1.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - Guest Login</td>
<td>This report shows logins to various Guest accounts.</td>
<td>RPT2003-02-2.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - Restricted Information Attempt</td>
<td>Restricted Information Attempt events describe a user attempt to access local or remote information that their level of authorization does not allow. These events may indicate user attempts to exploit services which they are denied access to or inappropriate access attempts to information.</td>
<td>RPT2003-02-3.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Authentication Report - Restricted Service Attempt</td>
<td>Restricted Service Attempt events describe a user attempt to access a local or remote service that their level of authorization does not allow. These events may indicate user attempts to exploit services which they are denied access to or inappropriate access attempts to services.</td>
<td>RPT2003-02-4.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Console</td>
<td>The Console report shows every event that passes through the system in the given time interval. It mimics the basic management console view. It does not contain the same level of field detail, but it is useful to get a quick snapshot of activity for a period, a lunch hour, for example. This report can be very large, so you will only want to run for small time intervals, such as hours.</td>
<td>RPT2003-10.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Console - Overview</td>
<td>An overview of all events during the specified time range. Shows graphs of the most common generic event field data from the console report.</td>
<td>RPT2003-10-00.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>FileName</td>
<td>Schedule</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Event Summary - Graphs</td>
<td>The event summary report gathers statistical data from all major event categories, summarizes it with a one-hour resolution, and presents a quick, graphical overview of activity on your network.</td>
<td>RPT2003-01.rpt</td>
<td>Daily</td>
</tr>
<tr>
<td>Event Summary - Top Level Statistics</td>
<td>Event Summary Sub Report - Top Level Statistics</td>
<td>RPT2003-01-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Machine Audit</td>
<td>Track activity associated with machine process and service audit events. This report shows machine-level events such as software installs, patches, system shutdowns, and reboots. It can be used to assist in software license compliance auditing by providing records of installs.</td>
<td>RPT2003-09.rpt</td>
<td>Weekly</td>
</tr>
<tr>
<td>Machine Audit - File System Audit</td>
<td>This report tracks activity associated with file system audit events including mount file system and unmount file system events. These events are generally normal system activity, especially during system boot.</td>
<td>RPT2003-09-010.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Machine Audit - File System Audit - File System</td>
<td>Mount File System events are a specific type of File System Audit that reflect the action of creating an active translation between hardware to a usable files system. These events are generally normal during system boot.</td>
<td>RPT2003-09-012.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Machine Audit - File System Audit - Unmount File System</td>
<td>Unmount File System events are a specific type of File System Audit that reflect the action of removing a translation between hardware and a usable files system. These events are generally normal during system shutdown.</td>
<td>RPT2003-09-013.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Machine Audit - Process Audit</td>
<td>This report tracks activity related to processes, including processes that have started, stopped, or reported useful process-related information.</td>
<td>RPT2003-09-030.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Machine Audit - Process Audit - Process Audit</td>
<td>This report lists Process Audit events that are generated to track launch, exit, status, and other events related to system processes. Usually, these events reflect normal system activity. Process-related activity that may indicate a failure will be noted separately from normal activity in the event detail.</td>
<td>RPT2003-09-031.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Machine Audit - Process Audit - Process Info</td>
<td>Process Info is a specific type of Process Audit event that reflects information related to a process. Most of these events can safely be ignored, as they are generally normal activity that does not reflect a failure or abnormal state.</td>
<td>RPT2003-09-032.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Machine Audit - Process Audit - Process Start</td>
<td>Process Start is a specific type of Process Audit event that indicates a new process has been launched. Usually, Process Start reflects normal system activity.</td>
<td>RPT2003-09-033.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Machine Audit - Process Audit - Process Stop</td>
<td>Process Stop is a specific type of Process Audit event that indicates a process has exited. Usually, Process Stop reflects normal application exit, however in the event of an unexpected error the abnormal state will be noted.</td>
<td>RPT2003-09-034.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Machine Audit - Process Audit - Process Warning</td>
<td>Process Warning is a specific type of Process Audit event that indicates a process has returned a 'Warning' message that is not a fatal error and may not have triggered an exit of the process.</td>
<td>RPT2003-09-035.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Machine Audit - Service Audit</td>
<td>This report tracks activity related to services, including services that have started, stopped, or reported useful service-related information or warnings.</td>
<td>RPT2003-09-040.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>TITLE</td>
<td>DESCRIPTION</td>
<td>FILE NAME</td>
<td>SCHEDULE</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Machine Audit</td>
<td>This report tracks ServiceInfo events, which reflect information related to a particular service. Most of these events can safely be ignored, as they are generally normal activity that does not reflect a failure or abnormal state.</td>
<td>RPT2003-09-041.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>- Service Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Service Info</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine Audit</td>
<td>This report tracks ServiceStart events, which indicate that a new system service is starting.</td>
<td>RPT2003-09-042.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>- Service Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Service Start</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine Audit</td>
<td>This report tracks ServiceStop events, which indicate that a system service is stopping. This activity is generally normal, however, in the event of an unexpected stop the abnormal state will be noted.</td>
<td>RPT2003-09-043.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>- Service Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Service Stop</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine Audit</td>
<td>This report lists ServiceWarning events. These events indicate a service has returned a Warning message that is not a fatal error and may not have triggered an exit of the service.</td>
<td>RPT2003-09-044.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>- Service Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Service Warning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine Audit</td>
<td>This report tracks activity associated with system status and modifications, including software changes, system reboots, and system shutdowns.</td>
<td>RPT2003-09-020.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>- System Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine Audit</td>
<td>Machine Audit events are used to track hardware or software status and modifications. These events are generally acceptable, but do indicate modifications to the client system that may be noteworthy.</td>
<td>RPT2003-09-021.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>- System Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Machine Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine Audit</td>
<td>SoftwareInstall events reflect modifications to the system at a software level, generally at the operating system level (or equivalent, in the case of a network infrastructure device). These events are generated when a user updates a system or launches system-native methods to install third party applications.</td>
<td>RPT2003-09-025.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>- System Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Software Install</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine Audit</td>
<td>SoftwareUpdate is a specific type of SoftwareInstall that reflects a more current version of software being installed to replace an older version.</td>
<td>RPT2003-09-026.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>- System Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Software Update</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine Audit</td>
<td>System Reboot events occur on monitored network devices (servers, routers, etc.) and indicate that a system has restarted.</td>
<td>RPT2003-09-022.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>- System Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- System Reboot</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine Audit</td>
<td>System shutdown events occur on monitored network devices (servers, routers, etc.) and indicate that a system has been shutdown.</td>
<td>RPT2003-09-023.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>- System Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- System Shutdown</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

page 366
<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th><strong>Description</strong></th>
<th><strong>FileName</strong></th>
<th><strong>Schedule</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Audit - System Audit - System Status</td>
<td>SystemStatus events reflect general system state events. These events are generally normal and informational, however, they could potentially reflect a failure or issue which should be addressed.</td>
<td>RPT2003-09-024.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Machine Audit - USB-Defender</td>
<td>This report tracks activity associated with USB-Defender, including insertion and removal events related to USB Mass Storage devices.</td>
<td>RPT2003-09-050.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Malicious Code</td>
<td>This report tracks event activity associated with malicious code such as virus, Trojans, and worms, both on the network and on local machines, as detected by anti-virus software.</td>
<td>RPT2003-04-04.rpt</td>
<td>Weekly</td>
</tr>
<tr>
<td>Malicious Code - Service Process Attack</td>
<td>Members of the Service Process Attack tree are used to define events centered on malicious or abusive usage of services or user processes. These events include abuse or misuse of resources from malicious code placed on the client system.</td>
<td>RPT2003-04-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Malicious Code - Trojan Command Access</td>
<td>Trojan Command Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through malicious code commonly known as Trojan Horses. This event detects the communication related to Trojans sending commands over the network (infecting other clients, participating in a denial of service activity, being controlled remotely by the originator, etc.). Trojans are generally executables that generally require no user intervention to spread and contain malicious code that is placed on the client system and used to exploit the client (and return access to the originator of the attack) or exploit other clients (used in attacks such as distributed denial of service attacks).</td>
<td>RPT2003-04-05.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Malicious Code - Trojan Infection Access</td>
<td>Trojan Infection Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through malicious code commonly known as a Trojan Horse. This event detects the infection traffic related to a Trojan entering the network (generally with intent to infect a client). Trojans are generally executables that generally require no user intervention to spread and contain malicious code that is placed on the client system and used to exploit the client (and return access to the originator of the attack) or exploit other clients (used in attacks such as distributed denial of service attacks).</td>
<td>RPT2003-04-04.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>TITLE</td>
<td>DESCRIPTION</td>
<td>FILE NAME</td>
<td>SCHEDULE</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Trojan Traffic Access - Trojan Code</td>
<td>Trojan Traffic Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through malicious code commonly known as a Trojan Horse. This event detects the communication related to Trojans over the network (generally, 'trojaned' clients calling home to the originator). Trojans are generally executables that generally require no user intervention to spread and contain malicious code that is placed on the client system and used to exploit the client (and return access to the originator of the attack) or exploit other clients (used in attacks such as distributed denial of service attacks).</td>
<td>RPT2003-04-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Trojan Traffic Denial - Trojan Code</td>
<td>Trojan Traffic Denial events are a specific type of Denial event where the transport of the malicious or abusive usage originates with malicious code on a client system known as a Trojan. The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. Trojan Traffic Denial events may be attempts to exploit weaknesses in software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, attempts to spread the Trojan to other hosts, or other denial of service activities.</td>
<td>RPT2003-04-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Virus Attack Code - Virus Code</td>
<td>Virus Attack events reflect malicious code placed on a client or server system, which may lead to system or other resource compromise and may lead to further attack. The severity of this event will depend on the ActionTaken field, which reflects whether the virus or other malicious code was successfully removed.</td>
<td>RPT2003-04-06.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Virus Summary Attack Code - Virus Code</td>
<td>Virus Summary Attack events reflect malicious code placed on a client or server system, which may lead to system or other resource compromise and may lead to further attack. The severity of this event will depend on the Action Taken field which reflects whether the virus or other malicious code was successfully removed. These events differ from Virus Attack in that they may be a composite of virus events normally due to a scheduled scan on the client system as opposed to a real-time scan</td>
<td>RPT2003-04-07.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Malicious Code Report - Virus Traffic Access</td>
<td>Virus Traffic Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through malicious code commonly known as viruses. This event detects the communication related to viruses over the network (generally, the spread of a virus infection or an incoming virus infection). Viruses are generally executables that require user intervention to spread, contain malicious code that is placed on the client system, and are used to exploit the client and possibly spread itself to other clients.</td>
<td>RPT2003-04-08.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Attack Behavior - Access</td>
<td>This report tracks activity associated with top-level NetworkAttack events.</td>
<td>RPT2003-11-00.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access</td>
<td>This report shows malicious asset access via the network. For example, attacks on FTP or Windows Network servers, malicious network database access, abuses of services, or attempted unauthorized entry.</td>
<td>RPT2003-11.rpt</td>
<td>Weekly</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Access</td>
<td>Children of the Access tree define events centered on malicious or abusive usage of network bandwidth/traffic where the intention, or the result, is inappropriate or abusive access to network resources.</td>
<td>RPT2003-11-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Application Access</td>
<td>Application Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources where the related data is mostly or all application-layer. Generally, ApplicationAccess events will reflect attempted exploitation of weaknesses in server or client software, or information that is restricted/prohibited by device access control or policy.</td>
<td>RPT2003-11-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Configuration Access</td>
<td>Configuration Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via resource configuration traffic (using protocols such as DHCP, BootP, and SNMP). Generally, these events will reflect attempted exploitation of weaknesses in the configuration server or client software or attempts to gain system-level access to configuration servers themselves. In the case of SNMP and similar configuration protocols, it could reflect an attempt to enumerate a device or devices on the same network for further attack.</td>
<td>RPT2003-11-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Core Access</td>
<td>Core Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources where the related data is mostly or all core protocols (TCP, UDP, IP, ICMP). Generally, CoreAccess events will reflect attempted exploitation of weaknesses in network protocols or devices with intent to gain access to servers, clients, or network infrastructure devices.</td>
<td>RPT2003-11-04.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Database Access - Core Access</td>
<td>Database Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via application-layer database traffic. Generally, these events will reflect attempted exploitation of weaknesses in database server or client software.</td>
<td>RPT2003-11-05.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Core Access - File System Access</td>
<td>File System Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via remote file system traffic (using protocols such as SMB and NFS). Generally, these events will reflect attempted exploitation of weaknesses in the remote file system server or client software or attempts to gain system-level access to remote file system servers themselves.</td>
<td>RPT2003-11-06.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Core Access - File Transfer</td>
<td>File Transfer Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via application-layer file transfer traffic. Generally, these events will reflect attempted exploitation of weaknesses in file transfer server or client software.</td>
<td>RPT2003-11-07.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Link Control Access</td>
<td>Link Control Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources where the related data is low-level link control (using protocols such as ARP). Generally, Link Control Access events will reflect attempted exploitation of weaknesses in switching devices by usage of malformed incoming or outgoing data, with intent to enumerate or gain access to or through switching devices, clients that are also on the switching device, and entire networks attached to the switching device. In some cases, a managed switch with restrictions on port analyzing activity may be forced into an unmanaged switch with no restrictions - allowing a malicious client to sniff traffic and enumerate or attack.</td>
<td>RPT2003-11-08.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Mail Access</td>
<td>Mail Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via application-layer mail transfer, retrieval, or service traffic. Generally, these events will reflect attempted exploitation of weaknesses in mail-related server or client software.</td>
<td>RPT2003-11-09.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Naming Access</td>
<td>Naming Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via application-layer naming service traffic (using protocols such as DNS and WINS). Generally, these events will reflect attempted exploitation of weaknesses in the naming server or client software.</td>
<td>RPT2003-11-10.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - News Access</td>
<td>News Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via application-layer news traffic (over protocols such as NNTP). Generally, these events will reflect attempted exploitation of weaknesses in the news server or client software.</td>
<td>RPT2003-11-11.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Point to Point Access</td>
<td>Point To Point Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via point to point traffic (using protocols such as PPTP). Generally, these events will reflect attempted exploitation of weaknesses in point to point server or client software, attempts to enumerate networks, or attempts to further attack devices on trusted networks.</td>
<td>RPT2003-11-12.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Printer Access</td>
<td>Printer Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via application-layer remote printer traffic. Generally, these events will reflect attempted exploitation of weaknesses in the remote printer server or client software.</td>
<td>RPT2003-11-13.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Remote Console Access</td>
<td>Remote Console Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via application-layer remote console service traffic (services such as telnet, SSH, and terminal services). Generally, these events will reflect attempted exploitation of weaknesses in the remote console server or client software.</td>
<td>RPT2003-11-14.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Remote Procedure Access</td>
<td>Remote Procedure Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via remote procedure call traffic (using protocols such as the traditional RPC services, RMI, and CORBA). Generally, these events will reflect attempted exploitation of weaknesses in the remote procedure server or client software or attempts to gain system-level access to remote procedure servers themselves.</td>
<td>RPT2003-11-15.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Routing Access</td>
<td>Routing Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources where the related data is routing-related protocols (RIP, IGMP, etc.). Generally, Routing Access events will reflect attempted exploitation of weaknesses in routing protocols or devices with intent to enumerate or gain access to or through routers, servers, clients, or other network infrastructure devices. These routing protocols are used to automate the routing process between multiple devices that share or span networks.</td>
<td>RPT2003-11-16.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Time Access</td>
<td>Time Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via application-layer remote time service traffic (using protocols such as NTP). Generally, these events will reflect attempted exploitation of weaknesses in the remote time server or client software.</td>
<td>RPT2003-11-17.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Virus Traffic Access</td>
<td>Virus Traffic Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through malicious code commonly known as viruses. Generally, these events will reflect attempted exploitation of weaknesses in the web server or client software.</td>
<td>RPT2003-11-19.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Access - Web Access</td>
<td>Web Access events reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources via application-layer WWW traffic. Generally, these events will reflect attempted exploitation of weaknesses in the web server or client software.</td>
<td>RPT2003-11-18.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay</td>
<td>Track activity associated with network denial or relay attack behaviors. This report shows malicious asset relay attempts and denials of service via the network. For example, FTP bouncing, Distributed Denial of Service events, and many protocol abuses.</td>
<td>RPT2003-12.rpt</td>
<td>Weekly</td>
</tr>
<tr>
<td>TITLE</td>
<td>DESCRIPTION</td>
<td>FILE NAME</td>
<td>SCHEDULE</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - Application Denial</td>
<td>Application Denial events are a specific type of Denial event where the transport of the malicious or abusive usage is application-layer protocols. The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. Application Denial events may be attempts to exploit weaknesses in software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, or other denial of service activities.</td>
<td>RPT2003-12-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - Configuration Denial</td>
<td>Configuration Denial events are a specific type of Denial event where the transport of the malicious or abusive usage is protocols related to configuration of resources (DHCP, BootP, SNMP, etc.). The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. Configuration Denial events may be attempts to exploit weaknesses in configuration-related software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, or other denial of service activities.</td>
<td>RPT2003-12-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - Core Denial</td>
<td>Core Denial events are a specific type of Denial event where the transport of the malicious or abusive usage is core protocols (TCP, IP, ICMP, UDP). The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. Core Denial events may be attempts to exploit weaknesses in software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, or other denial of service activities.</td>
<td>RPT2003-12-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - Denial</td>
<td>Children of the Denial tree define events centered on malicious or abusive usage of network bandwidth/traffic where the intention, or the result, is inappropriate or abusive access to network resources through a denial of service attack.</td>
<td>RPT2003-12-04.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - File System Denial</td>
<td>File System Denial events are a specific type of Denial event where the transport of the malicious or abusive usage is remote file system-related protocols (NFS, SMB, etc.). The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. File System Denial events may be attempts to exploit weaknesses in remote file system services or software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, or other denial of service activities.</td>
<td>RPT2003-12-05.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - File Transfer Denial</td>
<td>File Transfer Denial events are a specific type of Denial event where the transport of the malicious or abusive usage is application-layer file transfer-related protocols (FTP, TFTP, etc.). The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. FileTransferDenial events may be attempts to exploit weaknesses in file transfer-related software to gain access to a host system, attempts to exploit weaknesses in the software to enumerate or reconfigure, or other denial of service activities.</td>
<td>RPT2003-12-06.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - Link Control Denial</td>
<td>Link Control Denial events are a specific type of Denial event where the transport of the malicious or abusive usage is link level protocols (such as ARP). The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. LinkControlDenial events may be attempts to exploit weaknesses in link-level control software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, or other denial of service activities.</td>
<td>RPT2003-12-07.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - Mail Denial</td>
<td>MailDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is application-layer mail-related protocols (SMTP, IMAP, POP3, etc.) or services (majordomo, spam filters, etc.). The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. MailDenial events may be attempts to exploit weaknesses in mail-related software to gain access to a host system, attempts to exploit weaknesses in the software to enumerate or reconfigure, or other denial of service activities.</td>
<td>RPT2003-12-08.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>TITLE</td>
<td>DESCRIPTION</td>
<td>FILE NAME</td>
<td>SCHEDULE</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - Relay</td>
<td>Children of the Relay tree define events centered on malicious or abusive usage of network bandwidth/traffic where the intention, or the result, is relaying inappropriate or abusive access to other network resources (either internal or external). Generally, these attacks will have the perimeter or an internal host as their point of origin. When sourced from remote hosts, they may indicate a successful exploit of an internal or perimeter host.</td>
<td>RPT2003-12-09.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - Remote Procedure Denial</td>
<td>Remote Procedure Denial events are a specific type of Denial event where the transport of the malicious or abusive usage is remote procedure-related protocols (traditional RPC, RMI, CORBA, etc.) or service (portmapper, etc.). The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. RemoteProcedureDenial events may be attempts to exploit weaknesses in remote procedure services or software to gain access to a host system, attempts to exploit weaknesses in the software to enumerate or reconfigure, or other denial of service activities.</td>
<td>RPT2003-12-10.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - Routing Denial</td>
<td>Routing Denial events are a specific type of Denial event where the transport of the malicious or abusive usage is routing-related protocols (RIP, IGMP, etc.). The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. Routing Denial events may be attempts to exploit weaknesses in routers or routing software to gain access to a host system, attempts to exploit weaknesses in the routing software or service to enumerate or reconfigure, or other denial of service activities.</td>
<td>RPT2003-12-11.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Attack Behavior - Denial / Relay - Web Denial</td>
<td>Web Denial events are a specific type of Denial event where the transport of the malicious or abusive usage is application-layer web-related protocols (HTTP, HTTPS, etc.) or services (CGI, ASP, etc.). The intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service attack. Web Denial events may be attempts to exploit weaknesses in web-related software to gain access to a host system, attempts to exploit weaknesses in the software to enumerate or reconfigure, or other denial of service activities.</td>
<td>RPT2003-12-12.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior</td>
<td>Track activity associated with suspicious network behaviors such as reconnaissance or unusual traffic. Specifically, this report shows potentially dangerous activity, such as excessive authentication failures, port scans, stack fingerprinting, and network enumerations.</td>
<td>RPT2003-07.rpt</td>
<td>Weekly</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Application Enumerate</td>
<td>Application Enumerate events reflect attempts to gather information about target hosts, or services on target hosts, by sending active application-layer data which will elicit responses that reveal information about the application or host. This enumeration may be a command sent to the application to attempt to fingerprint what is allowed or denied by the service, requests to the application which may enable an attacker to surmise the version and specific application running, and other information gathering tactics. These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the host or application that may work correctly the first time - enabling them to modify their methodology to go on relatively undetected.</td>
<td>RPT2003-07-01.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Banner Grabbing Enumerate</td>
<td>Banner Grabbing Enumerate events reflect attempts to gather information about target hosts, or services on target hosts, by sending a request which will elicit a response containing the host or service's 'banner'. This 'banner' contains information that may provide a potential attacker with such details as the exact application and version running behind a port. These details could be used to craft specific attacks against hosts or services that an attacker may know will work correctly the first time - enabling them to modify their methodology to go on relatively undetected.</td>
<td>RPT2003-07-02.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Core Scan</td>
<td>Core Scan events reflect attempts to gather information about target networks, or specific target hosts, by sending scans over core network protocols (TCP, IP, ICMP, UDP) which will elicit responses that reveal information about clients, servers, or other network infrastructure devices. The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target would, information such as a list of applications listening on ports, operating system information, and other information that a probe may discover without enumeration of the specific services or performing attack attempts.</td>
<td>RPT2003-07-03.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Enumerate</td>
<td>Enumerate events reflect attempts to gather information about target networks, or specific target hosts, by sending active data which will elicit responses that reveal information about clients, servers, or other network infrastructure devices. The originating source of the enumeration is generally attempting to acquire information that may reveal more than normal traffic to the target would.</td>
<td>RPT2003-07-04.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>FileName</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Footprint</td>
<td>Footprint events reflect attempts to gather information about target networks by tracing the network through routers, clients, servers, or other network infrastructure devices. The originating source of the footprint is generally attempting to acquire information that may reveal more about network behavior than normal traffic to the target would.</td>
<td>RPT2003-07-05.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - General Security</td>
<td>General Security events are generated when a supported product outputs data that has not yet been normalized into a specific event, but is known to be security issue-related.</td>
<td>RPT2003-07-17.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Host Scan</td>
<td>Host Scan events reflect attempts to gather information about specific target hosts by sending scans which will elicit responses that reveal information about clients, servers, or other network infrastructure devices. The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target would, such as a list of applications on the host, operating system information, and other information that a probe may discover without enumeration of the specific services or performing attack attempts. These scans generally do not occur across entire networks and generally have the intent of discovering operating system and application information which may be used for further attack preparation.</td>
<td>RPT2003-07-06.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - ICMP Query</td>
<td>ICMP Query events reflect attempts to gather information about specific target hosts, or networks, by sending ICMP-based queries that will elicit responses that reveal information about clients, servers, or other network infrastructure devices. The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target would, such as operating system information and other information that a probe may discover without enumeration of the specific services or performing attack attempts. These scans generally do not occur across entire networks, contain many sequential ICMP packets, and generally have the intent of discovering operating system and application information which may be used for further attack preparation.</td>
<td>RPT2003-07-07.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>TITLE</td>
<td>DESCRIPTION</td>
<td>FILE NAME</td>
<td>SCHEDULE</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - MS Networking Enumerate</td>
<td>MS Networking Enumerate events reflect attempts to gather information about target hosts, or services on target hosts, by sending active data to Microsoft networking services (using protocols such as NetBIOS and SMB/CIFS) that will illicit responses that reveal information about the application, host, or target network. This enumeration may be a simple command sent to the networking service to attempt to fingerprint what is allowed or denied by a service, requests to a service that may enable an attacker to surmise the version and specific service running, requests to a service that may enable an attacker to fingerprint the target network, and other information gathering tactics. These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the networking service, host, or application that may work correctly the first time - enabling them to modify their methodology to go on relatively undetected.</td>
<td>RPT2003-07-08.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Network Suspicious</td>
<td>Members of the Network Suspicious tree are used to define events regarding suspicious usage of network bandwidth/traffic. These events include unusual traffic and reconnaissance behavior detected on network resources.</td>
<td>RPT2003-07-09.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Port Scan</td>
<td>Port Scan events reflect attempts to gather information about target networks, or specific target hosts, by sending scans over core network protocols (TCP, IP, ICMP, UDP) that will elicit responses that reveal information about clients, servers, or other network infrastructure devices. The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target would, such as a list of applications listening on ports, operating system information, and other information that a probe may discover without enumeration of the specific services or performing attack attempts. Port Scans specifically operate by sending probes to every port within a range, attempting to identify open ports that may use applications or services that are easy to enumerate and attack.</td>
<td>RPT2003-07-10.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Recon</td>
<td>Children of the Recon tree reflect suspicious network behavior with intent of gathering information about target clients, networks, or hosts. Reconnaissance behavior may be valid behavior on a network, however, only as a controlled behavior in small quantities. Invalid reconnaissance behavior may reflect attempts to determine security flaws on remote hosts, missing access control policies that allow external hosts to penetrate networks, or other suspicious behavior that results in general information gathering without actively attacking.</td>
<td>RPT2003-07-11.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Remote Procedure Enumerate</td>
<td>Remote Procedure Enumerate events reflect attempts to gather information about target hosts, or services on target hosts, by sending active data to Remote Procedure services (using protocols such as RMI, CORBA, and traditional RPC) that will elicit responses that reveal information about the application or host. This enumeration may be a simple command sent to the remote procedure service to attempt to fingerprint what is allowed or denied by the service, requests to the remote procedure service that may enable an attacker to surmise the version and specific service running, and other information gathering tactics. These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the remote procedure service or application that may work correctly the first time - enabling them to modify their methodology to go on relatively undetected.</td>
<td>RPT2003-07-12.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Scan</td>
<td>Scan events reflect attempts to gather information about target networks, or specific target hosts, by sending scans which will elicit responses that reveal information about clients, servers, or other network infrastructure devices. The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target would, information such as a list of applications listening on ports, operating system information, and other information that a probe may discover without enumeration of the specific services or performing attack attempts.</td>
<td>RPT2003-07-13.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
<td>File Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Stack Fingerprint</td>
<td>Stack Fingerprint events reflect attempts to gather information about specific target hosts by sending a certain set of packets to probe a device's network stack, which will elicit responses that reveal information about clients, servers, or other network infrastructure devices. The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target would, such as operating system information (including type and version) and other information that a probe may discover without enumeration of the specific services or performing attack attempts. These scans generally do not occur across entire networks and generally have the intent of discovering operating system information which may be used for further attack preparation.</td>
<td>RPT2003-07-14.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Trojan Scanner</td>
<td>Trojan Scanner events reflect attempts of Trojans on the network to gather information about target networks, or specific target hosts, by sending scans which will elicit responses that reveal information about the host. The originating Trojan source of the scan is generally attempting to acquire information that will reveal whether a target host or network has open and available services for further exploitation, whether the target host or network is alive, and how much of the target network is visible. A Trojan may run a scan before attempting an attack operation to test potential effectiveness or targeting information.</td>
<td>RPT2003-07-15.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Network Events: Suspicious Behavior - Unusual Traffic</td>
<td>Unusual Traffic events reflect suspicious behavior on network devices where the traffic may have no known exploit, but is unusual and could be potential enumerations, probes, fingerprints, attempts to confuse devices, or other abnormal traffic. Unusual Traffic may have no impending response, however, it could reflect a suspicious host that should be monitored closely.</td>
<td>RPT2003-07-16.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Priority Event (reference)</td>
<td>This report is no longer in use. The Priority Event report tracks those events that the user has identified as a priority event. These events appear in the Priority filter of the Console.</td>
<td>RPT2003-16.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Priority Event By User (reference)</td>
<td>This report is no longer in use. This report mirrors the standard Priority Event report but groups the events received by Console User account. The same event may be seen by many users, so this report tends to be much larger than the standard Priority Event report.</td>
<td>RPT2003-17.rpt</td>
<td>As needed</td>
</tr>
<tr>
<td>Rule Subscriptions by User</td>
<td>The Rule Subscriptions report tracks those events that the user has subscribed to monitor.</td>
<td>RPT2006-28-01.rpt</td>
<td>Daily</td>
</tr>
</tbody>
</table>
Support reports included with LEM

Support Reports are diagnostic tools used by SolarWinds Customer Support. Only run these reports at the request of SolarWinds. The reports are listed alphabetically by title.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Filename/Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Connection Status</td>
<td>This report is a diagnostic tool used by Customer Support, and generally run only at their request. This report tracks internal Agent online and offline events.</td>
<td>RPT2009-33-1.rpt As requested</td>
</tr>
<tr>
<td>Agent Connection Status by Agent</td>
<td>This report is a diagnostic tool used by Customer Support, and generally run only at their request. This report tracks internal Agent online and offline events grouped by Agent.</td>
<td>RPT2009-33-2.rpt As requested</td>
</tr>
<tr>
<td>Agent Connection Summary</td>
<td>This report is a diagnostic tool used by Customer Support, and generally run only at their request. This report shows high level summary information for when Agents go online and offline.</td>
<td>RPT2009-33.rpt As requested</td>
</tr>
<tr>
<td>Audit - Internal Audit Report</td>
<td>Audit - Internal Audit Report</td>
<td>RPT2006-31-01.rpt As requested</td>
</tr>
<tr>
<td>Audit - Internal Audit Report by User</td>
<td>Internal Audit Report grouped by User</td>
<td>RPT2006-31-02.rpt As requested</td>
</tr>
<tr>
<td>Agent Maintenance Report</td>
<td>This report is a diagnostic tool used by Customer Support, and generally run only at their request. This report displays internal event data for possible misconfigured Agents.</td>
<td>RPT2007-32.rpt As requested</td>
</tr>
<tr>
<td>Database Maintenance Report</td>
<td>This report is a diagnostic tool used by Customer Support, and generally run only at their request.</td>
<td>RPT2006-26.rpt As requested</td>
</tr>
<tr>
<td>List of Rules for Rule Subscriptions</td>
<td>This report lists available rules for the Rule Subscriptions.</td>
<td>RPT2006-29-02.rpt As needed</td>
</tr>
<tr>
<td>TITLE</td>
<td>DESCRIPTION</td>
<td>FILE NAME</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>List of Subscription Rules by User</td>
<td>This report lists the rules that users have subscribed to.</td>
<td>RPT2006-29-03.rpt</td>
</tr>
<tr>
<td>List of Users</td>
<td>This report lists each user entered. Currently, the users are only used for Rule Subscriptions.</td>
<td>RPT2006-29-01.rpt</td>
</tr>
<tr>
<td>Tool Maintenance by Alias</td>
<td>This report is a diagnostic tool used by Customer Support, and generally run only at their request. List of New Tool Data events based on Tool Alias.</td>
<td>RPT2003-14.rpt</td>
</tr>
<tr>
<td>Tool Maintenance by Insertion Point</td>
<td>This report is a diagnostic tool used by Customer Support, and generally run only at their request. List of New Tool Data events based on Agent InsertionIP.</td>
<td>RPT2003-15.rpt</td>
</tr>
<tr>
<td>Tool Maintenance by Provider</td>
<td>This report is a diagnostic tool used by Customer Support, and generally run only at their request. List of New Tool Data events based on ProviderSID.</td>
<td>RPT2003-13.rpt</td>
</tr>
<tr>
<td>Tool Maintenance Detail Report</td>
<td>This report is a diagnostic tool used by Customer Support, and generally run only at their request. The report displays a summary of all SolarWinds error messages received from various tools.</td>
<td>RPT2003-14.rpt</td>
</tr>
<tr>
<td>Tool Maintenance Report</td>
<td>This report is a diagnostic tool used by Customer Support, and generally run only at their request. The report displays a summary of unique SolarWinds error messages received from various tools.</td>
<td>RPT2003-13.rpt</td>
</tr>
</tbody>
</table>
The LEM command-line interface: Using the CMC

About the CMC command line

The CMC provides a command-line interface (CLI) for performing routine administrative tasks on a LEM VM.

