Table of Contents

How do I get started with SolarWinds UDT? ................................................................. 4
Log in using the Orion Web Console ........................................................................... 6
Discover your network ................................................................................................. 7
Select Orion Nodes for monitoring with UDT .............................................................. 12
Select an Active Directory Domain Controller to track user logins ......................... 14
The Device Tracker Summary dashboard .................................................................... 15
Rogue devices and setting up a White List of allowed devices ..................................... 16
  What to do about rogue devices .................................................................................. 17
The Watch List ............................................................................................................ 20
  Manually adding a device to the Watch List ................................................................. 20
  The Device Watch List widget ...................................................................................... 21
Locate network devices ............................................................................................... 23
UDT Alerts .................................................................................................................... 25
Configure a UDT alert .................................................................................................. 26
UDT reports .................................................................................................................. 29
What next? ..................................................................................................................... 30
How do I get started with SolarWinds UDT?

Welcome to the User Device Tracker (UDT) Getting Started Guide.

UDT delivers automated endpoint tracking to help you quickly locate users or devices, as well as alert you when rogue devices enter the network. It also provides valuable switch port management capabilities to help you identify available ports, capacity plan your network, and manage port access.

For a video overview of using UDT to find devices and manage port use, click here.

To learn how to use UDT, we recommend that you complete the following tasks:

- **Install UDT**
  
  To install the User Device Tracker (UDT), see the SolarWinds Orion Installer.

- **Discover your network**
  
  Once UDT is installed, use the Network Sonar Wizard to discover the devices on your environment.

  If you are already monitoring your network with SolarWinds NPM or other Orion Platform products, you can skip this and go to the next step.

- **Select the Orion nodes to monitor with UDT**
  
  Now that you have a database of all the devices currently in your environment, select those you want to monitor with UDT.

- **Select an Active Directory Domain Controllers to track user logins**
  
  If you want to use UDT to track user logins, you will need to add an Active Directory Domain Controller.

- **Rogue Devices and setting up a list of allowed devices**
  
  Set up a white list of devices you regard as safe and not to be monitored. Devices detected on your network that do not appear on the white list are displayed on the Rogue Devices list. Devices stay on the Rogue Devices list until they are marked as safe or moved to the watch list.

- **Set up a watch list**
  
  Manually enter any devices you want to put on the Watch List.

- **Examine the Device Tracker Summary page**
  
  As soon as UDT begins to monitor your devices, the widgets on the Device Tracker Summary dashboard will begin to show data.
- **Locate network devices**
  Search for devices by user name, hostname, IP Address or Mac Address, node name, node port, or vendor using UDT's search tool.

- **Set up alerts**
  Create alerts to notify you by email when specific devices are detected on your network.

- **View reports**
  View reports showing historical data as it accumulates.

**Existing customers:** Access your licensed software from the [SolarWinds Customer Portal](https://www.solarwinds.com). If you need any implementation help, contact our [Support Reps](mailto:support@solarwinds.com).

**Evaluators:** Download your free 14-day evaluation from [www.solarwinds.com](https://www.solarwinds.com). If you need assistance with your evaluation, contact [sales@solarwinds.com](mailto:sales@solarwinds.com).
Log in using the Orion Web Console

1. Launch the Orion Web Console using either of the following methods:
   - Start the Orion Web Console from the SolarWinds Orion program folder.
   - Launch a browser and enter:
     
     http://ip_address
     
     or:
     
     http://hostname

     where ip_address is the IP address of your SolarWinds Orion server, and hostname is the domain name of your SolarWinds Orion server.

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

3. If this is your first time using the User Device Tracker, the Welcome to Orion Web Console page is displayed. Click Start to begin discovering your network.

4. After you have discovered your network and imported discovered devices into UDT, the Orion Summary Home dashboard is displayed. Click My Dashboard > Device Tracker > Device Tracker Summary to view the UDT dashboard.
Discover your network

SolarWinds User Device Tracker (UDT) is designed to be used as part of the SolarWinds Orion Platform suite of products or as a standalone application. If you are already using the Orion platform to monitor your environment, and have created a database of nodes and associated elements, you can skip this section and start adding nodes for UDT monitoring.

Discovery is the term used to describe the process SolarWinds Orion uses to identify network elements.

The tabs shown as you proceed through wizard depend on the SolarWinds Orion products you have installed. Click Next to skip a tab.

Before you discover your network:

- Determine which type of devices you want to monitor and which you want to ignore
- Enable the networking devices you want to monitor using SNMP
- Enable Windows devices for WMI

1. If the Discovery Wizard page is not displayed when you launch UDT, click Settings > Network Discovery.

   If you have already set up a discovery, you can add another by clicking Add New Discovery.

2. Click Start if necessary to display the following page:

   ![Network Sonar Wizard](image)

   3. If this is your first discovery, and you want to start seeing real data as soon as possible, just add a limited range of IP addresses by adding a start and end address.

   As you scale your implementation, you can also use the following scanning options:
## Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Ranges</td>
<td>Use this option to scan one or more IP ranges. If you have many IP ranges to scan, consider adding multiple discovery jobs rather than including all ranges in a single job.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Use this option to scan every IP address in a subnet. SolarWinds recommends scanning at most a /23 subnet (that is, a maximum of 512 addresses). Scanning a subnet returns everything that responds to ping, so we recommend only scanning subnets where you want to monitor the majority of devices.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>Use this option for a limited number of IP addresses that do not fall in a range.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Use this option to scan an Active Directory Domain Controller. You can add an Active Directory Domain Controller, as described later in this guide, for tracking user logins.</td>
</tr>
</tbody>
</table>

4. Click Next until the SNMP tab is displayed.

5. On the SNMP tab:
   - If all devices on your network require only the default SNMPv1 and SNMPv2 public and private community strings, click Next.
   - If any device on your network uses a community string other than public or private, or if you want to use an SNMP v3 credential, click Add Credential and provide the required information.

   If you use SNMPv3, you need to grant access to all Bridge MIBs. For more information, see the knowledgebase article, Enable SNMPv3 access for layer 2/3 Bridge MIBs for Cisco IOS.

6. On the Windows tab, click Add New Credential and provide the required information, if you want to discover WMI or RPC-enabled Windows devices.

7. On the Monitoring Settings tab, select Manually set up monitoring after devices are discovered, if this is the first time you have run discovery. This will give the opportunity to review the list of discovered objects, and decide which to monitor and which you are not interested in.

8. On the Discovery Settings tab, enter a name for this network discovery, and click Next.

9. On the Discovery Scheduling tab, accept the default frequency, and click Discover to run the discovery immediately.

   Discovery can take anywhere from a few minutes to a few hours, depending on the number of network elements the system discovers.

   After searching your network, the Network Sonar Results Wizard displays how many of each device type has been detected.
When you manually run discovery, the system automatically selects **all** network elements to be monitored. You must clear the check boxes for those elements you do not want to be monitored.

Discovered elements do not count against your license count; only elements that you import into the Orion database count against your license.

10. Ensure only the device types you want to monitor are selected, and click Next.
11. On the Ports tab, specify the ports you want to monitor.

By default only ports with the UP status are selected.
12