Use CMC commands for tasks such as:

- Upgrading the Manager software
- Manually applying connector updates
- Deploying new connector infrastructure to the Managers and Agents
- Rebooting or shutting down the network appliance
- Configuring trusted reporting hosts
- Configuring supplemental services on the Manager appliance
- Controlling your nDepth appliance

Special characters allowed in CMC commands and passwords

The following table lists the special characters you can use in your CMC commands and passwords.

<table>
<thead>
<tr>
<th>CHARACTER</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital letters</td>
<td>ABCDEFGHIJKLMNOPQRSTUVWXYZ</td>
</tr>
<tr>
<td>Lower-case letters</td>
<td>abcdefghijklmnopqrstuvwxyz</td>
</tr>
<tr>
<td>Numerals</td>
<td>0123456789</td>
</tr>
<tr>
<td>Symbols</td>
<td>_ ` ~ ! @ # $ % ^ &amp; * ( ) - = + ' [ { ] } \</td>
</tr>
<tr>
<td>White spaces</td>
<td>command1 command2 command3</td>
</tr>
</tbody>
</table>

LEM CMC main menu

The CMC main menu opens when you log in to the CMC command-line interface.

See About the CMC command line for information about using the CMC command line.
Top-Level CMC commands

Commands are listed in order of appearance.

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>appliance</td>
<td>Displays the appliance menu to run network and system commands on the LEM VM. You can activate the VM, configure network parameters, and change the CMC password. See LEM CMC appliance menu for more information.</td>
</tr>
<tr>
<td>manager</td>
<td>Displays the manager menu where you can run upgrade and debug commands on the LEM Manager. You can install a LEM hotfix, start and stop the LEM Manager service, and import a certificate used for desktop console communication. See LEM CMC manager menu for more information.</td>
</tr>
<tr>
<td>service</td>
<td>Displays the service menu to run restrictions and SSH. You can start and stop the SSH Service and restrict access to the reports application by IP address or host name. See LEM CMC service menu for more information.</td>
</tr>
<tr>
<td>ndepth</td>
<td>Displays the ndepth menu to run nDepth configuration and maintenance commands. You can set your log message archive and backup share settings, restart the Log Message search or storage service, and start and stop the Log Message search and storage services. See LEM CMC nDepth menu for more information.</td>
</tr>
<tr>
<td>upgrade</td>
<td>Installs the LEM upgrade package that you will use to upgrade your LEM VM. This command functions the same as the hotfix command.</td>
</tr>
<tr>
<td>admin</td>
<td>Opens the admin command-line interface in the Lynx text browser.</td>
</tr>
<tr>
<td>import</td>
<td>Imports a keytab file from Active Directory into LEM. This file is required to configure LEM for Active Directory single sign-on. See Set up single sign-on in LEM for details.</td>
</tr>
<tr>
<td>help</td>
<td>Displays the Help menu.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits the CMC management console.</td>
</tr>
</tbody>
</table>

**LEM CMC appliance menu**

The cmc: appliance> menu includes commands for managing network and system settings.

See About the CMC command line for information about using the CMC command line.

Type the appliance command at the main menu to open the cmc: appliance> prompt. Commands available from the appliance menu are listed in the following table in alphabetical order.

A ✓ in the "Restart Required" column indicates that a command requires an automatic restart of the LEM Manager service. See Start and Stop LEM components for help.
<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
<th>RESTART REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>activate</td>
<td>Configures essential LEM features. This command should be run after you install the LEM license.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See Run the activate command to secure LEM and configure network settings for documentation.</td>
<td></td>
</tr>
<tr>
<td>checklogs</td>
<td>Shows the contents of the LEM log files from sources such as syslog and SNMP.</td>
<td></td>
</tr>
<tr>
<td>clearsystmp</td>
<td>Removes all rotated and compressed local files.</td>
<td></td>
</tr>
<tr>
<td>cleantmp</td>
<td>Removes temporary files LEM created during normal operation. Run this command to recover used disk space, or at the suggestion of SolarWinds Support.</td>
<td></td>
</tr>
<tr>
<td>dateconfig</td>
<td>Sets/shows the LEM VM's date and time.</td>
<td></td>
</tr>
<tr>
<td>dbdiskconfig</td>
<td>Configures the database retention setting (that is, the percentage of free space for the database). This command requires an automatic restart of the LEM Manager service.</td>
<td>✓</td>
</tr>
<tr>
<td>diskusage</td>
<td>Checks disk usage consumed by the LEM Manager and several other internal components (such as the database or log files), and provides a summary. This information is included when you send SolarWinds Support information using the support command.</td>
<td></td>
</tr>
<tr>
<td>diskusageconfig</td>
<td>Sets the LEM Manager disk usage limit by the percentage of unavailable disk space or the amount of free disk space.</td>
<td></td>
</tr>
<tr>
<td>editbanner</td>
<td>Edits the SSH login banner.</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits the appliance menu and returns to the main menu.</td>
<td></td>
</tr>
<tr>
<td>exportsystmp</td>
<td>Exports the system logs.</td>
<td></td>
</tr>
<tr>
<td>hostname</td>
<td>Changes the hostname of the LEM VM.</td>
<td></td>
</tr>
<tr>
<td>import</td>
<td>Imports the SIM or LEM backup to the LEM.</td>
<td></td>
</tr>
<tr>
<td>limitssyslog</td>
<td>Interrogates and/or changes the number of rotated log files to be kept.</td>
<td></td>
</tr>
<tr>
<td>multimanageconfig</td>
<td>Enables or disables the multimanager.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you enable multimanager, some security scanners may generate cross-domain security warnings about LEM. If this feature is not required, keep it disabled.</td>
<td></td>
</tr>
<tr>
<td>setlogrotate</td>
<td>Sets the syslog rotation frequency to either hourly or daily.</td>
<td></td>
</tr>
</tbody>
</table>
### COMMANDS

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
<th>RESTART REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>netconfig</td>
<td>Configures network settings for the LEM VM, such as the IP address, subnet mask, and DNS server(s).</td>
<td></td>
</tr>
<tr>
<td>ntpconfig</td>
<td>Configures the Network Time Protocol (NTP) service on the LEM VM for synchronization with a time server.</td>
<td></td>
</tr>
<tr>
<td>password</td>
<td>Changes the CMC user password.</td>
<td></td>
</tr>
<tr>
<td>ping</td>
<td>Pings other IP addresses or host names from the LEM VM to verify network connectivity.</td>
<td></td>
</tr>
<tr>
<td>reboot</td>
<td>Reboots the LEM VM.</td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the LEM VM.</td>
<td></td>
</tr>
<tr>
<td>top</td>
<td>Displays and monitors CPU and memory usage, as well as per process information for the Manager Network Appliance.</td>
<td></td>
</tr>
<tr>
<td>tzconfig</td>
<td>Configure the LEM VM time zone information.</td>
<td></td>
</tr>
<tr>
<td>viewnetconfig</td>
<td>Displays the LEM VM network settings, such as the IP address, subnet mask, and DNS server(s).</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits the appliance menu and returns to the main menu.</td>
<td></td>
</tr>
</tbody>
</table>

### LEM CMC manager menu

The `cmc:manager>` menu includes commands for upgrading and debugging LEM.

See [About the CMC command line](#) for information about using the CMC command line.

Type the `manager` command at the main menu to open the `cmc:manager>` prompt. Commands available from the manager menu are listed in the following table in alphabetical order. A ✓ in the "Restart Required" column indicates that a command requires an automatic restart of the LEM Manager service. See [Start and Stop LEM components](#) for help.
<table>
<thead>
<tr>
<th><strong>COMMAND</strong></th>
<th><strong>DESCRIPTION</strong></th>
<th><strong>RESTART REQUIRED</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>cleanagentconfig</td>
<td>Reconfigures the Agent on the current LEM Manager instance to connect to a new LEM Manager.</td>
<td></td>
</tr>
<tr>
<td>configurendepth</td>
<td>Configures the LEM VM to use a self-signed certificate.</td>
<td></td>
</tr>
<tr>
<td>confselfsignedcert</td>
<td>Configures the LEM Manager to use an nDepth server.</td>
<td></td>
</tr>
<tr>
<td>dbrestart</td>
<td>Restarts the database.</td>
<td></td>
</tr>
<tr>
<td>debug</td>
<td>Sends debugging information from the LEM Manager to any given email address. The email message contains a collection of data that can be useful in diagnosing problems.</td>
<td></td>
</tr>
<tr>
<td>disabletls</td>
<td>Disables TLS for the database connections.</td>
<td></td>
</tr>
<tr>
<td>enabletls</td>
<td>Enables TLS for the database connections.</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits the manager menu and returns to the main menu.</td>
<td></td>
</tr>
<tr>
<td>exportcert</td>
<td>Exports the CA certificate so that you can import it into a computer running the LEM console or the LEM reports application.</td>
<td></td>
</tr>
<tr>
<td>exportcertrequest</td>
<td>Exports the LEM Manager certificate (along with its public and private key) so that your certificate authority (CA) can sign it using PKI tools.</td>
<td></td>
</tr>
<tr>
<td>hotfix</td>
<td>Installs a LEM hotfix. This command functions the same as the upgrade command.</td>
<td></td>
</tr>
<tr>
<td>importcert</td>
<td>Imports a certificate signed by any certificate authority (CA). A certificate is required to encrypt communication with the LEM console or the LEM reports application.</td>
<td>✓</td>
</tr>
<tr>
<td>importl4ca</td>
<td>Imports a CA of the other node in an L4 configuration.</td>
<td>✓</td>
</tr>
<tr>
<td>licenseupgrade</td>
<td>Upgrades your LEM Manager license.</td>
<td>✓</td>
</tr>
<tr>
<td>logbackupconfig</td>
<td>Configures the Manager appliance remote log backups to a remote file share on a daily, weekly, or monthly schedule.</td>
<td></td>
</tr>
<tr>
<td>resetadmin</td>
<td>Resets the admin password to <code>password</code>. This command does not affect other users on the system, and all settings are preserved.</td>
<td>✓</td>
</tr>
<tr>
<td>restart</td>
<td>Restarts the LEM Manager service. This will take the Manager offline for 1–3 minutes.</td>
<td>✓</td>
</tr>
</tbody>
</table>
### COMMAND | DESCRIPTION | RESTART REQUIRED
--- | --- | ---
sensortoolupgrade | Upgrades the LEM Manager's Sensor Tools from the command line. This command does not support cd rom and floppy options - only SB. | |
showlog | Allows you to page through the LEM Manager's log file. | |
showmanagermem | Displays the LEM Manager's configured memory utilization settings. | |
start | Starts the LEM Manager service. If the Manager is already started, then nothing will happen. | ✓
stop | Stops the LEM Manager service. This makes the Manager inactive until it is started again. | ✓
support | This command has been deprecated. Use the debug command. | |
togglehttp | Enables or disables HTTP on port 80. | ✓
viewsysinfo | Displays appliance settings and other information that is useful for support and troubleshooting. | |
watchlog | Displays 20 lines of the current LEM Manager log file and monitors the log for further updates. Any new log entries appear as they are written to the log. | |

### LEM CMC nDepth menu

The `cmc::ndepth>` menu includes commands for managing one or more nDepth VMs or appliances.

> See [About the CMC command line](#) for information about using the CMC command line.

Type the `ndepth` command at the main menu to open the `cmc::ndepth>` prompt. Commands available from the ndepth menu are listed in the following table in alphabetical order. A ✓ in the "Restart Required" column indicates that a command requires an automatic restart of the LEM Manager service. See [Start and Stop LEM components](#) for help.

### COMMAND | DESCRIPTION | RESTART REQUIRED
--- | --- | ---
exit | Exits the nDepth menu and returns to the main menu. | |
logmarchiveconfig | Sets the Log Message archive share settings. | |
logmbackupconfig | Sets the Log Message backup share settings. | |
### LEM CMC service menu

The `cmc::service>` menu includes commands for managing restrictions and SSH access.

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
<th>RESTART REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>restart</td>
<td>Restarts the Log Message search/storage service.</td>
<td>✓</td>
</tr>
<tr>
<td>start</td>
<td>Starts the Log Message search/storage service.</td>
<td></td>
</tr>
<tr>
<td>stop</td>
<td>Stops the Log Message search/storage service.</td>
<td></td>
</tr>
</tbody>
</table>

Find more information on nDepth log retention and additional database requirements [here](#).

#### Table of Commands

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
<th>RESTART REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>disableflow</td>
<td>Disables the flow Collection Service on the appliance (and in the SolarWinds Explorer).</td>
<td></td>
</tr>
<tr>
<td>enableflow</td>
<td>Enables the flow Collection Service on the appliance (and in the SolarWinds Explorer).</td>
<td>✓</td>
</tr>
<tr>
<td>exit</td>
<td>Exits the service menu and returns to the main menu.</td>
<td></td>
</tr>
<tr>
<td>help</td>
<td>Displays a brief description of each command within the service menu.</td>
<td></td>
</tr>
<tr>
<td>restartssh</td>
<td>Restarts the SSH service. If the SSH service is running, this command stops and then restarts the service.</td>
<td></td>
</tr>
<tr>
<td>restrictconsole</td>
<td>Restricts access to the LEM console to only certain IP addresses or hostnames. This command prompts you to provide the IP addresses or hostnames that should be allowed access. Once the restriction is in place, only the listed IP addresses or hostnames can connect to the LEM console. Also see unrestrictconsole.</td>
<td></td>
</tr>
</tbody>
</table>

Type the `service` command at the main menu to open the `cmc::service>` prompt. Commands available from the service menu are listed in the following table in alphabetical order. A ✓ in the "Restart Required" column indicates that a command requires an automatic restart of the LEM Manager service. See [Start and Stop LEM components](#) for help.
<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
<th>RESTART REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>restrictreports</td>
<td>Restricts access to reports to only certain IP addresses or hostnames. This command prompts you to provide the IP addresses or hostnames that should be allowed access. Once the restriction is in place, only the listed IP addresses or hostnames can create and view reports. Also see unrestrictreports.</td>
<td></td>
</tr>
<tr>
<td>restrictssh</td>
<td>Restrict the SSH service to only certain IP addresses. This command prompts you to provide the IP addresses that should be allowed access. Once the restriction is in place, only the listed IP address and user combinations can connect to the LEM Manager using the SSH service. Also see unrestrictssh.</td>
<td></td>
</tr>
<tr>
<td>snmp</td>
<td>Configures the SNMP Services.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- See <a href="https://www.solarwinds.com/support/article/articledetails.aspx?articleid=60022">Enable LEM to receive SNMP traps by turning on the SNMP Trap Logging Service</a> to configure LEM to receive SNMP traps.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- See <a href="https://www.solarwinds.com/support/article/articledetails.aspx?articleid=72888">Monitor LEM from NPM and the Orion Web Console using SNMP</a> to configure LEM and NPM to monitor LEM's CPU, memory, and other critical components.</td>
<td></td>
</tr>
<tr>
<td>startssh</td>
<td>Starts the SSH service.</td>
<td></td>
</tr>
<tr>
<td>stopopsec</td>
<td>Terminates any connections from the LEM Manager VM to Check Point® Open Platform for Security (OPSEC) hosts.</td>
<td></td>
</tr>
<tr>
<td>stopssh</td>
<td>Stops the SSH service. If you issue this command, you can only access the LEM Manager with a keyboard and monitor until you issue a reboot command.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To restrict access to the SSH service (outside of the user name and password requirements), see the restrictssh command.</td>
<td></td>
</tr>
<tr>
<td>unrestrictconsole</td>
<td>Removes access restrictions placed on the LEM console. The only remaining protection is the user name and password combination. This command removes all other restrictions and allows system users with a user name and password to connect to the console.</td>
<td></td>
</tr>
<tr>
<td>COMMAND</td>
<td>DESCRIPTION</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>unrestrictreports</td>
<td>Removes access restrictions placed on the LEM reports application. The only remaining protection is the user name and password combination. This command removes all other restrictions and allows anyone who has either the reports application or any alternative database connection software installed, to create and view reports and browse the database, provided that they have a valid username and password.</td>
<td></td>
</tr>
<tr>
<td>unrestrictssh</td>
<td>Removes access restrictions placed on the SSH service. The only remaining protection is the user name and password combination</td>
<td></td>
</tr>
</tbody>
</table>
LEMA console help

This section documents the screens that make up the LEM web console and desktop console.

About the LEM console

Use the console to manage and monitor LEM. This documentation topic applies to both the desktop console and the web console.

To open the LEM console, see Log in to the LEM web console or Log in to the LEM desktop console for steps.

The LEM console displays normalized information about the events on your monitored devices in real time. The items in this section address how to use the LEM console to view, respond to, and search for these events on a day-to-day basis. Unless otherwise stated, the functionality described in this section is identical between the web and desktop consoles.

Click the video icon for a video tour of the LEM console.

Console Views

The console is organized into functional areas called views. These views organize and present different information about the components that comprise the LEM system.

The views are located in the toolbar. You can access six top-level views in the console.

- **Ops Center** provides a graphical representation of your log data. It includes several widgets that help you identify problem areas and show trends in your network. You can select additional widgets from the widget library or add custom widgets that reflect your log activity.
- **Monitor** displays events in real time as they occur in your network. You can view the details of a specific event or focus on specific types of events. This view also includes several widgets to help you identify trends or anomalies that occur in your network.
- **Explore** provides tools for investigating events and related details.
  - Select nDepth to search or view event data or log messages.
  - Select Utilities to view additional utilities, such as Whois and NSlookup.
- **Build** creates user components that process data on the LEM Manager.
  - Select Groups to build and manage groups.
  - Select Rules to build and manage policy rules.
  - Select Users to add and manage console users.
- **Manage** manages properties for appliances and nodes.
  - Select Appliances to add and manage appliances.
  - Select Nodes to add and manage Agents.
- **Analyze** is a placeholder for future improvements.

**Grids**

Grids are used throughout the console. Using Grids, you can perform common tasks such as selecting rows and grid cells, resizing grid columns, rearranging grid columns, and sorting a grid by columns.

**Rearrange grid columns**

Rearrange the grid column order to meet your needs. The columns remain in your set order until you exit the console. When you reopen the console, the columns return to their default order.

To rearrange a grid column, click and drag the column header to a new position.

```
<table>
<thead>
<tr>
<th>Last Name</th>
<th>Role</th>
<th>Manager</th>
<th>Description</th>
<th>Last Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>last-name</td>
<td>Administrator</td>
<td>trigo-demo50</td>
<td>Fri Jul 17 2009</td>
<td></td>
</tr>
<tr>
<td>Puffinstuff</td>
<td>Contact</td>
<td>trigo-demo50</td>
<td>All around great</td>
<td>Wed Dec 31 196</td>
</tr>
<tr>
<td>McCavity</td>
<td>Administrator</td>
<td>trigo-demo50</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Sort a grid by columns**

Sort grid data in each view by clicking the column headers. Each column can be sorted in ascending or descending order.

To sort a grid by one column, click the selected column header. The ▲ indicates sorting in ascending order (from A to Z). The ▼ indicates sorting in descending order (from Z to A).

In the Monitor view, you can sort a grid by multiple columns by pressing the Ctrl key and clicking each column header. The sorting order number is displayed next to ▲ or ▼ in each selected column.

Before you sort the Monitor view event grid, click Pause to stop the incoming event traffic. Click Resume to start the incoming event traffic.

**LEM console grid column and data field descriptions**

The following table explains the meaning of each grid column or data field that can appear in various alert grids, event grids, and information panes throughout the Console. The actual columns and fields that are shown vary according to the alert, view, or grid you are working with. But the meaning of these fields remains the same, regardless of where you see them.

For convenience, the fields are listed in alphabetical order.
<table>
<thead>
<tr>
<th>Grid Column or Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventName</td>
<td>The name of the event.</td>
</tr>
<tr>
<td>ConnectionName</td>
<td>The name of the dial-up or VPN connection.</td>
</tr>
<tr>
<td>ConnectionStatus</td>
<td>The current status of the dial-up or VPN connection.</td>
</tr>
<tr>
<td>DestinationMachine</td>
<td>The destination IP address of the network traffic.</td>
</tr>
<tr>
<td>DestinationPort</td>
<td>The destination port number of the network traffic.</td>
</tr>
<tr>
<td>DetectionIP</td>
<td>The source network node for the alert data. This is usually a Manager or an Agent and is the same as the InsertionIP field. It can also be a network device, such as firewall or an intrusion detection system that may be sending log files over a remote logging protocol.</td>
</tr>
<tr>
<td>DetectionTime</td>
<td>The time the network node generated the data. This is usually the same as the InsertionTime field, but they can differ when the Agent or Manager is reading historical data, or if a network device has an incorrect time setting.</td>
</tr>
<tr>
<td>EventInfo</td>
<td>A short summary of the alert details. Additional details appear in the following fields, but EventInfo provides enough information to view a “snapshot” of the alert information.</td>
</tr>
<tr>
<td>ExtraneousInfo</td>
<td>Additional information relevant to the alert, but not reflected in other fields. This can include information useful for correlating or summarizing alert information in addition to the EventInfo field.</td>
</tr>
<tr>
<td>Host</td>
<td>The node the log message came from (the LEM or Agent that collected the message for forwarding to nDepth).</td>
</tr>
<tr>
<td>HostFromData</td>
<td>The originating network device (if different than the node) that the message came from. Normally, Host and HostFromData are the same, but in the case of a remote logging device (such as a firewall) this field reports the original remote device's address.</td>
</tr>
<tr>
<td>InferenceRule</td>
<td>The name of the correlation that caused this alert. The InferenceRule field will generally be blank, but in cases where the alert was related to a rule, it displays the rule name.</td>
</tr>
<tr>
<td>InsertionIP</td>
<td>The Manager or Agent that first created the alert. This is the source that first read the log data from a file or other source.</td>
</tr>
<tr>
<td>InsertionTime</td>
<td>The time the Manager or Agent first created the alert. This time indicates when the data was read from a log file or other source.</td>
</tr>
<tr>
<td>IPAddress</td>
<td>The IP address associated with the alert. This is a composite field, drawn from several different alert fields. It shows all the IP addresses that appear in alert data.</td>
</tr>
<tr>
<td><strong>GRID COLUMN OR FIELD</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Manager</td>
<td>The name of the Manager that received the alert. For data generated from an Agent, this is the Manager the Agent is connected to.</td>
</tr>
</tbody>
</table>
| Order                    | In the Event explorer's event grid, the Order field indicates when each event occurred:  
  - ✈️ indicates the event occurred before the central event shown in the event map.  
  - 🔔 indicates the event occurred during (as part of) the central event shown in the event map.  
  - ⏳ indicates the event occurred after the central event shown in the event map. |
| Protocol                  | Displays the protocol associated with this alert (TCP or UDP). |
| ProviderSID               | A unique identifier for the original data. Generally, the ProviderSID field includes information that can be used in researching information on the alert in the originating network device vendor's documentation. |
| SourceMachine             | The IP address the network traffic is coming from. |
| SourcePort                | The port number the network traffic is coming from. |
| ConnectorAlias            | The Alias Name entered when configuring the connector on the Manager or Agent. |
| ConnectorId               | The actual connector that generated the log message. |
| ConnectorType             | Connector category for the connector that generated the log message. |
| Username                  | The user name associated with the alert. This is a composite field, drawn from several different alert fields. It shows all the places that user names appear in alert data. |

### Ops Center view in the LEM console

Choose Ops Center in the LEM console to open the Ops Center view. Use this view to monitor network and system events using widgets. Widgets provide special dashboard functionality, such as displaying real-time information, or providing tools for investigating events and related details.

ℹ️ This topic provides page-level help for the Ops Center view in the LEM console.

See also: [LEM widgets and the Ops Center: Visually monitor network events in LEM](#)
This screen capture shows the Ops Center view in the LEM console:

The following table describes the default UI elements on the Ops Center view page:

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget Manager</td>
<td>Opens and closes the Widget Manager. The Widget Manager includes the Categories and Widgets panes.</td>
</tr>
<tr>
<td>Getting Started</td>
<td>Tips and shortcuts to get you started configuring and exploring LEM.</td>
</tr>
<tr>
<td>Node Health</td>
<td>A status view of each device monitored by LEM.</td>
</tr>
<tr>
<td>THWACK Community &amp; Support</td>
<td>Access to useful information from the THWACK community.</td>
</tr>
<tr>
<td>Top 10 Events</td>
<td>Displays the top 10 events in the selected time range.</td>
</tr>
<tr>
<td>Help</td>
<td>Links to different resources to help you learn more about LEM</td>
</tr>
<tr>
<td>What's New in LEM</td>
<td>A list of items added or improved in this version.</td>
</tr>
<tr>
<td>Events per Minute</td>
<td>Displays the total count of events per minute for the past 15 minutes.</td>
</tr>
<tr>
<td>Custom Widget</td>
<td>Displays an example of what you can create on a custom widget.</td>
</tr>
<tr>
<td>Top 10 Nodes by # of Events</td>
<td>Displays the top 10 most active nodes (by number of events).</td>
</tr>
<tr>
<td>Top 10 Users by # of Events</td>
<td>Displays the top 10 users with the most events in the selected time range.</td>
</tr>
<tr>
<td>NAME</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Network Events by Source Machine</td>
<td>Displays the top 10 machines generating network events.</td>
</tr>
<tr>
<td>User Logons by Source Machine</td>
<td>Displays the top 5 user logons by source machine.</td>
</tr>
<tr>
<td>Data Simulator</td>
<td>Plays back different kinds of simulated network data.</td>
</tr>
<tr>
<td>Top 10 Rules by Number of Rules Fired</td>
<td>Displays the top 10 most commonly triggered rules and how many times each rule was triggered over a selected time.</td>
</tr>
</tbody>
</table>

The User Details widgets

In the Top 10 Users by # of Events widget, click a user to open the User Details page. Every user has a User Details page that displays all related information, including all events for the selected user.

This screen capture shows the User Details page, which contains the User:Details and User:All Events widgets.

The User: Details widget

This widget displays detailed user information, such as user name, Manager, user type, and so on.

The User: All Events widget

This widget displays all event statistics generated by the selected user with a corresponding graph. Click an event to see the Event Details page for the selected event.

The User:All Events menus allow you to:

- Filter events by event group
- Switch between Grid and Details views
- Filter events by date and time

Color-coding allows you to easily locate events that may need attention. A green line on a graph represents informational events. A yellow line represents warning events. And a red line represents critical events.

The Node Details widgets

In the "Top 10 Nodes by # of Events" widget, click a node to open the Nodes Details page. This page displays an overview about every device monitored by LEM.

This screen capture shows the Nodes Details page, which contains the "Node: Details," "Node: Connectors Applied," and "Nodes: All Events" widgets.

The Node: Details widget

This widget displays detailed information about the specified node, such as node IP, node name, last event, and so on.
The Node: Connectors applied widget

This widget provides a list of connectors configured for the selected node and whether the connectors are enabled or disabled. You can also turn the connectors on or off and configure new connectors.

The Node: All events widget

This widget lists all events generated by the selected node and displays statistics of the events in a graph. Click an event to view the Event Details page for the selected event.

Using this widget, you can filter events by event group, switch between Grid and Details views, and adjust the view from the last ten minutes to last week.

Color-coding allows you to highlight events that may need attention. A green line on a graph represents informational events; a yellow line represents warning events; and a red line represents critical events.

The Widget Manager and Widget Builder

Use the Widget Manager to select widgets to add to a dashboard. Use the Widget Builder to create a new widget or edit an existing widget.

This topic provides page-level help for the Widget Manager and Widget Builder pages in the LEM console. For more information, see:

- Manage LEM widgets with Widget Manager: Add, edit, and more
- Create and edit widgets with Widget Builder

This screen capture shows the Widget Manager portion of the Ops Center view in the LEM console:

The Widget Manager UI

The following table describes the Widget Manager UI elements:

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories pane</td>
<td>Lists widgets you can add to the dashboard by category.</td>
</tr>
<tr>
<td></td>
<td>The Name column lists each available widget filter with one or more master</td>
</tr>
<tr>
<td></td>
<td>widgets.</td>
</tr>
<tr>
<td></td>
<td>The Count column lists the number of widgets associated with each filter.</td>
</tr>
</tbody>
</table>
|                    | Click the Name or Column headers to rearrange the categories by name or count.
| +                  | Opens the Widget Builder to add a new master widget to the selected category.|
| ⚙️                 | Opens the Widget Builder to edit the selected widget in the Widgets pane.    |
## Widget Builder UI

Enter the general widget settings

1. In the Name field, enter a name for the widget.

2. In the Description field, enter a description for the widget (up to 80 characters).

3. From the Filter drop-down list, select the filter data source.

   When you select your filter data source, use the following conventions:
   - If the filter appears in italics, the filter is turned off.
   - If you create a widget from a disabled filter, the widget will not display any chart information until the filter is re-enabled.
   - When you create a widget in the Monitor tab, this field defaults to the currently-active filter. If you select a different filter, the widget will be associated with your targeted filter and not the active filter.
   - When you create a widget in the Ops Center tab, this field defaults to the first option in the list.

4. Enter the visual configuration settings.
Enter the visual configuration settings

1. From the Visualization Type drop-down list, select the appropriate graph.

![Visual Configuration Settings](image)

2. Click Color and select a color palette for the chart or graph.
3. (Optional) In the X Axis Label field, enter a name for the chart or graph horizontal axis.
4. (Optional) In the Y Axis Label field, enter a name for the chart or graph vertical axis.
5. Enter the data configuration settings.

Enter the data configuration settings

1. From the Field drop-down list, select a data field to report in the widget.

![Data Configuration Settings](image)

2. From the Show drop-down list, select the data frequency reported in the widget.
   - Select Count to count the number of occurrences for the selected Field value. For example, if you select EventID in the Field drop-down menu, the widget will count the number of events.
   - Select Distinct Count to count the number of occurrences when a unique event occurs. For example, if you select a Field value such as Event Name or Detection IP, the widget counts each specific value once. This option reports all values as 1 in a single-dimension chart. As a result, this option is best suited for multidimensional charts.
3. From the Sort drop-down list, select the data sort method.
   a. Select Descending to list the data from highest to lowest (Z to A or 10 to 1).
   b. Select Ascending to list the data from lowest to highest (A to Z or 1 to 10)
4. For a second data dimension in the chart, select another data field from the Versus drop-down list (optional).
5. For a third data dimension in the chart, select another data field from the Split By drop-down list...
6. From the Limit drop-down list, select a value that limits the number of items to chart.
   The default value is 5.

7. From the Scope drop-down lists, select the appropriate time frame reported by the chart or graph.
   For example, selecting a scope of 30 minutes will display the last 30 minutes of data in the chart or graph.
   Choose a narrow scope for frequent events. Choose a wide scope for events that rarely occur.

8. From the Resolution drop-down lists, select the time values (displayed as tick marks) for the horizontal X-axis in the chart. This value is required when Versus is a time field.
   For example, if your Scope is 30 minutes, you can set the Resolution to five minutes to indicate five-minute tick marks on the X-axis.

9. From the Refresh drop-down lists, select the data refresh rate for the widget display.

10. Click Save.
Monitor view in the LEM console

Monitor view displays all monitored events on your network in real time. It includes features to help you review and analyze current events on your network.

This topic provides page-level help for the Monitor view in the LEM console.

See also:
- About LEM filters and filter categories
- LEM filters: Capture real-time events and historical data with filter criteria

This screen capture shows the Monitor view in the LEM console:

Monitor view includes:

- An All Events pane that displays a real-time event stream where you can apply event filters.
- An Events Details pane that displays details for any event you highlight in the event stream.
- A Widgets pane that displays a graphical representation of the current filter (if available).
- Several default filters to refine the data you see in the event stream.
- A GUI filter editor called Creation to create and edit event filters.
The Filters pane

The Filters pane stores all filters you can apply to the console event messages.

All filters are stored in groups. To add a filter to the events grid, click a filter group and then click a filter. The events grid title changes to the name of the event and the grid refreshes and displays the incoming events allowed by the filter conditions.

Click 🗂️ to create your own custom filters and filter groups. Click 📝 to edit, pause, resume, turn on, turn off, import, export, or delete filters.

The Filter Notifications pane

The Filter Notifications pane summarizes the event activity from your active notification filters that use blink, pop-up, or sound notifications. Click a filter name to view the events associated with the targeted filter.
The Events grid

The Events grid displays the events that occur for your selected filter. This grid displays each event that occurs for your selected filter, as well as every event logged to each Manager. The title bar displays the filter name you selected in the Filters pane.

<table>
<thead>
<tr>
<th>EventName</th>
<th>EventInfo</th>
<th>InsertionID</th>
<th>Manager</th>
<th>DetectionID</th>
<th>InsertionTime</th>
<th>DetectionTime</th>
<th>Severity</th>
<th>ToolBar</th>
<th>TimeFormat</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestTraffic</td>
<td>URL access by 192.168.199.10</td>
<td>test1</td>
<td>user1</td>
<td>192.168.167</td>
<td>15:00:00 Oct 02 2016</td>
<td>15:00:00 Oct 02 2016</td>
<td>P</td>
<td>N</td>
<td>1</td>
<td>P</td>
</tr>
<tr>
<td>TestTraffic</td>
<td>DHCP Request from 192.168.199.10</td>
<td>user2</td>
<td>user1</td>
<td>192.168.168</td>
<td>15:00:00 Oct 02 2016</td>
<td>15:00:00 Oct 02 2016</td>
<td>P</td>
<td>N</td>
<td>1</td>
<td>P</td>
</tr>
<tr>
<td>Application</td>
<td>Privileged User Operation from &quot;CORP-PC01&quot;</td>
<td>user3</td>
<td>user2</td>
<td>192.168.168</td>
<td>15:00:00 Oct 02 2016</td>
<td>15:00:00 Oct 02 2016</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>TestTraffic</td>
<td>URL access by 192.168.199.10</td>
<td>test1</td>
<td>user1</td>
<td>192.168.167</td>
<td>15:00:02 Oct 02 2016</td>
<td>15:00:02 Oct 02 2016</td>
<td>P</td>
<td>N</td>
<td>1</td>
<td>P</td>
</tr>
<tr>
<td>NetworkLogoff</td>
<td>Logoff &quot;CORP-PC01&quot;</td>
<td>user4</td>
<td>user3</td>
<td>192.168.168</td>
<td>15:00:00 Oct 02 2016</td>
<td>15:00:00 Oct 02 2016</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>UserLogoff</td>
<td>Logoff &quot;DANNYJohns&quot;</td>
<td>user5</td>
<td>user4</td>
<td>192.168.168</td>
<td>15:00:01 Oct 02 2016</td>
<td>15:00:01 Oct 02 2016</td>
<td>P</td>
<td>N</td>
<td>1</td>
<td>P</td>
</tr>
<tr>
<td>Unauthorized</td>
<td>Unauthorized login from &quot;127.0.0.1&quot; for &quot;bulletin&quot;</td>
<td>user6</td>
<td>user5</td>
<td>192.168.168</td>
<td>15:00:00 Oct 02 2016</td>
<td>15:00:00 Oct 02 2016</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>TestTraffic</td>
<td>Secure URL Access By unauthorized user</td>
<td>user7</td>
<td>user6</td>
<td>192.168.168</td>
<td>15:00:00 Oct 02 2016</td>
<td>15:00:00 Oct 02 2016</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>TestTraffic</td>
<td>Bypass URL Decode Encoding</td>
<td>user8</td>
<td>user7</td>
<td>192.168.168</td>
<td>15:00:00 Oct 02 2016</td>
<td>15:00:00 Oct 02 2016</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>TestTraffic</td>
<td>URL access by 192.168.199.10</td>
<td>test1</td>
<td>user1</td>
<td>192.168.167</td>
<td>15:00:00 Oct 02 2016</td>
<td>15:00:00 Oct 02 2016</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>MachineLogoff</td>
<td>Logoff &quot;CORP-PC01&quot;</td>
<td>user9</td>
<td>user8</td>
<td>192.168.168</td>
<td>15:00:00 Oct 02 2016</td>
<td>15:00:00 Oct 02 2016</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

As the Agents monitor each configured data source on your network, they send the events to each Manager. In turn, the event grid displays the events logged to each Manager that is connected to the console. By default, incoming events always appear at the top of the grid, allowing the Monitor view to always display the most recent activity.

The toolbar includes additional options:

- **Respond**: Click this option to respond to a particular event message. For example, you can choose to block an IP address, or restart or shut down machine that is the event activity source.
- **Explore**: Click this option to select a particular event message or one of its specific data elements with an explorer. The selected cell (or string) determines the explorers you can choose.
- **Pause**: Click this option to stop the event traffic reported by the filter. When finished, click Resume to continue.
- **Highlight Selected Row(s)**: Click ![highlight](highlight.png) to highlight rows in the Events grid with a selected color.
- **Settings**: Click ![settings](settings.png) and select an option to mark messages as read or unread, remove messages, or copy event information.
The Widget pane

The Widget pane displays the widgets associated with the filter currently applied to the events grid. Widgets automatically refresh themselves to reflect changes in events grid filtering.

![Widget pane example](image)

You can view the widgets associated with this filter by clicking the drop-down list and selecting an option.

You can also:

- Click ▼ to change the presentation format (such as pie chart, bar chart, and so on).
- Click + to create a new widget.
- Click ▶ to open Widget Builder and create a new widget.
- Click ◾ to display the widget legend.
- Hover your mouse over a format item to view specific information.

Change the widget display for a selected filter

1. In the LEM console, click Monitor.
2. In the Filters pane, maximize a category and click the filter you want to modify.
3. In the Widgets pane, click the drop-down list and select the widget you want your filter to display.
The Event Details window

The Event Details pane displays specific information about the last event you selected in the Events grid. When you click an event, the event is highlighted in the Event Details pane, along with supporting information. To view the event details for a specific event, select the event in the event stream and review the results in the Event Details pane.

<table>
<thead>
<tr>
<th>Event Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Name</td>
<td>VirusAttack</td>
</tr>
<tr>
<td>EventInfo</td>
<td>Virus &quot;TROJ_CONHOOK.AA&quot; detected, File quarantined</td>
</tr>
<tr>
<td>InsertionIP</td>
<td>wallace</td>
</tr>
<tr>
<td>Manager</td>
<td>scotdmoore04</td>
</tr>
<tr>
<td>DetectionIP</td>
<td>192.168.168.6</td>
</tr>
<tr>
<td>InsertionTime</td>
<td>9:43:01 Tue Nov 03 2015</td>
</tr>
<tr>
<td>DetectionTime</td>
<td>9:43:01 Tue Nov 03 2015</td>
</tr>
<tr>
<td>Severity</td>
<td>6</td>
</tr>
<tr>
<td>ToolAlias</td>
<td>OfficeScan</td>
</tr>
<tr>
<td>InferenceRule</td>
<td></td>
</tr>
<tr>
<td>ProviderSID</td>
<td>ofcService 500</td>
</tr>
<tr>
<td>ExtraneousInfo</td>
<td></td>
</tr>
<tr>
<td>VirusDetected</td>
<td>TROJ_CONHOOK.AA</td>
</tr>
<tr>
<td>SourceAccount</td>
<td>djonesa</td>
</tr>
</tbody>
</table>

You can also:

- Click 📏 to create a filter for this event.
- Click ⬅ to view the previous or next event.
- Click 🎯 to view the event description.
- Click ⬅️ to return to the event details.

The window fields vary according to your selected event type. For example, network-oriented events display IP addresses and ports in the window. Account-oriented events display account names and domains. The window may also include a severity level.

Click ⬆️ or the up and down arrow keys to select the previous or next event in the events grid.
Event Description window

The Event Description window displays a description of your selected event in the events grid.

![Event Description](image)

TCPTrafficAudit events are a specific subset of CoreTrafficAudit events where the protocol is known to be TCP.

TCPTrafficAudit events may indicate normal traffic inside the network, normal traffic pass-through, denied traffic, or other non-application TCP traffic that is not known to have any immediate attack basis.

Click ✰ to review the event description.

Click ✰ to return to the Event Details window.

Click ✰ to select the previous or next event and event description in the events grid.

Event Severity Levels

Each event is assigned a number indicating its severity. The following table explains each severity level.

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Debug</td>
<td>Detailed event information used for debugging by SolarWinds engineers.</td>
</tr>
<tr>
<td>1</td>
<td>System Error</td>
<td>Part of the system is unusable.</td>
</tr>
<tr>
<td>2</td>
<td>Informational</td>
<td>SolarWinds informational messages only.</td>
</tr>
<tr>
<td>3</td>
<td>Normal Audit</td>
<td>Normal behavior, but could be part of a signature attack.</td>
</tr>
<tr>
<td>4</td>
<td>Normal Notice</td>
<td>Normal behavior that you should monitor.</td>
</tr>
<tr>
<td>5</td>
<td>Suspicious</td>
<td>Normal behavior under most circumstances, but should be investigated.</td>
</tr>
<tr>
<td>6</td>
<td>Threatening</td>
<td>Investigation and action is required.</td>
</tr>
<tr>
<td>7</td>
<td>Critical</td>
<td>Immediate action is required.</td>
</tr>
</tbody>
</table>
The Create a Filter From This Event button

Click in the Event Details or Event Description windows to create a new filter that captures the currently selected event type. When completed, the Monitor view opens with the new filter open in the events grid. The new filter appears in the Filters pane under the last selected filter. If required, you can edit the filter so it captures specific events. See Manage LEM filters: Add, edit, view, and more for help.

Response actions

The Respond drop-down list in Monitor view provides a list of actions you can execute for a specific event message.

Each Respond command opens the Respond form. This form includes data from the field you selected and options for customizing the action—similar to configuring the active response for a rule in the Rule Creation.

The Respond menu is context-sensitive. The event type or cell currently selected in the event grid determines which responses you can choose.

Select an event response

In the Respond form, you can use the default field information to complete the form.

1. In Monitor view, locate an event in the event grid, and then click Pause.
2. Select the event in the grid.
3. Click Respond, and then select an action.

   ! The drop-down list contains commonly-used actions. If your action does not appear in the list, select All Actions.

4. In the Respond form, click the Action drop-down list, and then verify the action to your selected event.

5. Complete any remaining fields in the form.
6. To execute the action, click OK.
7. To receive new events in the event grid, click Resume.
Select an event response using drag-and-drop text

In the Respond form, you can drag and drop information from the Event and Information fields into the configuration fields to complete the form. Use this method to add content to a blank configuration field or replace the content of an existing configuration field.

1. In Monitor view, locate an event in the event grid and click Pause.
2. Select the event in the grid.
3. Click Respond, and then select an action.

   The drop-down list contains commonly-used actions. If your action does not appear in the list, select All Actions.

4. In the Respond form, click the Action drop-down list and verify the action to your selected event.

5. In the Respond form's event information grid, scroll to locate the field that contains the data element needed to configure the action.
6. Drag an event field into the appropriate action configuration field.

7. Complete any remaining fields as required.
8. To execute the action, click OK.
9. To receive new events in the event grid, click Resume.

Explore options

See [The Utilities view](#).

Notifications

The Notifications tab at the bottom of the Monitor view page summarizes the event activity from each of your active notification filters that use blink, popup, or sound notifications. Click a filter name in this tab to view the events associated with the targeted filter.

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>Time</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB-Defender Events</td>
<td>10:43</td>
<td>105</td>
</tr>
</tbody>
</table>

Nodes

The Nodes tab at the bottom of the Monitor view page opens the Nodes screen in Manage view, allowing you to connect or disconnect from a Manager, add a Manager Agent, and configure rules, policies, and network security connectors that apply to each Manager.

Appliances

The Appliance tab at the bottom of the Monitor view page opens the Appliance screen in Manage view to add, configure, and maintain each virtual appliance associated with and monitored by the LEM system.

Appliances is used here as a generic term that includes Managers, as well as database, logging, network, and nDepth servers.

The Filter Creation form

Use the Filter Creation form to create or edit filters in Monitor view in the LEM console.

- LEM filters: Capture real-time events and historical data with filter criteria
- Create a new LEM filter for real-time monitoring
- Get started building custom filter expressions in LEM
The Filter Creation form

Use the Filter Creation form to create or edit a filter in Monitor view.

**COMPONENT** | **DESCRIPTION**
--- | ---
The Filter Creation sidebar (also called the List pane) | Contains categorized lists of events, event groups, event variables, groups, profiles, and constants you can use to create conditions for your filters.
If more than one Manager is linked to the console, each item in the list pane lists the associated Manager.
The Events list contains a search box and associated buttons that switch the view between tree and list views.

Name | Displays the filter name.
Lines Displayed | Selects the number of lines displayed in the screen.
Description | Displays the filter description.
Filter Status | Lists warnings and error messages about the current configuration logic in your filter.
Conditions | Defines the data conditions reported by the filter.
To configure a condition, drag items listed in the List pane into the Conditions box.
Notifications | Defines how the console responds to your event (such as a sound or pop-up message).
Undo | Reverts the screen to your last desktop action (up to 20 actions).
<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redo</td>
<td>Forwards the screen to your next saved desktop action (up to 20 actions).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves your filter changes.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels your filter changes.</td>
</tr>
</tbody>
</table>

The filters and groups list pane

The following screen capture shows the filters and groups list pane on the Filter Creation screen in Monitor view.

To open the list pane, click Monitor, then click Filters to open the Filters sidebar, and then choose New Filter or Edit from the ✎ or ₤ menus.

![Filters List](image)

This table describes each option on the Filter Creation screen sidebar in Monitor view.

<table>
<thead>
<tr>
<th>FILTER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>All console event types. Click 📃 to display the list as a hierarchical node tree. Click 📃 to list event types alphabetically, regardless of their position in the hierarchy.</td>
</tr>
<tr>
<td>Event Groups</td>
<td>Preconfigured groups of events used to initiate a specific event filter condition or rule creation.</td>
</tr>
<tr>
<td>User-Defined Groups</td>
<td>Groups of preferences used in rules and event filters to match, include, or exclude events, information, or data fields based on their membership with a particular group. In most cases, these groups are used in rules for choosing which events to include or to ignore. These groups apply to Managers and are created in the Group Builder.</td>
</tr>
<tr>
<td>Connector Profiles</td>
<td>Groups of Agents with common connector configurations. Use connector profiles with rules and filters to include or exclude Agents associated with a particular profile. You can create connector profiles in the Build &gt; Groups grid.</td>
</tr>
</tbody>
</table>
### Filter Description

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Service Groups</td>
<td>Preconfigured groups of network computers and system users you can use in rules and filters. They allow you to match, include, or exclude events to specific users or computers based on their group membership. These groups are synchronized through the Build &gt; Groups grid.</td>
</tr>
<tr>
<td>Time Of Day Sets</td>
<td>Specific groups of hours you can associated with rules and event filters. You can use time of day sets to enable your filters to include or exclude messages that occur during the hours associated with a particular time of day set, or to have your rules take different actions at different times of day. You can create time of day sets in the Build &gt; Groups grid.</td>
</tr>
<tr>
<td>Subscription Groups</td>
<td>All console user names, and the Manager associated with each user. Each name represents the list of rules subscribed to each individual user. When you add a subscription group to a filter, you can build the filter so it only displays events messages related to specific rules that a particular user is interested in (or “subscribed to”). You can create subscription rules in the Build &gt; Groups grid.</td>
</tr>
<tr>
<td>Constants</td>
<td>The constants rules and filters can use for comparing event data. These include text, number, and time.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Various notification methods the console can use to announce an event message for the filter. You can have the console display a pop-up message, display the new event as “unread,” play a sound, or have the filter name blink. You can also configure multiple notification methods for the same filter. This list only applies to filters.</td>
</tr>
</tbody>
</table>

### Managing events in Monitor view

This topic describes how to work with events in Monitor view.

This topic provides help for Monitor view in the LEM console. For Monitor view page-level help, see "The Monitor view" on page 1.

Events are messages created from Agent, Manager, and network device log entries. These log entries are processed (or normalized) to extract information and display the data in a common table format instead of the often-convoluted format you see in the source data. Monitor view displays all monitored events on your network in real time. It includes features to help you review and analyze current events on your network. The normalized events are sent from the Agent to the Manager for processing. At the Manager, the events are processed against your rules, sent to the database for archiving, and sent to the LEM console for monitoring.

When you click a filter in the Filters pane, inbound traffic is channeled through the filter and displayed in the events pane. You can pause the incoming event stream, sort and highlight the data, and respond to events with a corrective action. When completed, you can resume the incoming traffic that appears in the events grid.
To learn how to use LEM to view all real-time and historical activity from a single IP address, open the following URL in a web browser:

https://play.vidyard.com/wDGZ1B5oQdQ2BN1PXYQvbR

Review an event

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select a filter.
4. Locate an event in the event grid you want to explore.
5. To stop the event feed, click Pause.
6. Select the event in the grid.
7. From the Explore drop-down list, select Event.

   The Event explorer displays all events associated with your selected event. Your selected event name displays in the History pane.
   To view additional event information, click Event Details.

To apply a filter to the Monitor event stream

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. To open the Filters sidebar, click Filters in the upper-left corner.
4. Expand a filter category and select a default or custom filter from the Filters list.

   The events grid title bar displays the name of your selected filter, and the grid refreshed to display incoming events that match the conditions of your filter.

LEM saves event filters on the workstation running the LEM console. If you move to another workstation, you can export the filters to your new workstation and import them into the console.

To view the event details for a specific event in the event stream

1. Apply a filter to the Monitor event stream (as described above).
2. Select the event in the event stream and review the results in the Event Details pane.

Change the widget display for a selected filter

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, maximize a category, and then click the filter you want to modify.
4. In the Widgets pane, click the drop-down list, and then select the widget you want your filter to display.

To edit a widget chart presentation in Monitor view

Widgets displayed in Monitor view allow you to reconfigure the chart settings to suit your needs. These settings include the visualization type (line, bar, pie, or table), the color palette, and the X and Y axis labels.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Monitor dashboard, locate the widget you want to reconfigure.
4. On the widget toolbar, click  
   The widget rotates the interface to display the presentation format settings.
5. Reconfigure the widget settings as required.
   Your options are limited to the selected widget and the data it reports. For example, widgets that report in one dimension may be limited to a pie chart, while information in two dimensions can be reported in a bar or line chart.
6. Click  to close.
   The widget rotates, displaying the information in your chosen format.

Sort the events grid

You can sort the events in the events grid by clicking the appropriate column header. For example, if you click the Event Name column header, the grid sorts the filtered events by event name in ascending order. If you click the column header again, the events are sorted in descending order.

1. On the events grid toolbar, click Pause.
2. To sort your filtered events, click the appropriate column header.
3. When completed, click Resume to continue receiving filtered traffic.

Highlight events

In the Monitor view events grid, you can highlight events to call attention to them or mark them for future reference. This allows the events to stand out as you scroll through the contents of the grid. You can highlight multiple events at the same time. You can also choose the color you want for each set of events you are highlighting.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select a filter from a filter group.
4. To temporarily stop all incoming events, click Pause on the events toolbar.
Pausing incoming events is not required, but it places all events in static mode for review.

5. In the events grid, click the events you want to highlight.
   - To select two or more events, press <Ctrl>.

6. On the events grid toolbar, click to highlight a row with selected color or enter hexadecimal value.
   The events appear in your selected color.

7. To resume the incoming web traffic, click Resume.

Disable highlighted events

1. To temporarily stop all incoming events, click Pause on the events grid toolbar.
2. In the events grid, select the appropriate events to disable the highlight.
   - To select multiple events, press <Ctrl>.
3. On the events grid toolbar, click the drop-down list, and then select No Color.
4. To resume all incoming events, click Resume.

Copy event data to the clipboard

Copy event data for single or multiple events from the Monitor view events grid or Event Details pane to your clipboard. This allows you to paste the data into another application (such as Microsoft Excel for comparison or analysis), share the data with someone who does not have a console, or send to SolarWinds for technical support.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   - Click Monitor.
2. In the Filters pane, select a filter from a filter group.
3. In the events grid, select the event you want to copy.
   - To select two or more events, press <Ctrl>.
4. In the events grid, click 
   and then select Copy.
   The event data is now copied to your clipboard (as text).

Tag events as Read or Unread

You can mark events in event filter as unread and read. This process allows you to track examined and unexamined events.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Click Monitor.
2. In the Filters pane, select a filter from a filter group.
   The events grid displays your selected filter.
3. In the events grid, select the events you want to mark as read or unread.
4. To select two or more events, press <Ctrl>.
5. In the events grid, click 
   and then select one of the following options:
   - Mark Unread identifies one or more selected events as unread in bold text. Any events captured by other filters appear as unread in those filters as well.
   - Mark Read identifies one or more selected events as read in non-bold text.
   - Mark All Unread identifies all events as read in bold text.
   - Mark All Read identifies all events as read in non-bold text.
   The grid refreshes based on your selection.

Remove events

You can remove one or all events from a filter. This allows you to clean a filter of historical information that is no longer important.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Monitor.
3. In the Filters pane, select a filter from a filter group.
4. In the events grid, select the events you want to remove.
   To select two or more events, press <Ctrl>.
5. In the events grid, click 
   and then select Remove.
   Select Remove All to remove all events.
   The selected events are removed from the grid.
Explore view in the LEM console

The nDepth view

The nDepth search engine (Explore > nDepth) locates and analyzes events on your network.

This topic provides help for the nDepth view in the LEM console. For more information, see nDepth search: Explore event history using nDepth and other LEM utilities

The nDepth search view

The following illustration shows the nDepth view.

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>History</td>
<td>Displays links to your recent nDepth search results.</td>
</tr>
<tr>
<td>2</td>
<td>Saved Searches</td>
<td>Displays links to your saved nDepth search results.</td>
</tr>
<tr>
<td>3</td>
<td>Filters and groups sidebar</td>
<td>Displays categorized lists of events, event groups, event variables, and additional options you can use to create conditions for your filters.</td>
</tr>
<tr>
<td>4</td>
<td>Search bar</td>
<td>Searches all event data or the original log messages that pass through a LEM Manager. Drag the toggle switch to select Drag &amp; Drop or Text Search mode.</td>
</tr>
<tr>
<td>NUMBER</td>
<td>ITEM</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5</td>
<td>Respond</td>
<td>Displays a list of corrective actions you can execute when an event occurs, such as shutting down a workstation or blocking an IP address.</td>
</tr>
<tr>
<td>6</td>
<td>Explore</td>
<td>Displays several utilities you can use to research an event, including Whois, Traceroute, and NSlookup.</td>
</tr>
<tr>
<td>7</td>
<td>Time</td>
<td>Provides a drop-down list to select the time range for your search.</td>
</tr>
<tr>
<td>8</td>
<td>Play</td>
<td>Executes the selected search.</td>
</tr>
<tr>
<td>9</td>
<td>Histogram</td>
<td>Displays the number of events or log messages reported within the selected search time range.</td>
</tr>
<tr>
<td>10</td>
<td>Dashboard</td>
<td>Displays the search results in all available widgets. You can change this view by clicking a widget in the nDepth toolbar.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The icon indicates you are exploring event data. The icon indicates you are exploring log messages.</td>
</tr>
<tr>
<td>11</td>
<td>nDepth Toolbar</td>
<td>Organizes log data into categories to identify activity in your network. Click a selection to display the category below the histogram.</td>
</tr>
</tbody>
</table>

The nDepth history pane

Each nDepth explorer search adds an item to the Explore view history pane.

The icon represents an event data search. The icon represents an original log message search.

The following illustration displays an nDepth search of event data. When you hover over a history item, you can view the number of search results and your search string text.

![nDepth history pane illustration](image)

A new search adds a history item. If you click an earlier history item, the system takes you back to that search and does not make a new item. After you modify your nDepth search parameters and perform a new search, that search becomes a new history item.
The nDepth filters and groups list pane

Below is an example of the filters and groups list that appears in the Explore > nDepth view.

The following table describes each option in the filters and groups list pane.

<table>
<thead>
<tr>
<th>FILTER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine Fields</td>
<td>The top 100 data details for each field found in your nDepth search results. The details change, depending on whether you are searching event data or log messages. You can use these details to create, refine, or append nDepth search conditions. Click ABC to sort the details alphabetically within each category. Click 321 to sort the details by frequency within each category. The items that occur most often appear first within each category.</td>
</tr>
</tbody>
</table>
| Managers              | The various appliances monitored by the console. Use this list to select the Manager for your nDepth search. If you stored the original event log on a separate nDepth appliance, select this appliance to search that data.  
In Drag & Drop Mode, you can drag an item from this list into the search box to include that item in the search string. When using Search Builder, you can drag an item from this list into the Conditions box. |
<p>| Events                | All console event types. Click to display the list as a hierarchical node tree. Click to list event types alphabetically, regardless of their position in the hierarchy. |
| User-Defined Groups   | Groups of preferences used in rules and event filters to match, include, or exclude events, information, or data fields based on their membership with a particular group. In most cases, these groups are used in rules for choosing which events to include or to ignore. These groups apply to Managers and are created in the Group Builder. |
| Connector Profiles    | Groups of Agents with common connector configurations. Use connector profiles with rules and filters to include or exclude Agents associated with a particular profile. You can create connector profiles in the Build &gt; Groups grid. |</p>
<table>
<thead>
<tr>
<th>FILTER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Service Groups</td>
<td>Preconfigured groups of network computers and system users you can use in rules and filters. They allow you to match, include, or exclude events to specific users or computers based on their group membership. These groups are synchronized through the Groups grid.</td>
</tr>
<tr>
<td>Subscription Groups</td>
<td>All console user names, and the Manager associated with each user. Each name represents the list of rules subscribed to each individual user. When you add a subscription group to a filter, you can build the filter so it only displays events messages related to specific rules that a particular user is interested in (or “subscribed to”). You can create subscription rules in the Groups grid.</td>
</tr>
</tbody>
</table>

The nDepth search bar

The search bar provides a method to search all event data or the original log messages that pass through a LEM Manager. You can search logs from various devices using predefined search parameters (such as Change Management Events) or search for specific data using a text search. The toggle switch in the search bar allows you to switch between the drag-and-drop and text search modes.

The following table describes the key features of the nDepth search bar.

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode selector</td>
<td>Use this toggle switch to select how you intend to enter the search string for your queries:</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Drag &amp; Drop Mode</strong> (upper position) to drag items from the list pane or the <strong>Result Details</strong> view directly into the search box. This is the recommended position, as it is the easiest to use.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Text Input Mode</strong> (lower position) to type a search string directly in the search box. In this mode, the search box also shows the text version (or search string) of any search that is being run or configured in Search Builder or the Saved Searches pane.</td>
</tr>
<tr>
<td>Search box</td>
<td>This box contains your search conditions. You can enter search conditions many different ways.</td>
</tr>
<tr>
<td></td>
<td><strong>X</strong> Click a delete button next to a condition or a group to remove that condition or group from the current search configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>AND</strong> The search bar includes AND and OR operators. These operators let you include AND and OR relationships between conditions and groups of conditions, when you have multiple conditions in your search string. Click the operator icon to toggle between AND and OR relationships.</td>
</tr>
<tr>
<td></td>
<td><strong>OR</strong> When you have a group of conditions, the search bar displays the conditions as a summary. To see the actual conditions, point to them. A ToolTip appears that shows each condition in the group.</td>
</tr>
<tr>
<td></td>
<td><strong>X</strong> Click this <strong>Delete All</strong> button to delete the entire contents of the search box, so you can begin a new search.</td>
</tr>
</tbody>
</table>
**NAME** | **DESCRIPTION**
--- | ---
| | Click this button to begin a search, or to stop a search that is in progress.

- Click ⏯️ to begin searching.
- If the search button turns red ⚠️, it means the current search configuration is invalid.
- Click ✗ to stop a search that is in progress.

**Time selector**
In the time selector, select a time frame for the search. If needed, you can create your own custom time frame.

**Data selector**
Use this toggle switch to choose the data you want to nDepth to explore:

- Select **Events** (left position) to search LEM's normalized event data. This is the event data that appears in the **Monitor** view.
- Select **Log Messages** (right position) to search the actual log entries that are recorded on your network products' log files. If **Log Messages** is disabled, it means your equipment is either disabled, or it does not have the capacity to store and search the original log messages. However, you can still search the data in the **Events** position.

**Drag-and-drop search mode**

When the toggle switch is in the ✉️ (up) position, nDepth search is in Drag and Drop Mode. In this mode, you can drag items from the List pane or Results Details directly into the search box to initiate a search for a specific event.

![Drag search items here](drag_search_items.png)

In this mode, the search bar includes AND and OR operators. These operators let you include AND and OR relationships between conditions and groups of conditions, when you have multiple conditions in your search string.

For example, when you click a saved search, the search parameter populates the search bar. The icon at the end of the search bar indicates an OR operator.

![Change Management Events](change_management_events.png)

When you click the operator icon, it changes to the AND ✗ operator.

![Change Management Events](change_management_events.png)

Click ✗ next to a condition or a group to remove your condition or group from the current search configuration.

![The search bar synchronizes with Search Builder](search_builder.png)

The search bar synchronizes with Search Builder.
Creating search conditions

The following table describes how to add search conditions in Drag & Drop Mode and in Text Input Mode.

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear a search from the search box</td>
<td>Click Delete All ⌁ next to Play on the search bar.</td>
<td>Drag and Drop</td>
</tr>
<tr>
<td>Add a new search</td>
<td>Clear a search from the search box, and then add new search conditions using any method listed in this table.</td>
<td>Drag and Drop</td>
</tr>
<tr>
<td>Add conditions to an existing search</td>
<td>Use any method listed in this table. nDepth automatically adds new search conditions to the search string.</td>
<td>Drag and Drop</td>
</tr>
<tr>
<td>Add a search condition from a widget or other graphical tool</td>
<td>Click an item in a graphical tool to add that item to the search box.</td>
<td>Drag and Drop</td>
</tr>
<tr>
<td>Add a search condition from the list pane</td>
<td>In the Refine Fields list, double-click an item.</td>
<td>Drag and Drop</td>
</tr>
<tr>
<td>Add a search from Search Builder</td>
<td>Configure a search with Search Builder. Search Builder automatically populates the search bar with the search configuration. The search bar and Search Builder are different views of the same search.</td>
<td>Drag and Drop</td>
</tr>
<tr>
<td>Add a search condition from the Result Details view</td>
<td>Select a character string from the data, and then double-click the string to add it to the search box.</td>
<td>Drag and Drop</td>
</tr>
<tr>
<td>Type a string</td>
<td>Type a search string directly in the search box.</td>
<td>Drag and Drop</td>
</tr>
<tr>
<td>Perform the search</td>
<td>Click Play on the search bar.</td>
<td>Drag and Drop</td>
</tr>
</tbody>
</table>
The nDepth histogram

The nDepth histogram displays the number of events or log messages reported within your search time frame. nDepth returns search results chronologically so you can investigate a specific interval. You can minimize the search window to take a closer look or maximize the window to view additional activity.

nDepth's histogram summarizes event activity within a particular period. By default, the histogram displays the last 10 minutes of event activity. The bright zone shows the period that is currently being reported. The gray zones show activity outside of the reported period.

The bottom time bar is divided into one-minute intervals. The top bar is divided into 30-second intervals. The histogram displays a separate bar for each 30-second interval. Time is displayed in 24-hour (military) time.

Clicking a bar opens a pop-up window that shows a histogram for that bar's interval. Depending on range of the search's time frame, these intervals can be as little as 5-seconds. Pointing to a bar shows the total number of events that occurred in that interval. Clicking a bar opens a pop-up window to show a histogram for the selected interval.

When you switch to the Result Details view, the histogram displays two dashed vertical lines. These lines are markers, indicating where you are in the histogram for each page of the search results. The lines show the times of the first and last event on the current Result Details page.

By default, the ▲ shows the time of the first result on the page. If you select an event in the Result Details box, the pointer shows the time of that event.
When you view the search results of events number 1-200, the left line shows the time of event number 1, and the right line shows the time of event number 200. If you click event number 150, the ▲ shows the time that event occurred.

Search activity associated with a particular histogram bar

Use the histogram to search the event activity associated with a particular vertical bar in the histogram. To search activity for a bar, double-click a vertical bar. nDepth automatically refines the search and refreshes the data to show only the events from the time frame associated with that bar.

Adjust the search period

You can use the nDepth histogram to move the search period to an earlier or later start time. For example, when you search a 30-minute time frame, you can search the data for the same period, but adjust the search period within the 30-minute time frame.

1. Move your mouse pointer over the histogram.
2. Locate the gray slider that appears in the window.
3. Drag the slider to the left to move the period to an earlier starting point. Drag the slider to the right to move the period to a later starting point.

As you move the slider, a ToolTip displays the period’s midpoint time.

4. Click ▼ to run the search for the new time frame.

nDepth automatically refines the search and refreshes the data to display only the events from the new time frame. Modifying the period automatically changes the search bar time selector to Custom.

5. Click ◀ to restore the previous time frame (if desired).

Change the period start and end time

You can use the nDepth histogram to change the search period by changing its start time and end time. For example, if you run a search for a 30-minute period, you can expand the time frame (for example, 45 minutes) or reduce the time frame (for example, 20 minutes),

1. Move your mouse pointer over the vertical bar.
2. Drag the vertical bar to a new destination.
Drag the left or right slider to change the time frame start or end time, respectively. When you release the slider, a tooltip shows the new start time.

3. Click to run the search for the new time frame.

nDepth automatically refines the search and refreshes the data to show only the events from the new time frame. Changing the time frame automatically changes the search bar time selector to Custom.

4. Click to restore the previous time frame (if desired).

The nDepth explorer toolbar

This toolbar provides links to dashboards that display your data in different formats. You can also access Search Builder and details about your search results from the toolbar.

The following table describes the function of each option on the nDepth explorer toolbar. Each option provides a different view of the data from the most recent search.

<table>
<thead>
<tr>
<th>TOOL</th>
<th>VIEW</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>🛹️</td>
<td>Dashboard</td>
<td>Displays each nDepth view as a small widget. You can minimize and maximize each widget or edit the chart widgets to change their appearance. This is the default view.</td>
</tr>
<tr>
<td>🌉</td>
<td>Word Cloud</td>
<td>Displays keyword phrases that appear in your event data. Phrases appear in a size and color that relate to their frequency. You can filter this view to zero in on a range of activity or click a phrase to create or append a search based on that phrase.</td>
</tr>
<tr>
<td>TOOL</td>
<td>VIEW</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tree Map</td>
<td>Displays the items that appear most often in the data as a series of categorized boxes that correspond with the data categories in the Refine Fields list. The box size in each category is associated with its relative frequency. The more often an item occurs, the larger its box appears. You can hover over small boxes to open a tooltip and display its contents or click a box to create or append a search based on that item.</td>
<td></td>
</tr>
<tr>
<td>Bar Charts</td>
<td>A group of widgets that display your most frequent data items as a series of bar charts, which correspond to the relative frequency. The more often an item occurs, the larger its bar appears. You can hover over a bar to open a tooltip or click a bar to create or append a search based on that item.</td>
<td></td>
</tr>
<tr>
<td>Line Charts</td>
<td>A group of widgets that display your most frequent data items as a series of line graphs. The height of point on the graph corresponds with the item's relative frequency. The more often an item occurs, the higher the point appears on the graph. You can point to an item on the graph to show information about it. You can also click a point on the graph to create or append a search based on that item.</td>
<td></td>
</tr>
<tr>
<td>Pie Charts</td>
<td>A group of widgets that display your most frequent data items as a series of pie charts. The size of each pie wedge corresponds with the relative frequency. The more often an item occurs, the larger its wedge appears. You can hover over a wedge to view additional information or click a wedge to create or append a search based on that item.</td>
<td></td>
</tr>
<tr>
<td>Bubble Charts</td>
<td>A group of widgets that display your most frequent data items as a series of circles or bubbles. The size of each bubble corresponds with the relative frequency. The more often an item occurs, the larger its bubble appears. You can hover over a bubble to display additional information or click a bubble to create or append a search based on that item.</td>
<td></td>
</tr>
<tr>
<td>Result Details</td>
<td>A text-based view of the data you are investigating. This view also supports nDepth search capabilities. You can create or refine searches by dragging and dropping search strings from the data into the search box.</td>
<td></td>
</tr>
<tr>
<td>Search Builder</td>
<td>A graphical interface used to create and refine complex searches. You can drag items from the nDepth list pane directly into the Search Builder Conditions box to configure complex searches. Search Builder is similar to the Filter Creation tool.</td>
<td></td>
</tr>
</tbody>
</table>

The nDepth word cloud

The nDepth word cloud summarizes your event activity by displaying the top 100 keyword phrases that appear in your event messages.

Click in the toolbar to open the widget.
Phrases appear in a size and color that relates to their frequency. Phrases that appear in warm colors (red, orange, and yellow) and in larger print represent the phases that occur most frequently. These are your hot items.

Phrases that appear in cool colors (green and blue) and in smaller print occur with the least frequency. These are your cool items. Cool items may still be important. They just occur less frequently than hot items.

View Statistics in the word cloud

A word cloud includes statistics about each item listed in the cloud. To view your cloud statistics, point to a phrase in the word cloud. A tooltip appears, showing the keyword phrase, its count (the number of times it occurs in the reported period), and its percentage. The percentage is based on the relative frequency of the phrase compared to other reported phrases.

Filter the word cloud contents

Two horizontal bars display at the bottom of the word cloud. The top bar is a color gradient that goes from red (hot) to blue (cool). These colors correspond with the colors of the phrases displayed in the Word Cloud.

The lower bar controls which parts of the gradient the word cloud is allowed to display. You can use this bar to filter the word cloud so it only displays that section of the gradient you want to see. By default, the word cloud displays everything associated with the entire gradient—all items that are hot, cool, and in between.

By default, the word cloud displays the top 100 phrases, and the sliders are automatically adjusted to this width. If you manually adjust the sliders, nDepth remembers the left position and automatically adjusts the right position so the word cloud displays up to 100 phrases between the left and right positions. If all 100 phrases can be shown within the positions you've selected, the sliders will stay in place.

Slider settings are stored with each word cloud. As a result, you can create word clouds in the dashboard that are adjusted differently from the primary word cloud view.

To hide hot items, drag the lower bar's left-hand slider to the right. To hide cool items, drag the lower bar's right-hand slider to the left. To restore the Word Cloud, drag the sliders back to their far-left and far-right positions.
Exploring Items in the word cloud

You can use the word cloud to explore a particular phase, by using as the basis for a new search, or to append an existing search. To explore an item in the word cloud, click the phrase you want to explore. When the phrase appears in the search bar, click \( \rightarrow \) to show the results associated with your search.

The nDepth tree map

The tree map summarizes your event activity in categories based on common event data fields. The size of each box corresponds with the relative frequency of its occurrence. The more often a detail occurs, the larger its box appears.

Click the \( \rightarrow \) in the toolbar to open the widget.

Most categories correspond with actual event fields, as they appear in the Monitor view. When you are working with log messages, the tree map organizes into categories based on common log message data fields. Some data categories may not always be present. If there is no event activity associated with a particular data category or field, it will not appear in the tree map.

The items that appear in the tree map view are the same source files data field categories and values listed in the Refine Fields list at the top of the list pane. You can click and select an item from the tree map as a search condition. If a box is too small to show its contents, point to it to open a tooltip that displays its contents.

Resize tree map categories

To maximize a category, click \( \rightarrow \) in the targeted box toolbar. When maximized, a tree map category can show very small items within it. If a box is too small to show its contents, you can point to it to open a tooltip that shows its contents.

To restore a category to its proportional size, click \( \rightarrow \) icon in the targeted box toolbar.
Explore items in the tree map

You can use the Tree Map to explore a particular item by using the item as the basis for a new search, or to append an existing search. Click the item you want to explore. A search string for that item appears in the search bar. Click on the search bar. After a moment, nDepth refreshes to show the results associated with your search.

The Result Details view

The Results Details view displays the raw data displayed in the graphical views. You can create or refine searches by dragging and dropping search strings from the search data into the nDepth search box.

You can use Result Details in Events mode to view and search normalized event data found in the Monitor view or Log Messages mode to view and search the original log message data collected and stored on the LEM (or another dedicated nDepth appliance).

You can use your nDepth search results to refine your nDepth searches, explore event details with other explorers, or initiate an active response to event details.

Interpret search results in Events mode

Use Events mode to search all normalized event data reported in the Monitor view. This data is pulled from the LEM appliance.

The following table describes how to interpret your data search results in Events mode.

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event number</td>
<td>The incremented event number. Each row represents a new event.</td>
</tr>
<tr>
<td>Date and time</td>
<td>The time and date the event occurred.</td>
</tr>
<tr>
<td>stamp</td>
<td></td>
</tr>
<tr>
<td>Event name</td>
<td>The name of the event that occurred.</td>
</tr>
<tr>
<td>EventInfo</td>
<td>Additional information about the event. You can select these details to</td>
</tr>
<tr>
<td></td>
<td>refine your nDepth search, explore them with other explorers, or respond</td>
</tr>
<tr>
<td></td>
<td>to them with an active response.</td>
</tr>
</tbody>
</table>

Interpreting search results in Log Messages mode

In Log Messages mode, you can use nDepth to search all original log messages that pass through a particular network appliance (or host). Below is an example of the nDepth Result Details view with the original log message data.
The following table explains how to interpret search results of data in Log Messages mode.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Event number</td>
<td>The incremented event number. Each row represents a new event.</td>
</tr>
<tr>
<td>2</td>
<td>Data and time</td>
<td>The time and date the event occurred.</td>
</tr>
<tr>
<td></td>
<td>stamp</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Log message</td>
<td>The log message that matched your search criteria.</td>
</tr>
<tr>
<td>4</td>
<td>Host</td>
<td>The Manager or appliance that logged the message.</td>
</tr>
<tr>
<td>5</td>
<td>ToolId</td>
<td>The actual product or tool that generated the message.</td>
</tr>
<tr>
<td>6</td>
<td>ToolType</td>
<td>The SolarWind tool category that generated the message.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tool IDs and Tool Types match SolarWinds tool configuration categories.</td>
</tr>
</tbody>
</table>

Adding search strings from Result Details

Use the following procedures in the Results Details view to highlight and select character strings and create new search conditions from the data.

<table>
<thead>
<tr>
<th>TO</th>
<th>DO THIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selecting data</td>
<td></td>
</tr>
<tr>
<td>Highlight a continuous</td>
<td>Point to the character string.</td>
</tr>
<tr>
<td>character string</td>
<td></td>
</tr>
<tr>
<td>Select a continuous</td>
<td>Point to the character string to highlight it. Click the string to select</td>
</tr>
<tr>
<td>character string</td>
<td>it.</td>
</tr>
<tr>
<td></td>
<td>After you select a character string, an orange box surrounds the string.</td>
</tr>
<tr>
<td></td>
<td>Every matching character string in the search results is selected as</td>
</tr>
<tr>
<td></td>
<td>well.</td>
</tr>
<tr>
<td><strong>To</strong></td>
<td><strong>DO THIS</strong></td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Select a phrase (two or more character strings separated by spaces)</td>
<td>Click the first character in the string, and then drag across the string to select the remaining content. After you select a character string, an orange box surrounds the string. Every matching character string in the search results is selected as well.</td>
</tr>
<tr>
<td>Select a data row</td>
<td>Click the event number in the row. When the row is selected, an orange highlight bar appears to the left of the row.</td>
</tr>
</tbody>
</table>

**Creating search conditions from Result Details data**

| **Clear the search box to add a new search condition** | 1. On the search bar, click ✗ to clear the search box. 2. Add a new search condition by using any of the techniques in this table. |
| **Add a search condition from Result Details data** | 1. Select a character string in the data. 2. Double-click the selected string to add it to the search box. Select a character string in the data, and then drag it into the search box. |
| **Copy and paste a character string from Result Details data into the search box** | 1. Change the search bar to Text Input mode. 2. Select a character string in the data. 3. Copy the search string. 4. Click the search box, and then paste the character string into the text box. |
| **Type a search string in the search box** | 1. Change the search bar to Text Input mode. 2. Type the search string directly in the search box. |
| **Add conditions to an existing search** | 1. In the data, select the character string you want to append to the existing search conditions. 2. Double-click the selected string or drag the string into the search box. Your selection is appended to the existing conditions. |

**Using Explorers with Result Details**

Use the nDepth Result Details view to access additional explorers to investigate specific details that you find in your nDepth search results.

You can select specific values and pass them in to the value-based explorers (such as Whois, NSLookup, and Traceroute). For example, you can investigate a suspicious IP address with these explorers to learn more about that IP address.
When you view data in Events mode, each row in the search results represents the data for an individual event. You can select the row for an event you want to explore, and then pass the row into the Event Explorer to explore that event.

To explore details in search results:

1. Open the Result Details view.
2. Select the character string or row you want to explore.
   - Select the character string you want to investigate. When selected properly, the character string is surrounded by an orange box.
   - If you are viewing data in Events mode, select the row you want to explore in the Event Explorer. When you select a row, an orange highlight bar appears to the left of the row.
3. Click Explore and select the explorer you want to use.
   - The Explore > Utilities view appears, and the system passes the selected data to your selected explorer.
4. Click Search or Analyze to explore the string.

Search Builder

This section describes the main features of Search Builder.
The following table describes the Search Builder features.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Undo</td>
<td>Click to undo your last action. You can undo up to 50 steps.</td>
</tr>
<tr>
<td></td>
<td>Redo</td>
<td>Click to redo the last action. You can redo up to 50 steps.</td>
</tr>
</tbody>
</table>
| 2    | Search bar | Displays the current search parameters.  
If the search bar is in Drag and Drop mode, it displays your configuration search parameters, which match the parameters in the Conditions box. If the search bar is in Text Input mode, the search bar displays the current search parameter as a search string. |
| 3    | List pane | Contains categorized lists of events, event groups, event variables, groups, profiles, and constants you can use to creating conditions for your filters. For nDepth searches, you can only use the Refine Fields and Managers lists.  
The Refine Fields list summarizes all primary event details from your search results. The Managers list includes each Manager and appliance that can be used with nDepth for searching data. |
| 4    | Histogram pane | Investigates a specific time interval. Drag the left and right borders to increase or decrease the search time line. |
| 5    |         | Executes the search. |
| 6    | Conditions box | Defines the conditions for the data reported by the filter. Configure conditions by dragging items from the list pane into the Conditions box. |
| 7    |         | Adds a new group within the group box. A group within a group is a nested group.  
Each group is subject to AND and OR relationships with the groups around it and within it. By default, new groups appear with AND comparisons. |
| 8    |         | Deletes a condition, group, and any groups nested within the group. |
| 9    | Group   | Individual groups (and the entire Conditions box) can be expanded or collapsed to show or hide their settings:  
• Click to expand a collapsed group.  
• Click to collapse an expanded group. The number that appears in parentheses indicates how many conditions are contained in the group.  
After you configure a group, you can collapse it to avoid any unwanted changes. |
<table>
<thead>
<tr>
<th>ITEM</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>AND</td>
<td>Boolean operators that define the relationships between your search conditions. Click the operator icon to toggle between AND and OR conditions.</td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td></td>
</tr>
</tbody>
</table>

Manage nDepth search queries in LEM: Save, schedule, run on-demand, and more

This section explains how to save an nDepth search query, run it on-demand or at a later date, and export the search results. It also describes how to edit or delete saved queries.

Search queries can be saved and scheduled. Save and export your search query for disaster recovery purposes or to share it with another user when they are logged in to the console. A scheduled search can email the results to a defined user.

Save an nDepth search query

1. Create and run an nDepth search query. See Search normalized data using nDepth search in LEM for help.
2. In nDepth, click Save, and then select Save As.

![Save As Option]

If you are modifying an existing saved search, click Save.

3. In the Search Name field, enter a report name up to 200 characters in length, and then click OK.

SolarWinds recommends that you include the time frame in your search name, as saved searches always run with the saved time frame by default. For example, enter All Firewall Alerts - Last 24 Hours.

4. Click OK.

Your search appears in the Saved Searches pane appended with an icon.

- ![Event Data Search] indicates an event data search.
- ![Original Log Message Search] indicates an original log message search.
Edit a saved nDepth search query

To edit a saved search query, modify it and save it as a new search.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. To display the Saved Searches pane (if required), click History in the upper-left corner.
4. In the Saved Searches pane, click the search you want to modify.
5. In the search bar, reconfigure the search.
6. Click ➕ and then select Save.
   The search is saved with the new configuration.
7. Delete the old search query if you no longer need it. See Delete a saved nDepth search query for help (Optional).

Run a saved nDepth search query on demand

Saved searches are stored and listed alphabetically in the Saved Searches pane.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. To display the Saved Searches pane (if required), click History.
4. In the Saved Searches pane, click the search you want to run. Move the pointer over the search for tooltip information.
   nDepth displays your search data.

Schedule a saved nDepth search query

Schedule a saved search to run automatically at a prescheduled time. You can also share scheduled searches between users.

If the virtual appliance is offline for an extended amount of time (such as more than a day or two), the active schedules may not run at the expected time until the appliance is back online for several hours.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. To display the Saved Searches pane (if required), click History.
4. From the Saved Searches pane, select a Saved Search.
5. Click , and then select Schedule.
6. Complete the fields as required.

![Schedule nDepth Saved Search](image)

7. Click OK.

Delete a saved nDepth search query

You can permanently delete a search from your Saved Searches pane.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. In the Saved Searches pane, move the mouse over a search you want to delete.
4. To delete the search, click .
5. When prompted, click Yes to confirm.
   The saved search is deleted.

Export nDepth search results in CSV format

You can only export text results in CSV format. To export charts and graphs, see the PDF export procedure below.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. Review all alerts within the last ten minutes.
4. To refine your search parameters, modify the search to extend the time frame, or use the Refine Fields pane.
5. To retrieve your new results, click .
6. On the nDepth toolbar, click Result Details.
7. In the Result Details pane, click 🎨, and then select Export to CSV.
8. To continue, click Yes.
9. Save the file to the appropriate location.

Export nDepth search results in PDF format

You can export the results of your nDepth search to a printable report and save the report as a PDF file. PDF reports are limited to 25,000 events or log messages. If you need a larger report, use the Result Details view to export your search results to a spreadsheet in CSV format.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   Log in as an administrator or an auditor.
2. On the LEM toolbar, navigate to Explore > nDepth.
3. Review all alerts within the last ten minutes.
4. Modify the search to extend the time frame or use the Refine Fields pane to refine your search parameters.
5. To retrieve your new results, click 🎨.
6. On the nDepth toolbar, click Result Details.
7. On the nDepth page, click 🎨, and then select Export. Do not click the gear icon in the Result Details pane, click the gear in the upper-right corner above.
8. Customize your report layout:
   a. Replace nDepth Export Report Title with a custom title as required.
   b. Click the page thumbnails and remove page elements (such as charts, graphics, and text) as required.
   c. Adjust the page layout to Portrait or Landscape as required.
   d. Add a new page, click the Items tab, and drag item elements to add additional charts to your report (Optional).
   e. Click the Saved Layouts tab and click 🎨 to create a new layout or save your layout (Optional).
9. Click Export to PDF.
10. Save the file to the appropriate location.

The Utilities view

The Utilities view (Explore > Utilities) provides several IT analysis utilities, including Whois, NSLookup, Traceroute, and Flow (sFlow and NetFlow). These utilities are also available from the Explore > nDepth view, and Monitor view.

This topic provides help for the Utilities view in the LEM console. For more information, see Use the...
Explorer utilities in LEM to search or analyze nDepth query results.

This screen capture shows the Utility view in the LEM console:

![Utility view in LEM console](image)

The following table describes the key features of the Explore > Utilities view.

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>History pane</td>
<td>Displays a record of your explorer viewing history. Selecting an item in the history list displays the corresponding explorer event in the Explorer pane.</td>
</tr>
<tr>
<td>Utilities pane</td>
<td>Displays the explorers that are currently open. You can have multiple explorers open at the same time.</td>
</tr>
<tr>
<td>Cascade button</td>
<td>Arranges the open explorer windows so they appear in an organized cascade.</td>
</tr>
<tr>
<td>Respond</td>
<td>Responds to the event or event field that is the subject of the active explorer. You can also use the Respond menu to take action even when no explorer windows are open or active.</td>
</tr>
<tr>
<td>Explore</td>
<td>Contains options to open the other explorers. You can explore the event message or event field that is the subject of the active explorer or open a blank explorer to manually enter the item you want to explore.</td>
</tr>
<tr>
<td>Explorer windows</td>
<td>The active explorers within the Utilities pane. You can minimize, resize, and close each explorer window, as needed.</td>
</tr>
</tbody>
</table>
Minimized explorers

Any explorers that you have minimized appear at the bottom of the Utilities pane as a title bar. Click a title bar to reopen that explorer.

The Event explorer utility

The Event explorer displays all events related to an event that you select in the Monitor view events grid.

You can view events that occurred before, during, and after a selected event to identify the root cause of the event. This approach can help you visualize how an event occurred, as well as the system's response to that event.

When you explore an event, the console sends a request to the LEM Manager to determine which events are related to the event. In response, the Event explorer displays the events that triggered the event, as well as the events that resulted because of the event (such as a response or notification).

The Event explorer includes three sections: Event Details, Event Map, and Event Grid. This example shows an event explorer that provides information about the TCPPortScan event selected in the Monitor events grid.

Event Details

The Event Details pane provides detailed information about the event you select in the Monitor grid. Information about the event data fields may vary depending on the selected event type. For example, network-oriented events display fields for IP addresses and ports, while account-oriented events display account names and domains.
Click Event Details to open the Event Details window. Click [●] to read the event description and [●] to return to the event details. If you need to research this event further, click [●] to create a filter that displays this event type in the Monitor view event grid. The filter will display in the Filters pane under the last selected grid. When you complete your event review, click [●] to move to the previous or next event in the grid.

Event Map

The Event Map displays a graphical view of the event you are exploring, as well as the triggering and proceeding events. This allows you to move through the entire chain of events to analyze the relationships between each event.

Event explorer always places your selected event in the center of the map. Related prior events that triggered your selected event display to the left. If no prior events exist, a box labeled None displays in the map. Related events that follow the central event appear to the right. These events were caused by the central event (such as system responses). If no events follow, a box labeled None displays. If the same event occurs multiple times, they appear together in a box.

Events that appear in the event map can be events, rules, or commands (system responses to an event). Each event type includes an icon that categorizes the event, as shown below.

<table>
<thead>
<tr>
<th>ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Audit" /></td>
<td>Audit Event tree event.</td>
</tr>
<tr>
<td><img src="image" alt="Security" /></td>
<td>Security Event tree event.</td>
</tr>
<tr>
<td><img src="image" alt="Asset" /></td>
<td>Asset Event tree event.</td>
</tr>
<tr>
<td><img src="image" alt="Incident" /></td>
<td>Incident Event tree event.</td>
</tr>
<tr>
<td><img src="image" alt="Internal" /></td>
<td>Internal Event tree event that is not related to rules or active response activity.</td>
</tr>
<tr>
<td><img src="image" alt="Command" /></td>
<td>An internal command indicating the system is responding to an event.</td>
</tr>
<tr>
<td><img src="image" alt="Rule" /></td>
<td>Rule activity from a rule in test mode or a rule that initiated an active response.</td>
</tr>
</tbody>
</table>

Event Grid

The event grid lists all events that appear in the event map in chronological order—from the earliest event (top) to the latest event (bottom). The grid is useful for comparing events and exploring event data.

The event grid's Order column icons indicate when each event occurred, as shown below.

<table>
<thead>
<tr>
<th>ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Before" /></td>
<td>The event occurred before the central event.</td>
</tr>
<tr>
<td><img src="image" alt="During" /></td>
<td>The event occurred during (as part of) the central event.</td>
</tr>
</tbody>
</table>
The event occurred after the central event.

The Whois explorer utility

Whois explorer is a network utility that identifies the source of an IP address or domain name based on how it is registered with domain and network authorities. This explorer contacts the central databases for IP addresses and domain names and returns the results of any of your searches. It can tell you where something is located physically in the world, and who actually owns the device you are trying to locate. For example, you can use this explorer to identify who owns a domain that corresponds to the IP address that caused a rule to fire.

The example on the left shows the results for an IP address. The example on the right shows the results for the SolarWinds domain name, SolarWinds.com. From these results, you can find out who owns the IP address and where the server is hosted.

Opening the Whois Explorer adds a Whois explorer icon in the History pane of the Explore view.

nDepth explorer

nDepth is a search engine that locates all event data or the original log messages that pass through a particular LEM Manager. The log data is stored in real time as it occurs from each host (network device) and source (application or tool) that is monitored by the LEM Manager. You can use nDepth to conduct custom searches, investigate your search results with graphical tools, investigate event data in other explorers, and take action on your findings.

For more information about nDepth search, see:

- Search normalized data using nDepth search in LEM
- The nDepth view
The NSLookup explorer utility

The NSLookup explorer is a network utility that resolved IP addresses to host names and host names to IP addresses. Use this explorer to locate a name that corresponds to the IP address that caused the rule to fire. For example, you can resolve yourcompany.com to an IP address.

In this example, NSLookup explorer is searching for IP address of 192.168.168.10. The explorer retrieved the corresponding host name, which is grendel.corp.trigeo.com.

Opening the NSLookup explorer adds an NSLookup explorer icon to the History pane in the Explore view.

The Traceroute explorer utility

Traceroute explorer is a network utility that traces network links (or hops) from your host computer to a specific destination. Use this explorer to determine the network connections between yourself and the IP address that caused a rule to fire.
In this example, Traceroute explorer is tracing IP address 192.168.167.1. The interface displays the hops between your computer and the destination IP address. In this example, connecting to the IP address required two hops.

Opening the Traceroute Explorer adds a Traceroute explorer icon in the History pane of the Explore view.

The Flow explorer utility

Flow explorer performs flow analysis to determine which IP addresses or ports are generating or receiving the most network traffic. Use this explorer to analyze the volume of data (in bytes or packets) transferring to or from an IP address or port number on your network.

For example, if an unknown IP address displays at the top of the Flow explorer's activity list, you can select a bar on the graph or a row in the table and choose the Whois explorer from the Explore menu to identify the IP address and why it is transmitting so much data.

For more information, see Collect and view NetFlow and sFlow data in LEM.

Execute a Whois, NSLookup, or Traceroute task from an event or search result

1. Locate and select the event or search result you want to explore.
2. From the Explore drop-down list, select an option.

Execute a blank Whois, NSLookup, or Traceroute task

1. On the LEM toolbar, navigate to Explore > Utilities.
2. From the Explore drop-down list, select a utility.
3. Complete the form for the utility, and then click Search.

Display flow data

LEM supports flow exports from both NetFlow and sFlow devices. Use the Flow Explorer in the LEM console to view graphs, charts, and grids.

See Collect and view NetFlow and sFlow data in LEM to enable flow collection and analysis on the LEM appliance.
Common data field categories in LEM nDepth search

The categories in this topic frequently appear in the Refine Fields list, the Tree Map view, and the Result Details view.

This topic provides help for the Explore > nDepth view in the LEM console. For page-level help of the nDepth view, see The nDepth view

Common data field categories in Events Mode

This table describes the data fields that are most commonly seen when working with event data.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Name</td>
<td>The name of the event.</td>
</tr>
<tr>
<td>Detection IP</td>
<td>The network node that created the event data. The node is usually a Manager or an Agent.</td>
</tr>
<tr>
<td></td>
<td>The DetectionIP is identical to the InsertionIP field, but can also be a network device (such as a firewall or an intrusion detection system) that sends log files over a remote logging protocol.</td>
</tr>
<tr>
<td>Inference Rule</td>
<td>The name of the correlation that caused the event. The Inference Rule field will generally be blank, but displays the rule name when the event is related to a rule.</td>
</tr>
<tr>
<td>Insertion IP</td>
<td>The Manager or Agent that created the event. This is the source that first read the log data from a file or other source.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address associated with the event. This is a composite field drawn from several different event fields. It shows all the IP addresses that appear in event data.</td>
</tr>
<tr>
<td>Manager</td>
<td>The Manager that received the event. For data generated from an Agent, this is the Manager connected to the Agent.</td>
</tr>
<tr>
<td>Provider SID</td>
<td>A unique identifier for the original data. Generally, this field includes information used in researching information on the event in the originating network device vendor documentation.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity (0–7) of the event</td>
</tr>
<tr>
<td>Tool Alias</td>
<td>The alias name entered used to configure the tool on the Manager or Agent.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name associated with the event. This is a composite field, drawn from several different event fields. It shows all the places that user names appear in event data.</td>
</tr>
</tbody>
</table>
Common data field categories in Log Messages mode

This table describes the data fields that are most commonly seen when working with log messages. The fields are listed here alphabetically.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The node the log message came from (that is, the LEM or Agent that collected the message for forwarding to nDepth).</td>
</tr>
<tr>
<td>HostFromData</td>
<td>The originating network device (if different than the node) that the message came from. Normally, Host and HostFromData are the same. In the case of a remote logging device (such as a firewall) this field reports the original remote device's address.</td>
</tr>
<tr>
<td>ToolId</td>
<td>The tool that generated the log message.</td>
</tr>
<tr>
<td>ToolType</td>
<td>The category for the tool that generated the log message.</td>
</tr>
</tbody>
</table>
Build view in the LEM console

The Groups view

To open the Groups view in the LEM console, navigate to Build > Groups on the LEM toolbar. Use this view to create and manage groups in LEM.

This topic provides page-level help for the Groups view in the LEM console.

See also: LEM groups: Organize data elements for use with rules and filters

Below is an example of the Groups view.

The following table describes the meaning of each column in the Groups grid.

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The group type.</td>
</tr>
<tr>
<td>Name</td>
<td>The group name.</td>
</tr>
<tr>
<td>Description</td>
<td>The group description. Pointing to this field displays the complete description as a tooltip.</td>
</tr>
<tr>
<td>Created By</td>
<td>The console user who created the group.</td>
</tr>
<tr>
<td>Created Date</td>
<td>The group creation date.</td>
</tr>
<tr>
<td>Modified By</td>
<td>The console user who last modified the group.</td>
</tr>
<tr>
<td>Modified Date</td>
<td>The recent date when the groups were modified.</td>
</tr>
</tbody>
</table>
The Refine Results form in the Groups sidebar

Use the Refine Results form to search for groups. The form returns matching results in the Groups grid. The remaining grid items are available, but hidden. To restore the hidden items, click Reset or select All in the refinement lists you are using.

The Groups grid displays all groups associated with each Manager connected to the console. If the same group is configured for more than one Manager, it appears in the grid multiple times—once for each associated Manager. Use the Refine Results form to apply filters to the Groups grid to reduce the number of displayed groups.

When you select an option in the Refine Results pane, the grid refreshes to only display items that match your selected refinement options. The remaining items are hidden in the grid. To restore these items, click Reset or select All in your refinement lists.

Below is an example of the Refine Results form in the sidebar.

![Refine Results Form Example]

The following table describes the Refine Results form fields.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset</td>
<td>Returns the form and the Groups grid to their default settings.</td>
</tr>
<tr>
<td>Search</td>
<td>Performs keyword searches for specific groups. To search, enter your search text in the text box. The grid displays only those groups that match or include your entered text.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the group type that displays in the grid.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select a Manager to display groups associated with the Manager.</td>
</tr>
</tbody>
</table>
The Rules view

To open the Rules view in the LEM console, navigate to Build > Rules on the LEM toolbar. Use this view to create and manage rules, rule categories, and rule templates. This topic describes the Rules grid and the sidebar.

This topic provides page-level help for the Rules view in the LEM console. See also:

- LEM rules: Automate how LEM responds to events
- Building custom filter and rule expressions in LEM
- Rule Creation screen and the Rule Builder form

Below is an example of the Rules view.

![Rules view example](image-url)
The Rules grid

The Rules grid contains all policy rules configured for all Managers connected to the console. The Manager column indicates which Manager each rule applies to.

By default, this view displays the rules from the Custom Rules folder in the Folders pane. If you do not have any custom rules, click the Rules folder to list the rules included with the console.

The following table describes each column in the Rules grid.

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌒</td>
<td>Opens a drop-down with a list of commands you can perform on selected grid item.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates the rule availability for use with your policies.</td>
</tr>
<tr>
<td>🌒</td>
<td>indicates an enabled and active rule.</td>
</tr>
<tr>
<td>🌒</td>
<td>indicates a disabled and inactive rule.</td>
</tr>
<tr>
<td>Test</td>
<td>Indicates the rule test mode status.</td>
</tr>
<tr>
<td>🌒</td>
<td>When a rule is in test mode, the event appears in the console, but it cannot perform any active responses. This lets you see how the rule would behave when it is fully enabled, but without risking any negative unintended consequences.</td>
</tr>
<tr>
<td>🌒</td>
<td>indicates the rule is in test mode.</td>
</tr>
<tr>
<td>🌒</td>
<td>indicates the rule is not in test mode.</td>
</tr>
<tr>
<td>Name</td>
<td>The rule name.</td>
</tr>
<tr>
<td>Description</td>
<td>The rule description. Pointing to this field displays the complete description as a tooltip.</td>
</tr>
<tr>
<td>Folder</td>
<td>The folder name (in the Folders pane) where the rule is stored.</td>
</tr>
<tr>
<td>Created By</td>
<td>The console user who created the rule.</td>
</tr>
<tr>
<td>Created Date</td>
<td>The date the rule was created.</td>
</tr>
<tr>
<td>Modified By</td>
<td>The console user who last modified the rule.</td>
</tr>
<tr>
<td>Modified Date</td>
<td>The date and time the rule was last modified.</td>
</tr>
<tr>
<td>Manager</td>
<td>The Manager associated to the rule.</td>
</tr>
</tbody>
</table>

You can only test an enabled rule.
The Refine Results form

Use the Refine Results form to search for rules and rule templates. The form returns matching results in the Rules grid. The remaining grid items are available, but hidden. To restore the hidden items, click Reset or select All in the refinement lists you are using.

The following table describes the fields that make up the Refine Results form in the Rules sidebar.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset</td>
<td>Click Reset to clear the form. This returns the form and the Rules grid to their default settings.</td>
</tr>
<tr>
<td>Search</td>
<td>Use this Search field to perform keyword searches for specific rules. To search, type the text you want to search for in the text box. The grid displays only those rules whose Name fields match or include the text you entered.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this check box to display Enabled rules only. Clear this check box to display both Enabled and Disabled rules.</td>
</tr>
<tr>
<td>Test</td>
<td>Select this check box to display rules that are in test mode. Clear this check box to display rules that are in and out of test mode.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select a Manager to display all rules associated with the Manager.</td>
</tr>
<tr>
<td>Created By</td>
<td>Select the console user who created the rule and display only rules created by that user.</td>
</tr>
<tr>
<td>Created Date Range</td>
<td>Type or select a date range to display rules created within that date range.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Modified By</td>
<td>Select the console user who last modified and display only rules modified by that user.</td>
</tr>
<tr>
<td>Modified Date Range</td>
<td>Type or select the date range to display rules that were modified on or within that date range.</td>
</tr>
</tbody>
</table>

The Rule Categories & Tags pane in the Rules sidebar

Click a category to expand it and view the rules and rule templates filtered by the highlighted tag.

![Rule Categories & Tags]

Rule Creation screen and the Rule Builder form

Use the Rule Creation screen and the Rule Builder form to create or edit a rule. To open this form, navigate to Build > Rules on the LEM toolbar, and then click ☰ on the Rules toolbar.

ℹ️ This topic provides page-level help for the Rule Builder form in the LEM console.

For more information, see:

- [Create a new LEM rule to monitor and respond to events](#)
- [Get started building custom rule expressions in LEM](#)
Rule Creation screen

The following table describes the key features of the Rule Creation screen.

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Back to Rules Listing button</td>
<td>Hides Rule Creation and returns to the Rules grid. Rule Creation remains open in the background so you can return to it to continue working on your rules.</td>
</tr>
<tr>
<td></td>
<td>In the Rules grid, clicking Back to Rule Creation returns you to Rule Creation.</td>
</tr>
<tr>
<td>The Rule Creation sidebar (also called the List pane)</td>
<td>Contains categorized lists of the components you can use when configuring policy rules.</td>
</tr>
<tr>
<td></td>
<td>• To view the contents of a component list, click its title bar.</td>
</tr>
<tr>
<td></td>
<td>• To add a component to a rule, select it from its list and then drag it into the appropriate correlation box.</td>
</tr>
<tr>
<td>The Rule Builder form (also called the Rule window)</td>
<td>The working area where you name, describe, configure, edit, test, verify, and enable each rule.</td>
</tr>
<tr>
<td></td>
<td>You can have multiple rule windows open at the same time. You can also minimize, maximize, resize, and close each window, as needed.</td>
</tr>
<tr>
<td>Minimized rule window bar</td>
<td>Stores minimized Rule Builder forms at the bottom of the Rule Creation screen. Each minimized form shows the name of its rule. Click a minimized rule to open the rule in the Rule Creation screen.</td>
</tr>
</tbody>
</table>
The Rule Builder form

The following table describes each key feature and field of a rule window.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Title bar</td>
<td>Each rule you create or edit appears in its own configuration window. Upon naming a rule, the window’s title bar displays the name of the rule. You can also use the title bar to minimize, maximize, and resize rule window. Minimized rule windows appear at the bottom of the Rule Creation pane.</td>
</tr>
<tr>
<td>2</td>
<td>Name</td>
<td>Type a name for the rule.</td>
</tr>
<tr>
<td>3</td>
<td>on</td>
<td>When creating a new rule, use this list to select which Manager the rule is to be associated with. Otherwise, when editing a rule, this field displays which Manager the rule is associated with.</td>
</tr>
<tr>
<td>ITEM</td>
<td>NAME</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4</td>
<td>Tags</td>
<td>Click Add Tags to select categories and tags to add to the rule. Tags make it easier to categorize and find rules. For example, if you want a rule to appear in several different categories, select the corresponding tags.</td>
</tr>
<tr>
<td>5</td>
<td>Description</td>
<td>Type a description of what the rule does, or the situation for which the rule is intended. If the description extends beyond the visible area of the text box, a larger text box appears, so you can type a detailed description of the rule, its logic, its expected behavior, and its active response. When you are done typing, either press Tab or click anywhere outside the text box to close it.</td>
</tr>
<tr>
<td>6</td>
<td>Enable</td>
<td>Select this check box to enable the rule. Clear this check box to disable the rule.</td>
</tr>
<tr>
<td>7</td>
<td>Test</td>
<td>Select this check box to place the rule in test mode. Clear this check box to take the rule out of test mode. You must enable a rule before you can test it.</td>
</tr>
<tr>
<td>8</td>
<td>Subscribe</td>
<td>Use this list to select which Console users are to subscribe to the rule. This means the system will notify the subscribing users Consoles each time one of the subscribed-to rules triggers an alert. The alerts will appear in their alert grid.</td>
</tr>
<tr>
<td>9</td>
<td>Rule Status</td>
<td>The Rule Status bar lists warnings and error messages about your rule's current configuration logic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click &gt; to view a list of warning and error messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click a message flag to provide detailed information about the nature of that problem.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click a message to highlight the specific area or field that is the source of that problem.</td>
</tr>
<tr>
<td>ITEM</td>
<td>NAME</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 10   | Correlations     | Use the Correlations box to configure correlations between groups of alert events. You can coordinate multiple alert events into a set of conditions that will prompt the Manager to issue a particular active response.  
You set up correlations by dragging items from the Events and Event Groups lists into this box, and then setting the specific conditions or for the alert that are to prompt action.  
The Correlations connector bar lets you group alert conditions, and determine if they must all apply (an AND correlation) or if any of them may apply (an OR correlation) to prompt a response. |
| 11   | Correlation Time | Use the Correlation Time box to establish the allowable frequency and time span in which the correlation events must occur before the rule applies.  
The Advanced section lets you define an alert event threshold, and to define the re-inference period for the threshold. The threshold tells the Manager which specific fields to monitor to determine if a valid alert event has occurred (i.e., when to “count” the alert).  
The box’s Advanced section lets you define a Response Window that lets the rule ignore any events that occur outside (past or future) of the established period. |
| 12   | Actions          | Use the Actions box to dictate which actions the rule is to execute when the events described in the Correlations and Correlation Time boxes occur. Examples of actions include sending an email message to your system administrator, or blocking an IP address. |
| 13   | Undo/Redo        | Click the Undo button to undo your last desktop action. You can click the Undo button repeatedly to undo up to 20 steps.  
Click the Red button to redo a step that you have undone. You can click the Redo button repeatedly to redo up to 20 steps.  
You can only use Undo or Redo for any steps you made since the last time you clicked Apply. |
Use these commands to save or cancel your work:

- Click Save to save your changes to a rule and close the rule window.
- Click the Cancel button to cancel any changes you have made to a rule since the last time you clicked Save, and close the rule window. If you have any unsaved changes, the system will prompt you to save or discard them.
- Click Apply to save your changes to a rule, but keep the rule window open so you can continue working. You can click Apply at any time.

The Correlations box

To create a rule, you drag items from the list pane into the rule window's Correlations box to configure the relationships (or correlations) that define the rule. These correlations define the events that must occur for the rule to take effect.

Creating rule correlations is a lot like configuring conditions for custom filters, so the Correlations box in Rule Creation behaves a lot like the Conditions box in Filter Creation. The following table describes each item shown in the Correlations box, above.

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>▼</td>
<td>Groups can be expanded or collapsed to show or hide their settings:</td>
</tr>
<tr>
<td></td>
<td>- Click to ▼ expand a collapsed group.</td>
</tr>
<tr>
<td></td>
<td>- Click to ▼ collapse an expanded group.</td>
</tr>
</tbody>
</table>

Once a group is configured properly, you may want to collapse it to avoid accidentally changing it.

This is the Group button. It appears at the top of every group box. Click it to create a new group within the group box. A group within a group is called a nested group. You may then drag alert variables and other items from the list pane into the nested group box.

By using nested groups, you can refine correlations by combining or comparing one group of correlations to another to create the logic for complex correlations.

Each group is subject to AND and OR relationships with the groups around it and within it. By default, new groups appear with AND comparisons.

This is the Threshold button, which opens the Threshold form for a group. The Threshold form is described below.
<table>
<thead>
<tr>
<th><strong>NAME</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>X</strong></td>
<td>This is the Delete button. It appears at the top of every Group box and every correlation. Click this button to delete a correlation or a particular group. Deleting a group also deletes any groups that are nested within that group.</td>
</tr>
<tr>
<td>Event variable</td>
<td>From the Events, Event Groups, or Fields list, drag an alert, Event Group, or alert field into the Correlations box. This is called the alert variable. A rule can have multiple alerts and Event Groups in its correlation configuration. You can think of an alert variable as the subject of each group of correlations. As alerts stream through the Manager, the rule analyzes the values associated with each alert variable to determine if the alert meets the rule's conditions. If so, the Manager either initiates an active response, or stores the alert for comparison with other alerts that may occur within the rule's allotted time frame.</td>
</tr>
</tbody>
</table>
| Operators | Whenever you drag a list item or a field next to alert variable, an operator icon appears between them. The operator states how the filter is to compare the alert variable to the other item to determine if the alert meets the rule's conditions.  
- Click an operator to cycle through the various operators that are available for that comparison. Just keep clicking until you see the operator you want to use.  
- Ctrl+click an operator to view all the operators that are available for that comparison. Then click to select the specific operator you want to use. |
| List item | List items are the various non-alert items from the list pane. You drag them into groups to define rule correlations based on your Time Of Day Sets, Connector Profiles, User-Defined Groups, Constants, etc.  
Some alert variables automatically add a blank Constant as its list item. You can overwrite the Constant with another list item, or you can click the Constant to type or select a specific value for the constant.  
Note that each list item has an icon that corresponds to the list it came from. These icons let you to quickly identify what kinds of items are defining your rules' correlations. |
| Threshold | The Threshold section lets you define a threshold for the correlations in a Group box. You can think of a threshold as a correlation frequency for the grouping; that is, the number of times the events defined by the group must occur within a specified period before the rule takes effect.  
A group threshold behaves exactly like the threshold in the Correlation Time box. |
<p>| 📊 | This is the Set Advanced Threshold button. Whenever a group threshold's number of Events within [time] is greater than 1, this button becomes enabled so you can open the Set Advanced Thresholds form. This form lets you specify advanced threshold fields and define an advanced response window for the alert fields within the grouping. |</p>
<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND</td>
<td>Rule correlations and groups of correlations are subject to AND and OR comparisons. If you click an AND operator, it changes to an OR, and vice versa.</td>
</tr>
<tr>
<td>OR</td>
<td></td>
</tr>
</tbody>
</table>

**About advanced thresholds**

Whenever a group threshold or the "Events within" box in the "Correlation Time" form has a value greater than 1, the Set Advanced Thresholds icon is enabled. This icon opens the Set Advanced Thresholds form so you can define an alert event threshold and the re-inference period for that threshold. The threshold tells the Manager which specific alert fields to monitor to determine if a valid alert event has occurred (such as when to count the alert).

For example, threshold event x must occur multiple times on the same destination computer with the frequency defined in the Correlation Time box. Another example is threshold event y must occur on different destination computers with the frequency defined in the Correlation Time box. When the threshold event counter increases to the number displayed in the Events box, the threshold becomes true and triggers the next set of conditions in the rule.

To open the form, click in the Correlations box on the nested group you want to work with.

**Set an advanced threshold**

1. To open the Set Advanced Thresholds form, click the Set Advanced Thresholds icon . See About advanced thresholds for help.

2. If you want to define a second threshold, select the Re-Infer (TOT) check box. Use the adjacent fields to type or select the threshold time interval and unit of measure.

   The Re-Infer (TOT) option defines the period that an alert must remain above the threshold before the system issues a new notification and/or active response.

   For example, an alert exceeded the threshold and the Re-Infer (TOT) period for the alert is 1 hour. If the alert stays above the threshold for more than 1 hour, the system will issue an additional notification or active response at the end of 1 hour.

**Add a Threshold field**

1. To open the Set Advanced Thresholds form, click the Set Advanced Thresholds icon . See About advanced thresholds for help.

2. At the bottom of the form, click Add.

   The Available Fields pane has two boxes. The top box lists all alerts applied to the correlations box. The bottom box lists the alert fields associated with the alert that is currently selected in the top box.

3. In the top Available Fields box, select an alert. The fields associated with that alert appear in the lower Available Fields box.

4. In the lower Available Fields box, select the alert field used to define the alert threshold.
5. From the Select Modifier drop-down list, select an option.
   Select Same if the threshold will be defined by the selected field being the same multiple times.
   Select Distinct if the threshold will be defined by the selected field being different each time.

6. To display the field and its modifier, click in the Selected Fields grid.

7. For additional threshold fields, repeat steps 2 through 6.

8. To save the fields to the threshold and close the form, click OK.
   These fields raise the threshold for the correlation event and its active response to occur.

Edit a threshold field

You cannot actually edit a threshold field. Instead, you must delete it, and then replace it with a corrected field configuration.

To replace a threshold field:

1. To open the advanced threshold you want to work with, click the Set Advanced Thresholds icon.
   See About advanced thresholds for help.

2. To remove the field you want to change, click in the Selected Fields list.

3. In the Available Fields list, select the appropriate alert, and then the alert field.

4. In the Select Modifier list, select the new modifier for the field (Same or Distinct).

5. To display the corrected field and its modifier in the Selected Fields box, click .
   The corrected field and its modifier appear in the Selected Fields box.

6. To close the form, click OK.

Delete a threshold field

1. To open the advanced threshold you want to work with, click .

2. In the Selected Fields list, select the field you want to delete.

3. To remove the threshold field from the Selected Fields list, click .

4. To close the form, click OK.

The Actions box

Use the Actions box to define the action response that LEM should execute when the correlation events specified by the rule occurs. You can assign more than one action to a rule. For example, you can shut down an Agent and then notify your system administrator of the event through email.

The Actions box fields indicate where the action is performed, what the action does, and who receives the action. For example, if you want a rule to disable a user, you can select Disable Domain User Account. To apply the action, specify which account you want to disable and where you want to disable it (that is, which Agent).
Using constants and fields to make actions flexible

When configuring an action, you can assign constants that define fixed parameters for a rule or alert fields from the alerts in the Correlations box. Fields determine the rule parameters when some degree of flexibility is required. Constants and fields are useful, but fields provide actions with a great deal of flexibility.

For example, if you have two network users named Bob and Jane, you can disable Bob's user account and assign a constant to the rule that explicitly represents Bob's account. However, this limits the rule to Bob's account.

If you assign a field to the rule, the rule can be interpreted as follows: When user activity meets the conditions in the Correlations box to prompt the Disable Domain User Account action, use the UserDisable.SourceAccount field in the alert to determine which user account to disable.

If Bob triggered the rule, the Manager disables Bob's account. But if Jane also triggers the rule, the Manager can disable her account as well.

Configuring actions for a rule

1. In the list pane, click the Actions list.
2. Select and drag an action to the Actions box.

![Actions](image)

The top left of the Actions box shows the name the action that will execute. In most cases, the Actions form prompts you for specific parameters about the computer, IP address, port, alert, user, and so on that receives the action.

3. Use the list pane to assign the appropriate alert field or constant to each parameter.
   a. In the Events or Event Groups lists, select and drag an alert field to the appropriate parameter box in the Actions form.
   b. Select and drag a constant from the Constants lists to the parameter box in the Actions form (Optional). Typically, you will select a text constant.
   c. To edit the constant, double-click the parameter box.
4. To save your changes, click Save.

Users view in the LEM console

To open the Users view, navigate to Build > Users on the LEM toolbar. Use this view to manage LEM user system accounts.

This topic provides page-level help for the Users view in the LEM console.
The following example shows the Users view in the LEM console.

Users view main page elements

This section describes the main elements in the Users view.

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refine Results</td>
<td>Filters the Users grid based on your selections.</td>
</tr>
<tr>
<td>Users grid</td>
<td>Displays all users associated with each Manager throughout your network.</td>
</tr>
<tr>
<td></td>
<td>Click to add a user or import a user from Active Directory.</td>
</tr>
<tr>
<td>User Information for:</td>
<td>Displays information about the user selected in the Users grid. The form is read-only unless you are adding or editing a user.</td>
</tr>
</tbody>
</table>
The Users grid

By default, the Users grid displays all users configured for all Managers monitored by the console. Use the Refine Results form to filter the contents of the grid.

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌟</td>
<td>Click to edit or delete the user account.</td>
</tr>
</tbody>
</table>
| Status | The user login status. Indicates if the user is currently logged in to the console.  

- 🌟 indicates the user is logged in to the console.  
- 🌟 indicates the user is not logged in to the console. |
| User/Group Name | The account name used to log in to LEM Manager. |
| Type | Indicates if the user account is a local LEM user account, or a Directory Service (DS) account that is synchronized with Active Directory. |
| First Name | The user's first name. |
| Last Name | The user's last name. |
| LEM Role | The LEM role type assigned to the user. There are six role types: Administrator, Auditor, Monitor, Contact, Guest, and Reports. |
| Description | A brief description of the user's job function or responsibility. |
| Manager | The LEM Manager where the user account is located. |
| Last Login | Timestamp showing the time and date that the user last logged in to the system. |

The Refine Results form

By default, the Users grid shows all users across all LEM Managers. Use the Refine Results sidebar to limit the number of users displayed in the grid.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset</td>
<td>Click to return the grid and the form to their default settings.</td>
</tr>
<tr>
<td>Manager</td>
<td>Select a LEM Manager instance to view only the user accounts located on the selected instance.</td>
</tr>
<tr>
<td>LEM Role</td>
<td>Select a role type to view only users that match that role type. By default, the grid displays results for all LEM role types.</td>
</tr>
<tr>
<td>Last Login Date Range</td>
<td>Enter a start date and end date to view users who last logged in during the specified date range.</td>
</tr>
</tbody>
</table>
The User Information for form

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter a user account name. You cannot use admin_role, audit_role, or reports_role for the user name.</td>
</tr>
<tr>
<td>First Name</td>
<td>Enter the user's first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter the user's last name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a user password to access the Manager. This can be an initial system password or a temporary password that is assigned to replace a forgotten password.</td>
</tr>
<tr>
<td></td>
<td>* If you are creating a Contact user, a password is not required.</td>
</tr>
<tr>
<td></td>
<td>If the Must Meet Complexity Requirements check box is selected in the Manage &gt; Appliance &gt; Properties &gt; Settings tab, the console enforces the following policy:</td>
</tr>
<tr>
<td></td>
<td>- Passwords must have a minimum of six characters. Spaces are not allowed.</td>
</tr>
<tr>
<td></td>
<td>- Passwords must have two of the following three attributes: at least one special character, at least one number, and a mix of lowercase and uppercase letters.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the password again.</td>
</tr>
<tr>
<td>LEM Role</td>
<td>Select a LEM role for this user.</td>
</tr>
<tr>
<td></td>
<td>- Administrator - Has full access to the system, and can view and modify everything.</td>
</tr>
<tr>
<td></td>
<td>- Auditor has extensive view rights to the system, but cannot modify anything other than their own filters.</td>
</tr>
<tr>
<td></td>
<td>- Monitor - Can access the console, cannot view or modify anything, and must be provided a set of filters. See “Specify the filters that users assigned the Monitor role can use in the LEM console&quot; on page 129 for steps.</td>
</tr>
<tr>
<td></td>
<td>- Contact - Cannot access the console, but can receive external notification.</td>
</tr>
<tr>
<td></td>
<td>- Guest - Has extensive view rights to the system, but cannot modify anything other than their own filters.</td>
</tr>
<tr>
<td></td>
<td>- Reports - Cannot log in to the LEM console, but can log in to the LEM reports application. This role can access the LEM database over a secure channel if TLS encryption is enabled. See &quot;Enable transport layer security (TLS) in the LEM reports application&quot; on page 78 for details</td>
</tr>
<tr>
<td>View Role</td>
<td>Click to open the role privileges assigned to the new user. Role privileges cannot be changed.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a brief description (up to 50 characters). For example, provide the user title, position, or area of responsibility.</td>
</tr>
</tbody>
</table>
### FIELD DESCRIPTION

**Contact Information**
- Enter an email address. LEM Manager notifies users by email about network security events. You can add as many email addresses as required.

1. To add the address to the Contact Information box, type an email address, and then click [ ]. Use the following format: `username@example.com`
2. To send a test email to the email address, click Save, and then click [ ].
3. Verify that the user received the email test message.
4. Repeat these steps to add additional email addresses.

---

**The Privileges screen**

The Privileges screen provides details about the *access, modify,* and *audit* rights that are granted to each LEM role type. This information is read-only and cannot be changed. See also [View the system privileges associated with a role](page465).
Manage view in the LEM console

Manage view provides details about your LEM installation and lets you manage LEM VMs and nodes.

The Appliances view

To add and manage LEM VMs, legacy appliances, and global settings, navigate to Manage > Appliances on the LEM toolbar.

This topic provides page-level help for the Appliances view in the LEM console. See also, LEM setup, configuration, and maintenance.

The following example shows the Appliances view in the LEM console.

Tasks that you can perform using this view include:

- Connecting to (or disconnecting from) a particular LEM Manager.
- Adding a LEM Manager's Agents.
- Configuring rules, policies, and network security connectors that apply to each Manager.

Commands in the Appliances view can take a while to execute, because they must remotely access the Manager or network appliance.
The Appliances view is primarily concerned with managing LEM Managers. Customers with large LEM installations that include older LEM appliances may also see other components in the appliance list, including:

- Database servers
- Logging servers
- Network sensors
- nDepth servers

The Appliances main view

The following tables describe the Appliances view elements.

The Appliances menu bar

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Adds a new Manager or network appliance to the console.</td>
</tr>
<tr>
<td>+</td>
<td>Displays a drop-down menu to copy, import, or export user settings. You can copy grid information about your Manager and paste it to a Microsoft Excel spreadsheet for analysis or to the Remote Agent installer for updates.</td>
</tr>
</tbody>
</table>

The Appliances grid

The following table describes the columns and selections in the Appliances grid.

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>🏅</td>
<td>Displays a list of commands you can perform on the appliance. When you select a Manager in the grid, use Logout, Configure, and Connectors for connecting products to the appliance. Select Policy for assigning an event distribution policy.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the connection status of the appliance.</td>
</tr>
<tr>
<td>🔄</td>
<td>indicates connected and logged in.</td>
</tr>
<tr>
<td>🔄</td>
<td>indicates disconnected and logged off.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the name of the Manager or appliance.</td>
</tr>
<tr>
<td>Type</td>
<td>Describes the type of appliance as a Manager, database, logging server, or network sensor.</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the LEM Manager software version.</td>
</tr>
<tr>
<td>COLUMN</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Platform</td>
<td>Displays the Manager platform name. The platform can be Trigeo SIM, VMware vSphere, or Microsoft Hyper-V.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the IP address of the Manager or appliance.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the port number used by the console to communicate with the Manager, network appliance, or database.</td>
</tr>
<tr>
<td>Connectors Update</td>
<td>Indicates whether the appliance connectors are configured for automatic updates. If the icon is green, LEM is set up to automatically update whenever SolarWinds updates a connector. If the icon is gray, automatic connector updates are inactive and must be turned on for automatic connector updates.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the user currently logged on to the Manager.</td>
</tr>
</tbody>
</table>

To automatically apply connector updates and manually apply individual connector updates, use the Connector Updates menu at the top right of the Appliance grid.

The Details pane

The Details pane displays essential information about a LEM VM or appliance, including the VM's name, connection status, and IP address.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Displays the name of the Manager platform (VMware vSphere, Microsoft Hyper-V, or Trigeo SIM).</td>
</tr>
<tr>
<td>CPU Reservation</td>
<td>Displays the CPU space reservation. Reserving CPU space ensures you have adequate resources available for the allocated CPUs.</td>
</tr>
<tr>
<td>Number of CPUs</td>
<td>Displays the number of CPUs allocated to this LEM Manager.</td>
</tr>
<tr>
<td>Memory Allocation</td>
<td>Displays the amount of memory allocated to this LEM Manager.</td>
</tr>
<tr>
<td>Memory Reservation</td>
<td>Displays the amount of memory reserved for this system. Reserving memory ensures enough system memory is available when needed.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the LEM Manager or LEM appliance connection status.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the LEM Manager or LEM appliance name.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the appliance type: Manager, Database Server, nDepth, Logging Server, or Network Sensor.</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the LEM Manager's software version.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the LEM Manager or LEM appliance IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the port number used by the console to communicate with the LEM Manager or LEM appliance.</td>
</tr>
</tbody>
</table>
The Properties pane

The Properties pane consists of the Login, License, and Settings tabs.

The Properties pane is only used to configure LEM Manager settings. It is not active if you select another type of LEM VM in the Appliances grid.

The Login tab

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the user name to log in with if configuring the console to log in automatically.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password if configuring the console to log in automatically.</td>
</tr>
<tr>
<td>Login Automatically Next Time</td>
<td>Automatically log in to the Manager when you open the console. Clear this check box if you prefer to log in manually.</td>
</tr>
<tr>
<td>Save Credentials</td>
<td>Enable the console to save the LEM Manager user name and password locally. If the Login Automatically Next Time check box is selected, the console will automatically log on to the Manager when the console is started. Otherwise, the console automatically provides the user name and password when you manually log in to the Manager.</td>
</tr>
<tr>
<td>Reconnect on disconnection / Try to reconnect every $n$ seconds</td>
<td>Enable the console to reconnect with the LEM Manager when the Manager is disconnected for any reason.</td>
</tr>
<tr>
<td>Timeout reconnection attempts after $n$ tries</td>
<td>Select to have the Console quit its reconnection attempts with the LEM Manager after a given number of tries, especially if the previous connection attempts were unsuccessful.</td>
</tr>
</tbody>
</table>

The License tab

The License tab summarizes your available and allocated licenses, and activates your SolarWinds LEM license.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Nodes</td>
<td>Displays the total number of nodes allowed by your SolarWinds LEM license.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total Unused Nodes</td>
<td>Displays the number of unallocated nodes.</td>
</tr>
<tr>
<td>Total Agent Nodes</td>
<td>Displays the number of nodes allocated to LEM agent devices (such as workstations or servers).</td>
</tr>
<tr>
<td>Total Non-Agent Nodes</td>
<td>Displays the number of nodes allocated to non-agent devices (such as firewalls and switches).</td>
</tr>
<tr>
<td>Maintenance Expiration Date</td>
<td>Displays the date your current maintenance contract with SolarWinds Support expires.</td>
</tr>
</tbody>
</table>

### The Settings tab

The Settings tab defines the LEM Manager password policy settings and the global automatic update settings. Global automatic updates allow the LEM Manager to automatically send software updates to Agents as new software becomes available.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Policy</td>
<td></td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>Enter or select the minimum number of required password characters. Passwords must have at least six characters, but no more than 40 characters.</td>
</tr>
<tr>
<td>Must meet complexity requirements</td>
<td>Select this check box if passwords must meet the following complexity requirements:</td>
</tr>
<tr>
<td></td>
<td>- Passwords must not match or contain part of the user’s user name.</td>
</tr>
<tr>
<td></td>
<td>- Passwords must be at least six characters long.</td>
</tr>
<tr>
<td></td>
<td>- Passwords must contain characters from three of the following four categories:</td>
</tr>
<tr>
<td></td>
<td>- English uppercase characters (A through Z).</td>
</tr>
<tr>
<td></td>
<td>- English lowercase characters (a through z).</td>
</tr>
<tr>
<td></td>
<td>- Base 10 digits (0 through 9).</td>
</tr>
<tr>
<td></td>
<td>- Non-alphanumeric characters (!, $, #, %, ^, etc.).</td>
</tr>
</tbody>
</table>

### Remote Updates

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Global Automatic Updates</td>
<td>Select this check box to enable a LEM Manager to update its qualifying Agents with the latest software updates. Clear this check box to disable this feature.</td>
</tr>
<tr>
<td></td>
<td>Each Agent is also controlled by its Automatic Update settings on the Agents grid. The Agent Automatic Updates setting is disabled if you select the Enable Global Automatic Updates check box.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum Concurrent Updates</td>
<td>Select how many Agents the LEM Manager can update at one time. The default value is 10. If the number of Agents that require updates is greater than the value you entered in this field, the remaining Agents are queued for updates when an update slot is available.</td>
</tr>
<tr>
<td>Explorer Command Agent</td>
<td></td>
</tr>
<tr>
<td>Current Default Agent</td>
<td>Select the default Agent for performing SolarWinds explorer functions, such as NSLookup and Whois. For best results, choose an Agent that is normally online and will return the expected results.</td>
</tr>
<tr>
<td>Connection Requests</td>
<td></td>
</tr>
<tr>
<td>Minutes</td>
<td>Set the value for the amount of time before a timeout request is initiated.</td>
</tr>
<tr>
<td>Seconds</td>
<td>Set the value for the amount of time before a timeout request is initiated.</td>
</tr>
<tr>
<td>SolarWinds Improvement Program</td>
<td></td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter your email address.</td>
</tr>
<tr>
<td>Send usage statistics to</td>
<td>Select this check box to send statistics to SolarWinds.</td>
</tr>
<tr>
<td>SolarWinds to help us</td>
<td></td>
</tr>
<tr>
<td>improve our products</td>
<td></td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td></td>
</tr>
<tr>
<td>Allow LEM to detect threats</td>
<td>This check box is active by default. Threat intelligence identifies events as threats by matching event IP information against a list of known bad IP addresses.</td>
</tr>
<tr>
<td>based on list of bad IP</td>
<td></td>
</tr>
<tr>
<td>addresses</td>
<td></td>
</tr>
</tbody>
</table>

Only administrators have permissions to enable or disable the threat intelligence feed. Disabling and reenabling the threat intelligence feed forces a threat intelligence update and creates an **InternalAudit** event. Restarting LEM also forces the threat intelligence feed to update.
The Connect to SolarWinds Log & Event Manager Appliance form

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name or IP</td>
<td>Enter the LEM VM name or IP address.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user name to log in with.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the account.</td>
</tr>
<tr>
<td>Login on console startup</td>
<td>Select to automatically log in to LEM when the console is started.</td>
</tr>
<tr>
<td>Save Credentials</td>
<td>Select to save the login user name and password.</td>
</tr>
<tr>
<td>Appliance Type</td>
<td>Select the appropriate LEM Manager or server.</td>
</tr>
<tr>
<td>Connection Port</td>
<td>Enter the port number used by the console to communicate with the Manager network appliance or database.</td>
</tr>
<tr>
<td></td>
<td>The secure port number is 8443. This value defaults to 8080 for virtual appliances in the evaluation phase. This field only applies when the Appliance Type is Manager.</td>
</tr>
<tr>
<td>Model</td>
<td>Select Virtual if LEM is deployed as a VM, or select the appropriate appliance model (applies to older versions of LEM).</td>
</tr>
<tr>
<td></td>
<td>If you don't know the model type, select Unknown. If your model type does not appear in the drop-down list, select Other. Your selection will not impact Manager operations. If you selected a listed model type, an image of the appliance displays in the Details pane.</td>
</tr>
</tbody>
</table>
**FIELD** | **DESCRIPTION**
--- | ---
**Level** | This option does not apply if LEM is deployed as a VM. If you are adding a physical appliance, select the appliance level. This value is related to the appliance capacity and performance. If you are not sure which level to choose, select Unknown.

**Service Tag** | Enter the LEM appliance serial or registration number. This number uniquely identifies this piece of equipment and its specific configuration properties.

**Icon Color** | Select the desired color for your icon.

**See also:**
- Add another LEM VM or appliance to the console

The Configure your SolarWinds Log & Event Manager Appliance form

See [The Connect to SolarWinds Log & Event Manager Appliance form](#) for help.

The Connector Configuration form

The following table describes the key features of the Connector Configuration form.

<table>
<thead>
<tr>
<th><strong>NAME</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sidebar button</td>
<td>Hides and open the Refine Results pane.</td>
</tr>
<tr>
<td>Refine Results pane</td>
<td>Displays all supported products. You can apply filters to the grid to reduce the number of displayed products and show only those products configured for use with this Agent. You can also associate a particular product category or status (Running or Stopped).</td>
</tr>
<tr>
<td>Connectors grid</td>
<td>The Connectors grid lists all the sensor and actor connectors that are available to each Agent. These connectors are what allow LEM to monitor and interact with your network security products and devices. Connectors are organized by category and product name. Each connector is named after the third-party product it is designed to configure for use with LEM.</td>
</tr>
<tr>
<td>![+]</td>
<td>Click this button to create a new connector instance the sensor or actor that is currently selected in the Connectors grid.</td>
</tr>
<tr>
<td>Properties pane</td>
<td>This pane displays detailed information about the connector that is currently selected in the Connectors grid.</td>
</tr>
<tr>
<td></td>
<td>- If the connector is not configured, this pane displays a description of the connector.</td>
</tr>
<tr>
<td></td>
<td>- If the connector is configured, this pane displays the configuration settings as read-only information.</td>
</tr>
<tr>
<td></td>
<td>Whenever you add or edit a connector, this pane turns into an editable form for recording the configuration settings.</td>
</tr>
</tbody>
</table>
Connectors grid columns

The following table briefly describes the meaning of each column in the Connector Configuration form's Connectors grid.

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄️</td>
<td>The gear button opens a menu of commands that apply to the connector that is currently selected in the grid.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the connector's current connection status:</td>
</tr>
<tr>
<td>🟢</td>
<td>indicates the connector is connected and running.</td>
</tr>
<tr>
<td>🟠</td>
<td>indicates the connector is disconnected and not running.</td>
</tr>
<tr>
<td>Category</td>
<td>The high-level connector category, such as anti-virus connectors, firewall connectors, operating system connectors, etc.</td>
</tr>
<tr>
<td>Name</td>
<td>The actor, sensor, or connector instance name. Typically, connectors are named after the third-party products they are designed to configure for use with LEM.</td>
</tr>
</tbody>
</table>

The Connectors grid icons

The following table describes the icons used in the Connector Configuration utility's node tree.

<table>
<thead>
<tr>
<th>ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄️</td>
<td>A blue connector icon represents a sensor for a particular product. The sensor displays the name of the product it is designed to monitor.</td>
</tr>
<tr>
<td></td>
<td>Each connector instance (or alias) that is currently configured to monitor that product is listed below the connector. If no connector instances are listed, it means the product, on this Agent computer, has not been configured for use with LEM.</td>
</tr>
<tr>
<td></td>
<td>Whenever you select a sensor in the grid, the lower pane displays the connector's name and a description of the sensor, when available.</td>
</tr>
<tr>
<td>🧦</td>
<td>The orange connector icon represents an actor for a product that can perform an active response. The actor displays the name of the product it is designed to interact with.</td>
</tr>
<tr>
<td></td>
<td>Each connector instance (or alias) that is currently configured to initiate an active response on that product is listed below the connector. If no connector instances are listed, it means the product, on this Agent computer, has not been configured for use with LEM.</td>
</tr>
<tr>
<td></td>
<td>Whenever you select an actor in the grid, the lower pane displays the connector's name and a description of the actor, when available.</td>
</tr>
</tbody>
</table>
This icon represents a configured instance of a sensor connector. Each sensor can have more than one instance, where each configuration is identified by a different name, called an alias. In the grid, each configured connector instance appears below its connector.

Whenever you select a sensor connector instance in the grid, the lower pane displays the sensor connector's name, and the connector instance's name (or alias) and configuration settings. The Status column displays each instance's current status—Stopped (●) or Running (○).

This icon represents a configured instance of an actor connector. Each actor can have more than one instance, where each configuration is identified by a different name, called an alias. In the grid, each configured connector instance appears below its connector.

Whenever you select an actor connector instance in the grid, the lower pane displays the actor connector's name, and the connector instance's name (or alias) and configuration settings. The Status column displays each instance's current status—Stopped (●) or Running (○).

Refining the Connectors grid

By default, the Connectors grid shows every connector (sensor and actor) that can be configured for use with a particular Agent or Manager. To help you work more efficiently with a long list of connectors, the Refine Results pane lets you apply filters to the Connectors grid to reduce the number of connectors it shows.

When you select options in the Refine Results pane, the Connectors grid refreshes to show only those sensor and actors that match the options you have selected. The other connectors are still there; however, they are hidden. To restore them to the grid, click the Reset button or select All in the refinement lists you are using.

The following table explains how to use the Refine Results pane.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset</td>
<td>Clears the form and return the Connectors grid to its default state showing all connectors.</td>
</tr>
<tr>
<td><img src="search.png" alt="Search" /></td>
<td>Performs keyword searches for specific products.</td>
</tr>
<tr>
<td>Configured Connectors</td>
<td>Displays instances in the Connectors grid that are configured for your targeted Manager or Agent. Clear this check box to have the grid list both configured and unconfigured connectors.</td>
</tr>
<tr>
<td>Category</td>
<td>Select a high-level category to list the connectors that are available to support third-party products in that category. Each connector is named after the product it is designed to configure for use with LEM. If you cannot find a particular product, it is either not supported, or it is in a different category.</td>
</tr>
</tbody>
</table>
### Field Description

| Status | Select Running to list all connectors currently running on your targeted Manager or Agent. Select Stopped to list all connectors that currently stopped on your targeted Manager or Agent. |

The Connector Configuration form fields for data-gathering (sensor) connectors

This section describes each field on the Connector Configuration form when you configure sensors for data-gathering connectors.

Not every field appears with every connector. The fields that appear depend on the connector that you are configuring.
<table>
<thead>
<tr>
<th><strong>FIELD</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Type a name that easily identifies the application or appliance event log file that is being monitored. For active response connectors, we recommend you end the alias with “AR”. For example, an alias for the Cisco PIX Active Response connector might be “Cisco PIX AR”. This allows you to differentiate the active response connector from the data gathering connector.</td>
</tr>
</tbody>
</table>
| Log File / Log Directory | When you create a new alias for a connector, LEM automatically places a default log file path in the Log File box. This path tells the connector where the operating system stores the product’s event log file. For most connectors, you can change the log file path, as needed. However, some products write events to the Windows Application Log or the Windows System Log. In these cases, you are actually configuring the sensor that monitors events that are written to that log file. For these connectors, the Log File setting is disabled, and the system automatically populates the Log File field with the name of the Windows event log the sensor is monitoring. In most cases, you should be able to use the default log file path that is shown for the connector. These paths are based on the default vendor settings and the product documentation for each product. If a different log path is needed, type or paste the correct path in the Log File box, or use the Browse button to explore to correct folder or file. If you are uncertain about which file path to use, either refer to your original product documentation, or contact SolarWinds Technical Support.  

**i** If the product creates separate log files based on the current date or some other fixed interval, you can either select the log directory or any log file in that directory. If you select a log file, LEM reads through the directory’s log files in order, from the file you selected to the most current file. The LEM then reads new files as they are added.  

<p>| nDepth Host       | Only change this value if LEM is configured for nDepth log retention. If LEM is not configured to receive and store raw (unnormalized) log data in its own database, changing this value can cause all alert data to queue indefinitely. If you are using a separate nDepth appliance or nDepth VM, type the IP address or host name for the nDepth instance. Generally, the default setting is correct. Only change it if you are advised to do so. |</p>
<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>nDepth Port</td>
<td>Only change this value if LEM is configured for nDepth log retention. If LEM is not configured to receive and store raw (unnormalized) log data in its own database, changing this value can cause all alert data to queue indefinitely.</td>
</tr>
<tr>
<td></td>
<td>If you are using a separate nDepth appliance or nDepth VM, type the port number to which the connector is to send nDepth data. Generally, the default setting is correct. Only change it if you are advised to do so.</td>
</tr>
<tr>
<td>New File Name</td>
<td>Select the interval in which the connector posts and names each new log file. The interval tells the SolarWinds LEM when to begin reading the next log file. The default setting is Daily: yymmdd.</td>
</tr>
<tr>
<td>Interval</td>
<td></td>
</tr>
<tr>
<td>Output</td>
<td>Only change this value if LEM is configured for nDepth log retention. If LEM is not configured to receive and store raw (unnormalized) log data in its own database, changing this value can cause all alert data to queue indefinitely.</td>
</tr>
<tr>
<td></td>
<td>Select the appropriate data output option:</td>
</tr>
<tr>
<td></td>
<td>Event: This is the default option. It sends the connector's log file data as events to the SolarWinds LEM for processing by your correlation rules, associated active responses, SolarWinds Consoles, and databases.</td>
</tr>
<tr>
<td></td>
<td>nDepth: This option sends the connector's log file data to a separate nDepth appliance for archiving. The data does not go to the SolarWinds LEM, so any potential event activity does not appear in the Event Panel. However, you can still use the Console's nDepth explorer to search the data on this appliance.</td>
</tr>
<tr>
<td></td>
<td>Event, nDepth: SolarWinds recommends that you choose this option if you want to use nDepth to search log messages in addition to events. This option sends the connector's log file data to the SolarWinds LEM for event processing and to SolarWinds nDepth for data archiving. This means the LEM reports potential event activity in the Event Panel, and nDepth archives the connector's output data for later reference. Furthermore, you can use the Console's nDepth explorer to search either type of data.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>Type the IP address of the router or firewall. Use the following IP address format:</td>
</tr>
<tr>
<td>[Product] Server</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sleep Time</td>
<td>Type or select the time (in seconds) the connector sensor is to wait between event monitoring sessions. The default (and minimum) value for all connectors is one (1) second. If you experience adverse effects due to too many rapid readings of log entries, increase the Sleep Time for the appropriate connectors. Windows NT-based connectors automatically notify Windows Event Log sensors of new events that enter the log file. Should automatic notification stop for any reason, the Sleep Time dictates the interval the sensor is to use for monitoring new events.</td>
</tr>
<tr>
<td>Connector Version</td>
<td>This is the SolarWinds release version for this connector. This is read-only information for reference purposes.</td>
</tr>
<tr>
<td>Wrapper Name</td>
<td>This is an identification key that the SolarWinds LEM uses to uniquely identify the properties that apply to this particular connector. This is read-only information for SolarWinds reference purposes.</td>
</tr>
</tbody>
</table>

If the connector settings you need are not shown here, you are probably configuring an active response connector. (See the next section.) When you finish configuring the connector settings, start the connector.
The Connector Configuration form fields for active-response (Actor) connectors

The following table describes fields on the Connector Configuration form when configuring actors for active response connectors.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced</td>
<td>These settings are no longer applicable.</td>
</tr>
<tr>
<td>Auth Port</td>
<td>For CheckPoint OPSEC firewalls, select the port used to connect to the CheckPoint server via the LEA/OPSEC interface.</td>
</tr>
<tr>
<td>Base URL</td>
<td>Type the URL to connect to the SonicWALL firewall and perform the login. Include “http://” at the beginning of the URL. SolarWinds does not support HTTPS. Only use this connector for older SonicWALL firmware version.</td>
</tr>
<tr>
<td>Block Timeout</td>
<td>For CheckPoint OPSEC firewalls, type the timeout in seconds for the blocks to expire from the firewall. A value of zero (0) indicates never expire.</td>
</tr>
<tr>
<td>Client DN</td>
<td>For CheckPoint OPSEC firewalls, type the client DN string. The CN and O must be uppercase.</td>
</tr>
<tr>
<td>Configuration Mode</td>
<td>Select either telnet or SerialPort.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Type the connector’s password for entering Enable mode.</td>
</tr>
<tr>
<td><strong>FIELD</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Windows Active Response</td>
<td>For the Windows Active Response connector, select this check box to enable active response settings.</td>
</tr>
<tr>
<td>From Zone</td>
<td>Type the external zone used for configuring restrictions on firewall connections.</td>
</tr>
<tr>
<td>Incoming Interface</td>
<td>Type the Interface for which the block is to be made effective; that is, the Interface for which incoming traffic will be filtered to prevent traffic from the blocked IP address.</td>
</tr>
<tr>
<td>Password / Login Password</td>
<td>Type the connector's login password. For some products, the password name must be the same one that was used when the firewall was installed.</td>
</tr>
<tr>
<td>Port Name / Serial Port Name</td>
<td>Select a serial port for performing active response via console cable, if applicable. The port name represents the physical communication port on the computer. The port name is only relevant if the Configuration Mode (below) is set to SerialPort.</td>
</tr>
<tr>
<td></td>
<td>/dev/ttyS0 = serial port 1, and /dev/ttyS1 = serial port 2.</td>
</tr>
<tr>
<td></td>
<td>If the Configuration Mode is set to telnet, then this field is disabled and the Port Name box reads: There are no ports available.</td>
</tr>
<tr>
<td>Remote Connection Port</td>
<td>Type the firewall port used for connecting to and configuring the firewall.</td>
</tr>
<tr>
<td>Server DN</td>
<td>For CheckPoint OPSEC firewalls, type the server DN string. The “cn” and “o” must be lowercase.</td>
</tr>
<tr>
<td>Server Port</td>
<td>For CheckPoint OPSEC firewalls, select the port used to connect to the CheckPoint server via the SAM/OPSEC interface.</td>
</tr>
<tr>
<td>Server / Server Address / IP Address / [Product] IP Address</td>
<td>Type the IP address of the router or firewall. This address allows LEM to perform active responses to events on that particular router or firewall. Use the following IP address format: 192.123.123.123.</td>
</tr>
<tr>
<td>SSLCA</td>
<td>For CheckPoint OPSEC firewalls, click Browse to locate the SSL certificate file to upload to the server. If the connector is already configured, then use the existing certificate on the server. You can use the same path for both the LEA (log reading) and SAM (active response) certificates.</td>
</tr>
<tr>
<td>Take Admin Control</td>
<td>Only one person can configure the firewall at one time. Selecting this check box allows LEM's active response to take administrative control over the firewall when a user is logged into the WatchGuard Management Console. That is, LEM disconnects the user and takes control over the firewall.</td>
</tr>
<tr>
<td>To Zone</td>
<td>Type the internal zone used for configuring restrictions on firewall connections.</td>
</tr>
</tbody>
</table>
**FIELD** | **DESCRIPTION**
---|---
Connector Configuration Instance (Alias) | Type a name that easily identifies the product that LEM is to act on. For active response connectors, we recommend you end the alias with “AR”. For example, an alias for the Cisco PIX Active Response connector might be “Cisco PIX AR”. This allows you to differentiate the active response connector from the data gathering connector.

User Name / Login User Name | Type the user name needed to log onto and configure the firewall. For some products, the user name must be the same one that was used when the firewall was installed.

If the connector settings you need are not shown here, you are probably configuring a connector (data gathering) connector. When you finish configuring the connector settings, start the connector.

The System Tools connector form fields

LEM uses the System Tools connectors to interface with external notification systems.

**FIELD** | **DESCRIPTION**
---|---
Append Text to File Active Response

Description | Use this connector to have the Agent “write” the specified event data or text to the specified file.

How to append | Select Newline to write the event data to the file so that each event is on a distinct line (that is, one event per line), by inserting a return or newline character.

Select No Newline to stream the event data to the file by appending the new data immediately following any existing data in the file.

Maximum file size (MB) | Type the allowable maximum file size for the text file, in Megabytes.

Directory Service Query

Description | Use this connector to have the Manager communicate with existing directory services on the network to retrieve and update group information. This allows you to synchronize your existing Directory Service Groups for use with rules and filters.

User Name | Type a user name that is valid on the configured domain and server for authenticating to the domain and retrieving group information.

Directory Service Server | Type the IP address or host name of your directory services server (commonly, this is a domain controller).

Domain Name | Type the fully-qualified domain name of your directory services domain.

Password | Type the password for the above user name that is valid on the configured domain and server for authenticating to the domain and retrieving group information.
### FIELD DESCRIPTION

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Service Server's Port</td>
<td>Type the port used to communicate with the directory service server.</td>
</tr>
<tr>
<td>Email Active Response</td>
<td><strong>Description</strong> Use this connector to have a Manager automatically notify users of events by event policy. The event policy requires configuration.</td>
</tr>
<tr>
<td>Return Display Name</td>
<td>Type the name that you want to appear in the From field of active response e-mail messages.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port used to communicate with the internal email server.</td>
</tr>
<tr>
<td>Return Address</td>
<td>Type the email address that you want to appear in the From field of active response email messages.</td>
</tr>
<tr>
<td>Mail Host</td>
<td>Type the IP address or host name of an internal SMTP server that the Manager can use to send email messages through without authentication.</td>
</tr>
<tr>
<td>Authentication Server Username</td>
<td>Type the user name needed to access the internal email server, if required.</td>
</tr>
<tr>
<td>Authentication Server Password</td>
<td>Type the password needed to access the internal email server, if required.</td>
</tr>
<tr>
<td>Test E-mail Address</td>
<td>Type the e-mail address you want to use to test the Mail Host assignment. When you click Test Email, a test message should appear at this email address.</td>
</tr>
<tr>
<td>Test Email button</td>
<td>This button tests your email notification settings to ensure that you entered the correct e-mail host.</td>
</tr>
<tr>
<td></td>
<td>Click Test Email. Then check the email address's in-box. If you entered the correct address, the in-box should receive the test message.</td>
</tr>
</tbody>
</table>

**The Event Distribution Policy form**

Configure the event distribution policy to control how events are routed through the LEM system.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event/Field</td>
<td>Lists event categories and event types. Click ▼ to maximize an event category.</td>
</tr>
<tr>
<td>Console</td>
<td>Select a check box to indicate whether an event time or event category is sent to the console or local database.</td>
</tr>
<tr>
<td>Database</td>
<td>When selected, the event type is routed to that destination. Clear a check box to prevent the event type from being routed to that destination.</td>
</tr>
<tr>
<td>Warehouse Rules</td>
<td></td>
</tr>
<tr>
<td>Export</td>
<td>Exports a Manager event policy to a spreadsheet file.</td>
</tr>
</tbody>
</table>
FIELD | DESCRIPTION
--- | ---
![field_icon] | Click to select the Apply State to Branch command. This command pushes (or propagates) the selected event node check box settings down to the related, lower-level event types in the node tree hierarchy.

Description | Provides a description of the event type or event category currently selected in the grid.

See also:

- [Configure the LEM event distribution policy](#) for more information.

Nodes view

To add and manage remote logging devices and LEM Agents, navigate to Manage > Nodes on the LEM toolbar.

This topic provides page-level help for the Nodes view in the LEM console. See also [Send event data to LEM via Agents, syslog, and SNMP](#).

The following example shows the Nodes view in the LEM console.
The Nodes main view

The following tables describe the Nodes view elements.

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sidebar</td>
<td>Hides and opens the Refine Results pane.</td>
</tr>
<tr>
<td>Refine Results pane</td>
<td>Applies filters to reduce the nodes that appear in the Nodes grid based on your selection parameters (such as Manager or connector profile).</td>
</tr>
<tr>
<td>Nodes grid</td>
<td>Displays all Agent and non-Agent nodes associated with each Manager and appliance monitored by the LEM console. You can also add or scan for a new node.</td>
</tr>
<tr>
<td>Respond menu</td>
<td>Performs a selected action on a specific Agent. For example, you can send an Agent a pop-up message or shut down the host computer. This menu is similar to the Respond menu in the Monitor view event grid.</td>
</tr>
<tr>
<td>Remote Updates menu</td>
<td>This menu lets you control the Agent's automatic update status. Remote updates are a way for the Agent to automatically accept updated Agent software from the Manager when new software becomes available.</td>
</tr>
</tbody>
</table>

The gear button at the top of the grid opens commands that you can perform on multiple selections in the grid, and commands that do not require a grid selection. It includes commands for copying Agent information and for deleting Agents.

Nodes grid columns

The following table describes the columns in the Nodes grid.

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Node</td>
<td>Displays a wizard to assist you with adding nodes.</td>
</tr>
<tr>
<td>Scan for New Nodes</td>
<td>Scans syslog data sent to the LEM.</td>
</tr>
<tr>
<td></td>
<td>Displays a menu of commands you can perform on the selected item.</td>
</tr>
<tr>
<td></td>
<td>- Select Connectors to configure an Agent connector.</td>
</tr>
<tr>
<td></td>
<td>- Select Delete to delete Agent licenses from a Manager.</td>
</tr>
<tr>
<td></td>
<td>- Select Copy to copy Agent information to configure the Remote Agent Installer or for analysis in another application (such as Microsoft Excel).</td>
</tr>
<tr>
<td>Status</td>
<td>The Agent's current connection status:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ICON</th>
<th>STATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>🎀</td>
<td>Enabled</td>
<td>The Agent is connected to a Manager.</td>
</tr>
<tr>
<td>🎀</td>
<td>Disabled</td>
<td>The Agent is not connected to a Manager.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Node IP</td>
<td>The node IP address.</td>
<td></td>
</tr>
<tr>
<td>Node Name</td>
<td>The computer name that hosts the node. Typically, this is the computer name or host name assigned to the node.</td>
<td></td>
</tr>
<tr>
<td>Agent Node</td>
<td>The LEM Manager or Agent where the node logs are stored. This column is blank for LEM Agents.</td>
<td></td>
</tr>
<tr>
<td>USB</td>
<td>The current USB-Defender status of the node. A green icon 🟢 indicates USB-Defender is installed on the node. If no icon is present, USB Defender is not installed on the node. This column is blank for non-Agent nodes.</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>The node software version number. This column is blank for non-Agent nodes.</td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td>The operating system of the computer hosting the node. This column is blank for non-Agent nodes.</td>
<td></td>
</tr>
<tr>
<td>Profile</td>
<td>The connector profile associated with the node (if applicable). This column is blank for non-Agent nodes.</td>
<td></td>
</tr>
<tr>
<td>FIM</td>
<td>The current FIM status of the node.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Icon</strong></td>
<td><strong>Status</strong></td>
</tr>
<tr>
<td></td>
<td>🟢</td>
<td>Operational</td>
</tr>
<tr>
<td></td>
<td>🔴</td>
<td>Non-operational</td>
</tr>
<tr>
<td></td>
<td>No icon</td>
<td>Not configured</td>
</tr>
<tr>
<td>Updates Enabled</td>
<td>This field indicates whether the node is enabled for receiving remote updates.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Icon</strong></td>
<td><strong>Status</strong></td>
</tr>
<tr>
<td></td>
<td>🟢</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>🔴</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
### COLUMN | DESCRIPTION
--- | ---
Update Status | This field indicates the current software updated status for the Agent.

<table>
<thead>
<tr>
<th>ICON</th>
<th>STATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="current" /></td>
<td>Current</td>
<td>The Agent software is current.</td>
</tr>
<tr>
<td><img src="image" alt="outdated" /></td>
<td>Outdated</td>
<td>The Manager is running an update that is newer than the version used by this Agent.</td>
</tr>
<tr>
<td><img src="image" alt="updating" /></td>
<td>Updating</td>
<td>The Manager is sending an update to this Agent.</td>
</tr>
<tr>
<td><img src="image" alt="queued" /></td>
<td>Queued</td>
<td>The Agent is waiting to be updated while other Agents are updated.</td>
</tr>
<tr>
<td><img src="image" alt="unknown" /></td>
<td>Unknown</td>
<td>The Manager cannot determine the Agent software status.</td>
</tr>
<tr>
<td><img src="image" alt="canceled" /></td>
<td>Canceled</td>
<td>The user canceled the update during the update process.</td>
</tr>
<tr>
<td><img src="image" alt="error" /></td>
<td>Error</td>
<td>An error occurred during the update.</td>
</tr>
</tbody>
</table>

ID | The Agent unique identification number.
Manager | The Manager connected to the Agent. An Agent can only be connected to one Manager.
Install Date | The time and date the Agents were installed and connected to the Manager.
Last Connected | The time and date the Agent was last connected to the Manager.

The Nodes Refine Results sidebar

By default, the Agents grid shows every Agent associated with every LEM Manager that is monitored by the LEM console. Use the Refine Results sidebar to limit the number of Agents displayed in the grid.

When you select options in the Refine Results pane, the grid refreshes to show only those items that match the refinement options you have selected. The other items in the grid are still there, but they are hidden. To restore them, click the Reset button or select All in the refinement lists you are using.

The following table explains how to use the Refine Results form.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset</td>
<td>Clear the forms and the Agents grid to their default settings, displaying all Agents for all Managers.</td>
</tr>
</tbody>
</table>
### FIELD | DESCRIPTION
--- | ---
Search | Performs a keyword search for a specific Agent in the Name field.
Manager | Select the Manager you want to work with. Select All to include Agents from every Manager.
Profile | Select the connector profile you want to work with. Select All to include Agents from all connector profiles.
Node | Select whether you want to view Agent or non-Agent nodes.
Status | Select the connection status of the Agents you want to work with (Connected or Not Connected). Select All to include both.
Version | Select the Agent software version. Select All to include Agents of every version.
OS | Select the operating system of the computer hosting the Agent. Select All to include all operating systems.
USB | Select the USB-Defender status of the Agent (Installed or Not Installed). Select All to include both.

The Connector Configuration form

See [The Appliances view](#)

Add syslog and Agent nodes to LEM

This section describes several different ways you can add syslog and Agent nodes to LEM so that LEM can monitor their events.

**Add a syslog node to LEM using the Add Node wizard**

Complete these steps to add a syslog node to monitor a network device. The wizard locates the new node for you and recommends the appropriate connector.

1. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. Click Add Node.
4. Select Syslog node.
5. Enter the IP Address of the node.
6. From the drop-down list, select a node vendor.
7. Configure the node so LEM can receive syslog messages.
8. Select the I have configured this node so that LEM can receive its Syslog messages check box.
9. Click Next.
   LEM scans for new devices.
Use Scan for New Nodes to find new syslog sources and add connectors.

Use the Scan for New Nodes feature to configure and enable multiple connectors simultaneously.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, click Ops Center, and then locate the Node Health widget.
3. Click Scan for New Nodes in the widget toolbar.

![Node Health widget](image)

LEM begins scanning for new nodes in your network. If new nodes are found, the New Connector(s) found banner displays in the console. Otherwise, the No nodes found banner displays.

This process may require several minutes to complete. During the scan, a message appears indicating the scan is continuing in the background. A progress bar also displays at the bottom of the console.

4. Click View Now.

![New Connector(s) Found](image)

5. Select the recommended connectors you want to install, and then Click Next.

Move your pointer over the connector name for details.

6. Review the Summary information, and then click Finish.
The Nodes grid displays with the new nodes.
Click Monitor to view the events collected from the new nodes.
7. On the LEM toolbar, navigate to Manage > Appliances.
8. Click ☑️, and then select Connectors.
9. In the Refine Results pane, enter a keyword for your new connector.

10. Locate your connector in the list.

11. Next to the connector, click ☑️, and then select Edit.
12. Edit your connector settings as required, and then click Save.
   The node connector is enabled.

Manually add a new Agent or syslog node connector

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. In the Nodes grid, locate the nodes that are monitored by LEM.
4. Next to your targeted node, click ☑️, and then select Connectors.
5. Search Agent nodes by category or use the search box to locate a node by keyword.
6. Next to a search result, click ☑️, and then select new.
7. Configure the new node.
8. To start the node, click Start.

Other ways to add nodes to LEM

You can add nodes from the Getting Started wizard by clicking Add Nodes to Monitor.

A dialog box prompts you to choose the type of node you want to add.

Click the drop-down list, select an Agent or non-Agent node to monitor, and then follow the instructions to add the monitored node.

You can also click Add Node in the Node Health widget to perform the same function.

LEM Events Console

The LEM Events Console provides instant access to live event monitoring and filtering as well as historical record archives for in-depth analysis and troubleshooting. Within the console view, you can quickly switch between real-time event streaming and historical log views based on user-defined date and time parameters. In addition to live and historical keyword search options, all established LEM Monitor filters are accessible in the LEM Events Console Filters pane. You can access the console view by clicking Visit LEM Events Console in the top-right section of the LEM Console.
<table>
<thead>
<tr>
<th>NUMBER</th>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Events</td>
<td>The Events table displays the events that exist for your selected filter, live and historical. The title bar displays the filter name you select in the Filters pane. In Live Mode, events stream into the viewer as they occur in your network. Enter Live filter keywords in tandem with the Filters pane to monitor specific activity as it occurs. Click Historical Search to apply filters and view your aggregated event logs.</td>
</tr>
<tr>
<td>2</td>
<td>Filters</td>
<td>All established LEM Monitor filters are accessible in the LEM Events Console Filters pane. The Filters pane displays all filters you can apply to the console event messages. All filters are stored in groups. To add a filter to the events table, click to expand a filter group, and then select a filter. The events table title changes to the name of the event and the grid refreshes and displays the incoming events allowed by the filter conditions. To create or edit filters, return to the Monitor view in the LEM Console.</td>
</tr>
<tr>
<td>3</td>
<td>Toolbar</td>
<td>Use the console toolbar to return to LEM, view your notifications, and access the Settings page where you can establish a maximum search threshold and user access configurations. You can also log out, and launch the Success Center.</td>
</tr>
<tr>
<td>4</td>
<td>Detail</td>
<td>The Detail pane displays specific information about the last event you selected in the Events table. When you click an event, the event is highlighted in the Detail pane along with supporting information. To view the event details for a specific event, select the event in the event stream and review the results in the Detail pane. Click the Hide Panel icon to collapse the pane, or the Show Panel icon to expand it. Click the icon to copy CSV-formatted event details to your system clipboard. You can also enter specific keywords in the pane to filter and view specific event data.</td>
</tr>
</tbody>
</table>
View the LEM Events Console in HTML5

The LEM Events Console view is presented in HTML5 format, which means no requirement for Adobe® Flash® or other third-party media players. This update also results in a more robust console that can run on any computer operating system as well as most web browsers. Find more information here.

Enable log forwarding

On the LEM Events Console Settings page, enable log forwarding to direct your raw (unnormalized) log messages to a dedicated server. This option allows you to forward log data to third-party systems and other SIEM tools.

When you configure connectors to send original log data to LEM, the messages are then auto-forwarded to the designated location. To use this feature, configure nDepth log retention and applicable connectors accordingly.

When enabled, you can switch between storing logs in the raw logs database (nDepth) and forwarding logs with syslog protocols (RFC3164 and RFC 5244). There is no option to filter logs based on IP address, connectors, rules, etc.

- Rules do not fire on raw (unnormalized) log data. Rules can only fire on normalized data.
- Raw (unnormalized) log messages do not appear in Monitor view in the console.
- If you enable original log storage (raw database storage), and you enable connectors to send data to both databases, LEM storage requirements may double for the same retention period, and extra resource reservations of at least two additional CPUs and 8-16GB of RAM may be required.

Configure LEM Manager to store original log files in their own database

The following procedure must be completed prior to configuring any connector to send log messages to your LEM appliance.

1. Open the CMC command line. For steps, see Log in to the LEM CMC command line interface.
2. At the cmc> prompt, enter manager.
3. At the cmc::manager> prompt, enter configurendepth and follow the prompts to configure your LEM Manager to use an nDepth server:
   a. Enter y at the Enable nDepth? prompt.
   b. If you are prompted with Run nDepth locally? (Recommended), enter y. This will configure a separate database on your LEM appliance to store original log files.
   c. If your LEM implementation consists of several appliances, follow the prompts to complete the process for your dedicated database or nDepth appliance. For additional information about this process, contact Support.
4. Back at the `cmc::manager>` prompt, enter `exit` to return to the previous prompt.

```
NOTE: Commands with an asterisk (*) include an automatic manager service restart
CMC::manager> configurendepth
Configuring the nDepth manager system.
* Manager is already configured to use nDepth at localhost
* Disable nDepth? (y/N) y
Run nDepth locally? (Y/n) y
cmc::manager> exit
```

5. At the `cmc>` prompt, enter `ndepth`.

6. At the `cmc::nDepth>` prompt, enter `start`. This command will start the Log Message search/storage service.

7. Enter `exit` to return to the previous prompt.

8. Enter `exit` to log out of your LEM appliance.

Configure connectors to send original log data to LEM

1. Open the connector for editing in the Connector Configuration window for the LEM Manager or LEM Agent, as applicable:
   - **If the connector has already been configured**, stop the connector by clicking gear > Stop, and then click gear > Edit.
   - **If the connector has not been configured**, create a new instance of the connector by clicking gear > New next to the connector you want to configure.
2. In the Connector Details pane, change the Output value to Alert, nDepth. Leave the nDepth Host and nDepth Port values alone unless otherwise instructed by Support.

The Output values are defined as:

- **Alert**: Sending data to the alert database
- **nDepth**: Sending data to the RAW (original log) database

For help, see [The Connector Configuration form fields for data-gathering (sensor) connectors](#).

3. If you are finished configuring the connector, click Save.

4. Start the connector by clicking gear > Start.

5. Click Close to close the Connector Configuration window.

6. Repeat these steps for each connector you want to send original log data to your LEM appliance.

   Learn more about using connector profiles to create forwarding policies [here](#).

Establish log forwarding settings

1. In the LEM Events Console, click the Settings button.
2. On the Settings page, click the Log Forwarding tab.

3. To enable log forwarding for adjusted connectors, select the Enable log forwarding for adjusted connectors check box.

   Log Forwarding can only be enabled for connector output set to nDepth.

4. Enter the destination IP address or host name, and then enter the destination port.

5. Make a selection from each of the following drop-down lists (the standard settings appear by default):
   - Protocol: UDP or TCP
   - RFC format: 3164 or 5424
   - Severity: The severity level is applied to all forwarded logs
   - Facility: The destination application
6. Enter an App name (optional), and then click Save.
7. To return to the LEM Events Console, click Monitor.

Node management

Through the HTML5-based LEM Management feature, you can add agent nodes, configure connectors, and then monitor activity in the LEM Events Console. Upon node and connector configuration, click the Monitor tab to view your network activity, and then create and apply filters to tailor your log feed to view event logs vital to maintaining the health of your network environment.

- Agents: An agent is a software application installed on the device that collects and normalizes log data before it is sent to the LEM Manager.
- Non-Agent devices: These are devices that send log data directly to the LEM Manager for normalization and processing, such as firewalls, switches, and routers.

On the Nodes tab, you can view a list of both agent and non-agent nodes, and select multiple nodes to conduct bulk operations, such as deleting nodes, upgrading agent nodes, and starting File Integrity Monitoring (FIM) on agent nodes.

Select one or more items in the Refine Results panel to organize your nodes view, or use the Nodes toolbar to search for nodes, or organize nodes by Name, IP address, OS type, or version.

Add an agent node

1. In the LEM Events Console, navigate to Manage > Nodes, and then click Add Agent Node.
The Add agent node window appears displaying options for remote and local installation.

Add agent node

To install the appropriate agent for your device, download the agent for either remote or local installation.

A) Remote Installation (only for Windows)
   You can directly download the Windows Agent Remote Installer.

B) Local Installation
   Log on to the device you want to install the agent on, then download and install the appropriate agent from the following:
   AIX Agent Installer
   HP UX Itanium Agent Installer
   Linux 64 Agent Installer
   Linux Agent Installer
   Mac OS Agent Installer
   Solaris Agent Installer
   Solaris Intel Agent Installer
   Windows Agent Installer

After running the agent installer, you should see the events for your agent device appear in the Monitor window.

2. Select an option, and then follow the instructions to add the monitored node.

Start the FIM driver

File Integrity Monitoring (FIM) monitors all file types for unauthorized changes. Using FIM, you can detect changes to critical files to ensure systems have not been compromised.

You must first configure FIM in the legacy LEM Console under Manage > Nodes.
1. In the LEM Events Console, navigate to Manage > Nodes.
2. In the Refine Results panel, expand the Type group, and then select Agent.
3. Select an agent to view the configuration toolbar.
4. From the More drop-down list, select Start FIM Driver.
5. Upon successful configuration, a success dialog appears in the upper-right console.

From the More drop-down list, you can start an FIM driver, and enable or disable FIM on Agent startup.

Add and modify connectors for agent devices

Connectors intercept events sent from a specific product on your network and convert those events into normalized messages that LEM can understand.

1. To view your connectors, select an agent on the Nodes tab, and then click Manage Node Connectors.

- or -

For Manager connectors, click the Manager Connectors tab to view configured and available connectors.
2. Find the connector to configure. Type part of the connector name in the search box, or use the filter menus in the Refine Results panel.
3. Select an available connector, and then click Add Connector.

4. Complete the connector configuration form. The following fields are common across most connectors:
   - **Name**: Enter a user-friendly label for your connectors.
   - **Log File**: Enter the location of the log file that the connector will normalize. This is a location on either the local computer (Agents), or the LEM appliance (non-Agent devices).
   - **Output**: Normalized, Raw + Normalized, Raw. You only need to configure these values if LEM is configured to save raw (unnormalized) log messages.

5. Click Add.

6. To start a connector, select a configured connector, and then click Start.
Create filters in the LEM Events Console

In the LEM Events Console, you can create custom filters for your event log stream to complement existing LEM Monitor filters. On the Add New Filter page, create filters by dragging and dropping default filter values, or by adding your own custom filter values. The filter builder also guides you through selecting operators and conditions to group a particular type of event, or to monitor specific events and activity.

You can add and edit filters at the root or group level. Find more information about LEM groups here.

1. In the LEM Events console, click the Monitor tab.
2. To create a filter at the group level in the Filters panel, move the mouse pointer over a group heading to expose the vertical ellipsis, and then select Add New Filter.

-OR-

To create a filter at the root level, click the add icon, and then select Add New Filter.

3. Enter a descriptive name for your new filter.

To establish notifications for the new filter, go to the filter builder in the legacy LEM console.
4. Drag a value into the filter builder. The drag panel on the left contains searchable filter values that you can drag into the filter builder. Expand a filter group to select a value, or locate your value by entering a term in the search field.

When you drag a value into the filter builder, the correct drop location is illuminated with a blue line.

If you know the specific values for your filter, click the add icon, and then enter your custom values.
5. From the drop-down list, select an option, or enter a specific value or keyword directly.

To change the And operator, or to group (bracket) the filter values, click And, and then select Or, or Group. Follow the same steps to ungroup the values.

**Edit filters**

In the Filters pane, you can edit existing filter values to adjust event types streaming into your log feed.
1. In the LEM Events console, click the Monitor tab.

2. In the Filters panel, scroll down to locate your filter, move the pointer over the filter to expose the vertical ellipsis, click it, and then select Edit.

3. The selected filter conditions appear on the Edit Filter page.

   Name *
   Rule Activity

   Filter is true when

   - InternalRuleFired occurred
   - InternalTestRule occurred

   OR

   Click or drag item from the left panel.

4. To adjust the filter conditions, move the pointer over any of the filter conditions.
5. The edit a condition, click the pencil icon.

![Edit Condition](image)

6. Adjust one or more values, and then click Save.

7. To delete a condition, click the delete icon.

8. To add a new condition, click the add icon.

9. To keep your edits, click Save.

Set maximum number of search results

In the LEM Events Console, you can set the maximum number of results per search query. Initiating searches with a high maximum threshold can negatively impact LEM performance, so consider a low-to-moderate maximum threshold.

1. In the LEM Events Console, click the Settings button.

- ![Go to LEM Console](image)

2. On the Settings page, click the Search tab.

3. Set the max number of search results, and then click Save.

4. On the confirmation message, click Save.

5. To return to the LEM Events Console, in the upper-left corner, click Monitor.

Filter and monitor events in Live Mode

Switch the LEM Events Console to Live Mode to monitor events as they occur in your environment. This is particularly useful when troubleshooting active network problems. You can apply "live" filters to target and identify issues using the Filters pane and Live filter keywords, and then conduct a historical log search for additional event analysis.
Live Mode also reconciles device polling gaps by processing and correlating a consistent stream of log event data.

1. In the LEM Events Console, switch to Live Mode.
2. In the Filters pane, select an event filter.
3. In the Live filter field, enter one or more keywords. The Live filter updates the event stream as you type. Do not click the Historical Search button.

   Live events continue to stream into the viewer table, but only records meeting the defined search criteria are visible. Adjust the filters and keywords at any time to monitor different event groupings.

4. Click an individual event in the event stream to view additional information in the Event Details pane.

   As you scroll through the event log table or select an individual event, the console enters Paused Mode, so new events will not stream into the viewer until you return to Live Mode. However, when you are in Paused Mode, the number of new live events matching your filter criteria appear next to the selected search filter.

You can also move out of Live Mode and apply the same search criteria to your historical records for additional reference.

The LEM Events Console supports the * wildcard for real-time and historical searches.

## Search and filter historical event logs

The LEM Events Console includes an advanced search capability to access your aggregated event logs based on existing Live Mode filter values and a specified time range.

1. On the LEM Events Console search bar, click Historical Search.

   When you click Historical Search, the search is initiated with the most recent filter values used in Live Mode. Changing the selection in the Filters cancels the search and returns to Live Mode.

2. In the search field, enter one or more keywords.
3. Next to the Search button, click the time setting to open the custom time picker.
4. Select a quick pick option, or specify your own date and time range.
5. Click Search.

To return to Live Mode, click the arrow next to the search field. The live event stream resumes using the last search filter you applied.

View multiple console tabs

You can open and monitor multiple LEM Events Console tabs in your web browser. You can apply the same filters simultaneously in live and paused mode, and initiate multiple search queries.

Running multiple searches simultaneously can negatively impact LEM performance due to hardware resource limitations.

Remote database (L4) configuration

Configuring the LEM Events Console with a remote database limits available console functionality. You can still search, filter, and monitor live events, but not historical records or event details. In this instance, a remote database notification appears in the upper right of the console reminding you of the limited functionality.
LEM troubleshooting

Troubleshoot alerts in the LEM console

This section describes how to troubleshoot unmatched data or internal new connector data alerts that may appear in your LEM console.

Typically, unmatched data and internal new connector data alerts indicate that one or more of the connectors on the LEM VM or appliance cannot properly normalize the associated log data.

1. Ensure that your syslog devices are sending logs to a syslog facility on your LEM appliance.
2. Determine which devices are logging to each facility, and whether those devices conflict with each another.
3. Ensure that your LEM Agent connectors, such as Windows-based and database connectors are running correctly.
4. Apply the latest connector update package.
5. Generate a syslog sample from the LEM appliance, and then open a ticket with SolarWinds Technical Support for further assistance.

Task 1: Troubleshoot syslog devices

Complete the following troubleshooting procedures for devices that send logs to a syslog facility on your LEM appliance.

1. Verify the connector and device are pointed at the same local facility.
2. Check the configuration on your device to determine what local facility it is logging to on your LEM appliance. In some cases, you cannot modify this setting.

   a. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   b. On the LEM toolbar, navigate to Manage > Appliances.
   c. Locate your LEM appliance in the grid.
   d. Click 🗝️, and then select Connectors.
   e. Locate the connector in the list.

   For additional information, search for your device in the Connectors section of the SolarWinds Success Center. Except for CheckPoint firewall, the LEM receives UDP syslog data on port 514.

3. Verify that the connector is pointed to the same logging facility as the device.
Use the search box at the top of the Refine Results pane or select Configured.

f. Select the configured connector and view its details. Verify the Log File value matches the output value in the device configuration.

4. If the device and connector configurations do not match, point the connector to the appropriate location.
   a. Click 👁, and then select Stop.
   b. Click 👁, and then select Edit.
   c. Change the Log File value so it matches your device.
   d. Click Save.
   e. Click 👁, and then select Start.

💡 For a video presentation about how to troubleshoot syslog nodes in LEM, open the following URL in a web browser:
https://thwack.solarwinds.com/docs/DOC-176148

Task 2: Troubleshoot device logging

Certain devices (including Cisco devices) have similar logging formats that cause connector conflicts when logging to the same facility on your LEM appliance. Use the following procedure and table to determine what devices are logging to each facility, and whether those devices conflict with one another.

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. At the cmc> prompt, type appliance.
3. At the cmc::appliance> prompt, type checklogs.
4. Enter an item number to select and view a local facility.
5. To view the device sending the event, open the log facility.

   The EPOCH timestamp (1427722392000) starts each event, which is the date and time in Unix numeric format. The device sending the event (such as 192.168.2.251) follows. You will typically see ProviderSID (ASA-1-106021), which is similar to an Event ID.

6. If two or more devices are logging to the same facility, see Troubleshoot conflicting devices to determine whether those devices conflict with each other.

Troubleshoot conflicting devices

Different firewall types should log to different facilities. For example, Cisco firewalls and Palo Alto should log to different facilities. However, both devices should log to their own facilities. Ensure that the devices in each of these groups are logging to distinct local facilities on your LEM VM. For example, if a device in Group 1 is logging to local1, make sure a device in Group 2 is not also logging to that facility.

SolarWinds recommends splitting the devices and vendors to different facilities. Having all devices pointed at one facility with multiple connectors reading that facility will impact your LEM performance.
### Task 3: Troubleshoot Agent devices and connectors

Complete the following procedure to troubleshoot LEM Agent connectors, such as Windows-based and database connectors.

1. **Verify the connector is pointing to the appropriate folder or event log.**
2. **Check the configuration on the host computer to determine which folder or event log it is logging in to.**
   
   In some cases, you cannot modify this setting. For additional information, search the SolarWinds Success Center for your device.

3. **Verify that the connector is pointed to the same folder or event log as the device:**
   a. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   b. On the LEM toolbar, navigate to Manage > Nodes.
   c. Locate the LEM Agent for the host computer.
   d. Click ✤, and then select Connectors.
   e. Locate the connector in the list.
      
      Use the search box in the Refine Results pane or select Configured.
   f. Select the configured connector and view its details. Ensure the Log File value matches the output value in the host computer configuration.

4. **If the host computer and connector configurations do not match, point the connector to the appropriate location:**
   a. Click ✤, and then select Stop.
   b. Click ✤, and then select Edit.
c. Change the Log File value so it matches the host computer.
d. Click Save.
e. Click , and then select Start.

Task 4: Apply the latest connector update package

If you completed the procedures in this section and you still see the unmatched data or internal new connector data alerts, apply the latest connector package before you contact Technical Support. See Apply a LEM connector update package to learn how.

Task 5: Contact SolarWinds Technical Support

If you are unable to resolve your issue using this article, open a ticket with SolarWinds Technical Support for further assistance. Be prepared to provide the following information to a support technician:

- A copy of the LEM report (in Crystal Reports format) entitled Tool Maintenance by Alias for the last 24 hours or the period during that the unmatched data was detected.
- (Syslog devices only). A sample of the logs currently sent to LEM for the affected connector. For more information, see Export log files using the CMC exportsyslog command.
- (Windows connectors only). A copy of the entire event log in English and EVTX formats.
- (Database connectors only). A sample of the event table containing the unread events and the details about these events.
- (Database connectors only). The database schema (if available).

Generate a syslog sample from the LEM appliance

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
2. At the cmc> prompt, type appliance.
3. At the cmc::appliance> prompt, type exportsyslog.
4. Enter an item number to select a local facility to export.
5. Repeat the previous step to specify more than one facility.
6. Enter q to proceed.
7. Follow the on-screen instructions to complete the export.

Troubleshoot the LEM desktop console

Refer to the topics in this section if the LEM desktop console is not working properly.

The LEM desktop console cannot resolve the LEM VM hostname

Ensure that the system hosting the LEM desktop console can resolve the LEM VM hostname using either DNS, or a manual entry in the Windows hosts file. If the desktop console cannot get an IP address for the LEM VM hostname, the console will be unable to connect to the VM, or the connection may be unreliable.
On your DNS server, configure forward and reverse DNS entries (a HOST and PTR record) for the LEM VM on your DNS server. When you create the DNS entries, use either the default hostname, or the hostname you specified during activation.

If you cannot configure DNS directly on your DNS server, configure the local Windows `hosts` file on the computer running the LEM desktop console.

⚠️ Create a backup copy of your Windows `hosts` file before you edit it.

1. Open the `hosts` file in a text editor. The file is located here:
   ```
   Windows\System32\drivers\etc\hosts
   ```
2. Add a line break, followed by a line with the LEM VM IP address and hostname. The IP address and hostname should be separated by a tab or space.

The LEM desktop console cannot connect after you activate the license or change the LEM VM hostname

The desktop console automatically attempts to reconnect to the LEM Manager after you activate the license. If the desktop console cannot connect, or if you changed the LEM Manager hostname, try the following:

1. Log in to the LEM desktop console.
   See [Log in to the LEM desktop console](#) for steps.
2. On the LEM toolbar, navigate to Manage > Appliances.
3. Delete the LEM VM configuration.
4. Add back the LEM VM settings.

Troubleshoot LEM Agents and network devices

If you do not see the events you expected to see in the LEM console, use the following procedures to troubleshoot your LEM Agents and network devices.

Determine if LEM is receiving data from the device that you are troubleshooting

SolarWinds recommends starting with this task before moving on to the other troubleshooting tasks.

1. Open the CMC command line. See [Log in to the LEM CMC command line interface](#) for steps.
2. At the `cmc>` prompt, enter:
   ```
   appliance
   ```
3. At the `cmc::appliance>` prompt, type:
   ```
   checklogs
   ```
4. To select a local facility to view, enter an item number.

5. Search for the specific device logging to this facility (such as the product name, device name, or IP address).

See also:
- Troubleshoot devices not logging to a log file
- Troubleshoot devices logging to a log file

Troubleshoot devices not logging to a log file

Perform the following procedure for network devices that do not show data on the LEM appliance.

1. Ensure that the device is configured to log to the LEM appliance.
2. Ensure that the device is logging to the correct IP address for the LEM appliance.
3. If the device sends SNMP traps to the LEM appliance, ensure that the LEM Manager is configured to accept SNMP traps.
   See Enable LEM to receive SNMP traps by turning on the SNMP Trap Logging Service for details.
4. Ensure that a firewall is not blocking data communications between the device and the LEM appliance.

Troubleshoot devices logging to a log file

Perform the following procedure for network devices that display data in LEM.

1. Ensure that the appropriate connector is configured on the LEM appliance.
2. Ensure that your configured connector is running.
3. If the connector is running, delete and recreate the connector instance.

Troubleshoot a LEM Agent

To begin, ensure that the LEM Agent is connected to the LEM appliance:

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Manage > Nodes.
3. In the Refine Results sidebar, click the Node drop-down menu and select Agent.
4. In the Status column, note the status icon for the LEM Agent:
   - If the LEM Agent does not appear in the Nodes screen, see Troubleshoot a missing LEM Agent
   - If the LEM Agent appears in the Nodes screen with a Connected status, see Troubleshoot a connected LEM Agent
   - If the LEM Agent appears in the Nodes screen with a Disconnected status, see Troubleshoot a disconnected LEM Agent.
Troubleshoot a missing LEM Agent

1. Verify that the LEM Agent is installed on the host computer.
2. Verify that the LEM Agent service is running on the host computer.

Troubleshoot a disconnected LEM Agent

1. On the host computer, verify that the LEM Agent Service is running.
   - If the service is not running, start the service.
   - If the service is running, go to the next step.
2. On the host computer, ping the LEM VM or appliance by hostname.
   - If the ping is successful, clear the LEM Agent certificate.
   - If the ping is not successful, go to the next step.
3. On the host computer, ping the LEM VM or appliance by IP address.
   - If the ping is successful, the LEM Agent is connected. See Troubleshoot a connected LEM Agent.
   - If the ping is not successful:
     a. Resolve any network or firewall issues between the LEM Agent and the LEM VM/appliance.
     b. Change your DNS settings so the LEM Agent computer can resolve the LEM appliance hostname (recommended).
     c. Edit or delete the spop.conf file (based on your system bit type) so that the LEM Agent calls the LEM VM or appliance by its IP address instead of its hostname. See Edit or delete the spop.conf file.

Edit or delete the spop.conf file

Perform the following procedure so the LEM Agent calls the LEM appliance by its IP address (Windows systems only).

1. Stop the SolarWinds Log and Event Manager Agent service.
2. If you are running a 32-bit Windows system, delete the spop folder. Do not delete the ContegoSPOP folder.
   - The folder is located at:
     C:\Windows\System32\ContegoSPOP\spop
   - If you are running a 64-bit Windows system:
a. Open the following directory:
   C:\Windows\SysWOW64\ContegoSPOP\spop
b. Open the spop.conf file in a text editor.
c. Replace the ManagerAddress value with the LEM appliance IP address.
d. Save and close the file.

3. Start the SolarWinds Log and Event Manager Agent service.

Troubleshoot a connected LEM Agent

1. Verify that you configured the appropriate connectors on the LEM Agent.
   For example, the LEM Agent for Windows runs the connectors for the Windows Application and Security Logs by default. However, you must configure the connector for the DNS server role.
2. Verify that all configured connectors are running properly.
3. If all configured connectors are running properly, delete and recreate the non-working connectors.

Contact SolarWinds Customer Support

If events from your network device do not appear in the LEM console after completing these procedures, send a screen shot of the device logging configuration screens and the appropriate system files to SolarWinds Customer Support:

https://support.solarwinds.com/Success_Center

If you are running a 32-bit Windows system, send the following files to SolarWinds Customer Support:

- C:\Windows\System32\ContegoSPOP\spoplog.txt (the most recent version)
- C:\Windows\System32\ContegoSPOP\tools\readerState.xml

If you are running a 64-bit Windows system, send the following files to SolarWinds Customer Support:

- C:\Windows\SysWOW64\ContegoSPOP\spoplog.txt (the most recent version)
- C:\Windows\SysWOW64\ContegoSPOP\tools\readerState.xml

Troubleshoot syslog error messages in LEM

If a No Device Found error message appears in the widget, make sure that you configured the device to send logs to the correct IP address. See Troubleshoot alerts in the LEM console for troubleshooting steps.

LEM console does not display syslog data

Verify that your devices are configured to forward syslog data to the LEM virtual appliance IP address. If your appliance cannot receive logs, your device may not be supported.
If your devices are configured correctly and your LEM appliance is still not receiving syslog data, identify the facilities that are collecting log data. When you complete this process, configure the appropriate connector from the facility to the log device so Log & Event Manager can normalize and monitor this information in the LEM Manager.

**Identify your syslog data facilities containing log data**

Verify that Log & Event Manager is receiving the raw data from your syslog devices.

- See your hypervisor documentation for information about using the virtual console.

1. Open the CMC command line. See [Log in to the LEM CMC command line interface](#) for steps.
2. At the `cmc>` prompt, type `Appliance`.
3. At the `cmc::appliance>` prompt, type `checklogs` and press Enter.

   The appliance displays all facilities receiving logs from syslog devices, such as firewalls, routers, and switches.
In this example, 1, 12, and 18 are active syslog facilities because they contain stored log data. Facilities 13, 15, 16, and 17 are inactive because their syslog log files are empty.

4. Match a facility with a monitored device.
   a. Choose a facility number and record the local number (such as local2) for a future step.
   b. Enter your chosen facility number (for example, 14 for local2), and then press Enter.
   c. Enter b or E to view the beginning or end of the log file, respectively, and press Enter.
   d. Enter the number of lines to display on your screen, and then press Enter.

   Pressing Enter defaults the output to 500 lines.

   e. Press Enter again.

       The raw data appears on your screen.

   f. Review and match the data to a monitored syslog device in your network.

5. Repeat steps 3 and 4 in this section to match additional facilities with log data to a monitored syslog device in your network.

Configure a connector from the facility to the device

The following table maps each syslog facility to the file name in the LEM Manager. The connectors defined in LEM Manager read these logs to normalize the Log & Event Monitor events.

<table>
<thead>
<tr>
<th>SYSLOG FACILITY</th>
<th>LOG FILE PATH</th>
</tr>
</thead>
<tbody>
<tr>
<td>local0</td>
<td>/var/log/local0.log</td>
</tr>
<tr>
<td>local1</td>
<td>/var/log/local1.log</td>
</tr>
<tr>
<td>local2</td>
<td>/var/log/local2.log</td>
</tr>
<tr>
<td>local3</td>
<td>/var/log/local3.log</td>
</tr>
<tr>
<td>local4</td>
<td>/var/log/local4.log</td>
</tr>
<tr>
<td>local5</td>
<td>/var/log/local5.log</td>
</tr>
<tr>
<td>local6</td>
<td>/var/log/local6.log</td>
</tr>
<tr>
<td>local7</td>
<td>/var/log/local7.log</td>
</tr>
</tbody>
</table>

The hardened operating system will prevent you to access the file system.

After you verify that data is received from a device, manually enable the log connector that supports the device. The connector maps events from the monitored Windows system event log to a LEM normalized event.

1. Match the facility of your monitored device with the corresponding log file path.
2. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for
3. On the LEM toolbar, navigate to Manage > Appliances.

4. Next to the appliance name, click 🛠, and then select Connectors.

5. In the Refined Results pane search field, enter the brand name of the monitored device and press Enter.

If your device does not display in the list, contact Customer Sales (for an evaluation license) or Technical Support (for a production license) for assistance with unsupported devices.

6. Next to the device, click 🛠, and then select New.

7. In the Log File field, make sure the localx portion of the path matches the facility number you configured on your device or the facility you recorded in the previous procedure.

   For example, if your recorded facility is local2, enter /var/log/local2.log in the field.

8. Verify that the remaining fields and selections are correct, and then click Save.

   The connector appears in the Connectors grid with a gray status icon.

9. Next to the connector, click 🛠, and then select Start.

   When the status icon turns green, the LEM connector is configured correctly.

View the data from the device

After you configure a connector to the facility, verify that the LEM appliance is receiving log data from the device.

You may need to authenticate to the device to generate data, as some devices do not generate a continuous stream of data.

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

2. On the LEM toolbar, click Monitor.

3. In the Filters pane, expand Overview, and then click All events.

4. Watch for new events that appear in the grid with the device IP address in the DetectionIP column.

   When new events display with your device IP address, the device is sending log data to the LEM appliance.
Troubleshoot LEM rules and email responses

This section provides troubleshooting steps to try if your LEM rules that are not firing as expected or if your rules are not sending the expected notifications.

General rule troubleshooting

If you created a rule that generates unexpected results, verify the following to track down the root cause:

1. On the LEM toolbar, click Monitor, and then check for the requisite events.
   For example, if your rule is based on the NewGroupMember event, locate a requisite event in the All Events or default Change Management filter.

2. If you cannot view the requisite events, troubleshoot your devices and connectors to move the events into LEM.

3. Check for an InternalRuleFired event in the SolarWinds Events filter.
   If you see an InternalRuleFired event for your rule, go to the next step.
   If you do not see an InternalRuleFired event for your rule, verify that:
   - The rule is enabled.
   - The Correlation Time or Response Window in your rule was not modified.
   - You did not click Activate Rules after saving your rule.
   - The time on your device is not more than five minutes off from the time on your LEM appliance.

4. If you see an InternalRuleFired event for your rule but LEM does not respond to the rule as expected, check the following:
   - **Send Email Message**
     Verify you configured and started the Email Active Response connector on the LEM Manager. Additionally, verify you associated an email address for your selected LEM user as your email account.
   - **Agent-based Actions**
     Verify you installed the LEM Agent on a computer that will respond to LEM.
   - **Block IP**
     If using the Block IP active response, verify that you configured the active response connector for the targeted firewall that will respond to this action. The active response connector is separate from the data-gathering connector.
The rule fires but you do not receive an email

Problem statement: You see the expected `InternalRuleFired` alerts in the default SolarWinds Alerts and Rule Activity filters in the LEM console, but you are not getting the expected email notification.

To resolve this issue:

1. Verify that the `ExtraneousInfo` field of the `InternalRuleFired` alert shows the associated email action in `Email [recipient]` format.
2. If this action is not present, add the Send Email Message action to the rule.
3. Verify that the intended recipient has an email address associated with his LEM user account:
   a. Open the LEM console. See [Log in to the LEM web console](#) or [Log in to the LEM desktop console](#) for steps.
   b. On the LEM toolbar, navigate to Build > Users.
   c. Click the LEM user account associated with the intended recipient.
4. If the Contact Information box is blank in the User Information pane, edit the user to add an email address.

   If you cannot add an email address to an Active Directory user, create a separate user, add the email to that user account, and then select that user in the email template.

5. Verify that the Email Active Response connector is configured on your LEM Manager.
   a. On the LEM toolbar, navigate to Manage > Appliances.
   b. Next to your LEM Manager, click ⚙, and then select Connectors.
   c. In the Connector Configuration window, select the Configured check box.
6. If Email Active Response is not in the list, clear the Configured check box configure the missing connector.

The rule does not fire and expected alerts do not display

Problem statement: You cannot see the expected `InternalRuleFired` alerts in the default SolarWinds Alerts or Rule Activity filters in the LEM console or the alerts needed to fire your rule anywhere in your LEM console.

To determine if the requisite alerts are in your LEM console, create a filter or nDepth search that matches the correlations in your rule.

If the alerts are not present, complete the following procedure:

1. Review the network devices sending syslog data to the LEM and validate the configurations on that network device to send data. Verify that one of your devices is logging the events you want to capture.
For example:

- Remote logging devices, such as firewalls and web filters, should be logging your web traffic events
- Domain controllers and end-user computers should be logging domain-level and local authentication and change management events

If you have multiple domain controllers, they will not all replicate every domain event. Each server only logs the events they execute.

- Other servers, such as database servers and web servers, should be logging events associated with their particular functions.

2. Verify that the LEM is receiving data.

Verify that the LEM icons display a syslog or Agent connection. Syslog device IPs display with the 🆙 icon in the Manage > Nodes grid. Agent host names and IP addresses appear in the Manage > Nodes list with the 🆙 icon.

Next, verify that the syslog facility or Agent is receiving data. If a network syslog device is sending syslog data to the LEM, you can view the LEM syslog files for that data.

a. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.

b. Type appliance, and enter the checklogs command.

You can also open a PuTTY session on port 32022 as a cmc user.

c. View the syslog that was chosen by the network device. All the data received in this area is UDP traffic received on port 514.

3. If your device is not in the Nodes list, configure your computers by installing a LEM Agent or configure other devices (such as firewalls) to log to your LEM VM or appliance. After your device is in the list, continue to the next step.

4. If your device is in the Nodes list, configure the appropriate connectors:

a. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.

b. On the LEM toolbar, navigate to Manage > Appliances.

c. Next to the Agent or LEM Manager, click 🕵️, and then select Connectors.

Use the Search box at the top of the Refine Results pane to locate the appropriate connectors.

d. Configure the syslog connector according to your needs.

e. On the LEM toolbar, navigate to Manage > Nodes.

f. Next to the Agent, click 🕵️.

g. Configure the Agent connector as required.
Alerts display but the rule does not fire

Problem statement: You see the alerts required to fire your rule in the LEM console, but your rule still doesn't fire.

To resolve this issue:

1. Verify that all your rules are activated in all open LEM consoles:
   a. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
   b. On the LEM toolbar, navigate to Build > Rules.
   c. Click Activate Rules.
      All rule changes you implemented in your LEM Manager are synchronized.
   d. Repeat these steps for all open LEM consoles in your environment.

2. Compare the InsertionTime and DetectionTime values in the alerts you expected to fire your rule.
   If the time is off by more than five minutes, verify and correct the time settings on your LEM VM or appliance, and any remote logging devices as necessary.

3. If your rules will not fire, restart the Manager service on your LEM VM/appliance.
   In general, consider doing this once every six months:
   a. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.
   b. At the cmc> prompt, enter manager and press Enter.
   c. At the cmc::manager> prompt, type restart and press Enter.
   d. To confirm your entry, press Enter.
      Restarting the LEM Manager service disconnects the Manager for a few seconds. No data is lost during this process.
   e. To leave the CMC interface, enter exit, and then press enter twice.

The rule fires but the email is blank

Problem statement: You receive an email notification for the alert, but the fields in the custom email template are blank.

To resolve this issue:

1. Open the LEM console. See Log in to the LEM web console or Log in to the LEM desktop console for steps.
2. On the LEM toolbar, navigate to Build > Rules.
3. Locate your rule in the Rules grid.
4. Next to your targeted rule, click 📬, and then select Edit. Notice that the files in the Action box are
5. Copy the event assigned to this rule.

   This is the string before the dot in the Correlation box.

6. Click Events, and then enter the event in the search field.

7. Drag the event fields required for your rule into the Actions box.

8. To close the Rule Creation window, click Save.

9. Click Activate Rules.

View and modify the time on your LEM appliance

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.

2. At the cmc> prompt, enter appliance.

3. At the cmc::appliance> prompt, enter dateconfig.

4. Press Enter through all the prompts to view the current date and time settings on your LEM appliance.

   By default, LEM receives a time synchronization from the VM host computer. Without the synchronization, the LEM time is not correct and the rules may not trigger when required.

5. Disable the time sync on the VM host computer and enable LEM to receive time information from an NTP server.

   a. At the cmc::appliance> prompt, enter ntpconfig and press Enter.

   b. Press Enter to start the configuration script.

   c. Enter the IP addresses of your NTP servers separated by spaces.

   d. Enter y and press Enter to verify your entry.

6. To leave the CMC interface, enter exit, and then press Enter twice.

The rule is not triggered when it should be

Check your rule logic and timestamps. The LEM VM host layer may need to be configured for NTP. By default, rules will not fire when incoming data drifts more than five minutes from the LEM VM clock.

1. Open the CMC command line. See Log in to the LEM CMC command line interface for steps.

2. To enter the appliance menu, type appliance.

3. Enter the dateconfig command, and confirm the date and time. You can change the time with this command, but when the vSphere/Hyper-V time sync pushes the time to LEM, this will change.
## Troubleshoot the LEM reports application

This section provides information to help you troubleshoot LEM reports.

### Troubleshoot the LEM reports application database connection

Use the following table to troubleshoot error messages that may occur with the ping test used to test the connection between the LEM reports application and the data warehouse or the primary data source.

<table>
<thead>
<tr>
<th>PROBLEM OR ERROR MESSAGE</th>
<th>DESCRIPTION</th>
<th>CORRECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager ping timed out.</td>
<td>The reports application was unable to connect to the LEM Manager host name or IP address. Confirm the host name (or IP address) you entered is correct.</td>
<td>Confirm that you entered the warehouse host name properly and it matches a valid DNS entry. Try entering the warehouse IP address in the Host Name field.</td>
</tr>
<tr>
<td>Sending the authentication packet failed. Could not flush socket buffer.</td>
<td>Reports could resolve and connect to the IP address, but could not authenticate to the database server at that location.</td>
<td>Confirm that the host name (or IP address) is correct and allows connections from the location where you are running the reports application. This error may also require you to modify the report restrictions.</td>
</tr>
<tr>
<td>Server ping test successful, but database connection test failed. Login incorrect. Login failed for user [user name].</td>
<td>Reports could resolve, connect to the IP address, and connect to SQL Server, but could not log in using the reports user credentials.</td>
<td>Confirm that the host name (or IP address) you specified contains the SolarWinds database. The warehouse may require a password for reporting purposes. In this case, click Security and enter the warehouse reporting password.</td>
</tr>
<tr>
<td>Logon failed. Database Vendor Code 210</td>
<td>The system running the LEM reports application is not on the list of authorized reporting computers.</td>
<td>To resolve this issue, add the system running the reports application to the list of authorized reporting computers. To allow specific systems to run the LEM reports application, or to remove all reporting restrictions, see <a href="#">Restrict access to the LEM reports application</a>.</td>
</tr>
</tbody>
</table>
Repair the LEM reports application

If you cannot open the LEM reports application or run reports, complete the following steps.

1. Uninstall the LEM Reports and Crystal Reports v11 Runtime.
2. Log in as an administrator and reinstall both components.
3. On older systems running Windows 7 and Windows Server 2008, adjust the LEM Reports properties to run the program in Windows XP compatibility mode:
   a. Right-click the LEM Reports shortcut on your desktop or in the SolarWinds Log and Event Manager program group in your Windows Start menu and select Properties.
   b. Click the Compatibility tab.
   c. Select Run this program in compatibility mode for, and then select Windows XP (Service Pack 3).
   d. Select Run this program as an administrator.
   e. Click OK.
4. Launch LEM Reports.
Glossary of LEM terms

Active response – An action that you or a LEM rule can take in response to suspicious activity or an attack. Active response actions include the Block IP active response, the Disable Networking active response, the Log off User active response, the Kill Process active response, the Detach USB Device active response, and so on.

Actor – A connector sub-type that can perform an active response. The actor connector allows the Agent to receive instructions from the LEM Manager and perform active responses locally on the Agent computer, for example, sending pop-up messages or detaching USB devices. In the LEM console, an orange connector icon represents an actor connector. Also see sensor.

Agent – In LEM, a software application that collects and normalizes log data before it is sent to the LEM Manager. The Agent runs as a standalone service and provides additional event alerting on workstations and servers. An Agent is required for some active responses, including logging off a user, shutting down a computer, and detaching a USB device. LEM Agents use Secure Socket Layer/Transport Layer Security (SSL/TLS) to securely transmit log data. Also see connector.

Agent node – In LEM, a single Agent, syslog, or SMTP instance that sends events to LEM. For example, an environment with 10 routers, 50 switches, 5 firewalls, 300 servers, and 500 workstations has 865 nodes sending data to LEM Manager.

Alert – See event.

Appliance – Originally, LEM was sold as a physical appliance that you deployed on your network. Today, LEM is the virtual image of a Linux-based appliance.

CMC – A command-line interface you can use to interact with the LEM Manager VM to perform routine administrative tasks without root access.

Connector – In LEM, a connector is a stand-alone file that allows LEM to monitor and interact with third-party vendor products, for example a firewall, an anti-virus application, a router, and so on. Each connector is named after the specific product that it is designed to support. Connectors can reside either on a LEM Agent, or on the LEM VM. Connectors installed on an Agent monitor local log files, but they can also monitor events sent from remote devices that cannot run an Agent. Connectors can intercept syslog events sent by third-party network devices and translate them into normalized events. Whereas LEM Agents actively send normalized log events to the LEM Manager, connectors rely on the host system to send syslog events to the LEM Manager. Connectors have two subtypes: sensors and actors. A sensor retrieves data from the product that the connector supports, whereas an actor carries out active responses.

Console – See desktop console or web console.

Correlation – See event correlation.

Desktop console – The optional LEM desktop console lets you manage and monitor LEM without a web browser. The desktop console provides the same functionality as the LEM web console, but as a Windows-only native app.
Directory service group – In LEM, directory service groups are Windows users and computer accounts that LEM pulls from Active Directory. You can associate directory service groups with rules and filters. Use directory service groups if Active Directory is available so that you do not have to manually update lists of user and computer accounts in user-defined groups.

Event – Any alert or notification written to a log that is monitored by LEM. In LEM, the terms event and alert are interchangeable.

Event correlation – The process of extracting useful and/or significant information from the large number of events flowing into LEM. Event correlation works by looking for and analyzing relationships between different event sources.

Event distribution policy – LEM’s event distribution policy controls how events are routed through the system. By configuring the event distribution policy, you can disable (or exclude) specific event types at the event level from being sent to the LEM console and/or the LEM database. Use the event distribution policy to prevent events of little or no value from being processed by the console or stored in the database.

Event group – A group type used to organize events for use with rules and filters. If you use an event group in a rule, LEM fires the rule when any event in the group triggers an alert.

Event response – See active response.

Facility code – A numeric code specified by the syslog protocol to identify the type of program that is logging the message. Sixteen facility codes, ranging from 0 (kernel messages) to 15 (clock daemon), are reserved for known program types, whereas facility codes 16 through 23 are reserved for local use (local use 0 up to local use 7). In LEM, facility codes are used to route vendor-specific events to designated log files.

Filters – Filters capture events and alerts that take place on your network. Filter conditions can be broad or specific. For example, you can create a filter without conditions that captures all events, regardless of the source or event type, or you can create a filter that has one specific condition, such as UserLogon Exists, which only captures user logon events. LEM ships with filters that support best practices in the security industry. You can modify these filters to meet your needs.

Filter groups – Also called filter categories. Filter categories are used to organize filters in LEM. LEM installs with seven default categories in the Filters pane: Overview, Security, IT Operations, Change Management, Authentication, Endpoint Monitoring, and Compliance. Administrators can remove or rename these categories, or add new categories as needed.

File Integrity Monitoring – Also called FIM. A LEM feature that monitors system and user file activity to protect sensitive information from theft, loss, and malware. FIM detects changes to critical files and registry keys to ensure that they are not accessed or modified by unauthorized users. FIM ensures systems comply with regulatory regulations, including Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Sarbanes-Oxley. FIM is enabled either by adding a FIM connector to a node, or by adding FIM to an existing connector profile.

Flat file log – Any log output to one or more ASCII-based text files. Systems that write to flat file logs include Linux system logs, web server logs, DNS server logs, custom application logs, and others.
Groups – In LEM, groups organize related elements into logical units so that they can be used in rules and filters. Various group types are used to group events, data elements (such as IP addresses, user names, web site URLs, and so on), Active Directory users and computers, email templates, Agents and connectors, and time-of-day sets.

Hypervisor – Computer software that runs virtual machines. The LEM VM can be installed on two hypervisors: Microsoft Hyper-V Server, and VMware vSphere ESX 4.0 or ESXi 4.0 and later.

LEM console – See desktop console or web console.

LEM Events Console - An HTML5 console that provides instant access to live event monitoring and filtering as well as historical record archives for in-depth analysis and troubleshooting.

LEM Manager – The LEM component that collects and processes log messages sent by one or more network systems. The LEM Manager consists of a syslog server, an optimized database, a web server, a correlation engine, and a hardened Linux operating system. LEM Manager is deployed as a single VM to a hypervisor (either Hyper-V or vSphere) running on Windows Server.

Local Agent Installer – A standalone installer that you or another administrator runs on a local host system to install the LEM Agent. The Local Agent Installer can be used for attended or unattended LEM Agent installations. Also see Remote Agent Installer.

Manager – See LEM Manager.

NCR – An initialism for New Connector Request. An NCR is a request for SolarWinds to create a connector for a system or application that does not have one.

NCD – An initialism for New Connector Data. An NCD is a request for SolarWinds to update an existing connector to receive data that is either being missed or is coming in as unmatched.

nDepth log retention – The nDepth log retention component in LEM is a separate data store to which you can send raw (unnormalized) log messages. The nDepth database is an optional component that is disabled by default. To save raw log messages, you need to enable it. Note that, other than the name, the nDepth log retention component is unrelated to the nDepth search engine.

nDepth search engine – The nDepth search engine can locate any event data, or any original log message that passes through a particular LEM Manager instance. The log data is stored in real time as it occurs from each host (network device) and source (application or tool) that is monitored by the LEM Manager. You can use nDepth to conduct custom searches, investigate your search results with graphical tools, investigate event data in other LEM explorer utilities, and take action on your findings.

Node – An Agent instance monitored by LEM. In the LEM console, navigate to Manage > Nodes to display the Agents monitored by each of your LEM Managers.

Normalization – The process by which LEM translates raw log data into a standard format prior to storing the message in the database. The LEM Manager component and the LEM Agent component are both capable of normalizing raw event messages received from devices on a network. If the nDepth log retention feature is enabled, LEM also saves raw (unnormalized) log messages in a separate nDepth data store.

Ops Center – See Ops Center view.

Ops Center view – In the web console, the user interface view that provides a dashboard made up of multiple widgets to help identify trends and problem areas in the network. Administrators can customize the dashboard by adding, editing, and removing widgets.
Remote Agent Installer – A standalone installer that pushes LEM Agents to Microsoft Windows hosts across your network without the need to step through an installation wizard. The installer unzips the installation files to a temporary folder of your choice, searches for Windows systems across the network, and installs the LEM Agent one at a time to the targeted systems. Also see Local Agent Installer.

Reports application – An optional LEM component that can schedule and execute over 300 audit-proven reports. Install the reports application on either a workstation or a separate networked server. The LEM reports application requires the free Crystal Reports runtime application.

Roles – LEM uses roles to restrict user access to sensitive data. Each LEM user account must be assigned to one of six LEM role types: Administrator, Auditor, Monitor, Contact, Guest, and Reports.

Rules – Rules monitor event traffic and automatically respond to events in real time. When an event (or a series of events) meets a rule condition, the rule prompts the LEM Manager to carry out a response action. A response action can be discreet, such as sending notifications to the appropriate users by email; or it can be active, for example blocking an IP address or stopping a process.

Sensor – A connector sub-type that cannot perform an active response. In the LEM console, a blue connector icon represents a sensor connector. See also actor.

Severity – In the syslog protocol, severity is a numeric code used to specify the urgency of the notification. Severity ranges from 0 (emergency: system is unusable) to 7 (debug: debug-level messages).

SIEM – A category of software products and services that monitor and analyze security events generated by applications and hardware devices on a network and send notifications when a set threshold is reached. Template Product Name (LEM) is a fully-featured SIEM solution. SIEM is an initialism for security information and event management.

Single sign-on – LEM supports Active Directory single sign-on (SSO). When enabled, LEM does not request a user name and password if the user is already logged in to Active Directory (AD). Instead, AD authenticates the user in the background, and automatically logs the user in to LEM with the appropriate user access rights.

SNMP, SNMP monitoring – Simple Network Management Protocol is used to collect information from network devices. LEM can receive SNMP traps from SolarWinds solutions to correlate performance alerts with LEM events. LEM can also send SNMP traps to SolarWinds solutions to enable NPM to monitor CPU, memory, and other critical LEM components. Versions of LEM older than 6.3.0 do not support sending health or status updates to other devices over SNMP. LEM versions older than 6.3.0 can only send SNMP traps to devices when rules fire.

SSO – See single sign-on.

Syslog – A message logging protocol used by a wide range of devices, including most network devices, such as routers, switches, and firewalls. Devices send event notification messages to a central logging server (a syslog server) that consolidates logs from multiple sources. Syslog messages have a numeric facility code that LEM uses to route messages to a log. to specify the type of program that is logging the message, and a numeric severity level to specify the urgency of the notification.

Syslog server – A software application (such as Kiwi Syslog Server) that collects syslog messages and SNMP traps from network devices (such as routers, switches, and firewalls).
USB defender – A free add-on for all LEM Agents installed on Windows computers. USB defender tracks events related to USB mass storage devices like flash drives and smart phones, and allows the LEM Manager to send commands to detach offending devices both manually and automatically.

User-defined group – User-defined groups are groups of data elements that can be used in rules and filters to match, include, or exclude events, information, and data fields. Data elements can be IP addresses, user names, email addresses, web site URLs, and so on.

Virtual appliance – A type of virtual machine that hosts a single application on a hypervisor. To keep things simple, the LEM documentation refers to the LEM virtual appliance as the LEM virtual machine (or the LEM VM). The LEM virtual appliance runs on a hardened, Linux-based software stack that includes a database, a web server, a correlation engine, a syslog server and a SNMP trap receiver.

vSphere – A hypervisor distributed by VMware. The LEM virtual machine can be deployed on vSphere.

Web console – The primary LEM user interface that runs in a web browser. Use the web console to manage and monitor the LEM application. The web console has five views: Ops Center (provides a dashboard made up of widgets that display a graphical representation of your log data), Monitor (displays events in real time as they occur on your network), Explore (provides tools for investigating events and related details), Build (creates user components that process data in LEM Manager), and Manage (manages properties for appliances and nodes). See also: desktop console.

Widget – A user interface component that provides special dashboard functionality, such as displaying real-time information about network activity, or providing tools for investigating events and related details. In the LEM console, widgets are displayed in OpsCenter view, Monitor view, and nDepth view. Use Widget Manager to select and add a widget to the dashboard. Use Widget Builder to create a new widget or edit an existing widget. Master widgets are widget templates located in the Widget Manager categories list (in Ops Manager view), in the Widgets pane based on the filter you select as a data source (in Monitor view), or in the nDepth toolbar (in nDepth view). Copy a master widget to the OpsCenter dashboard or to Monitor view to create a dashboard widget.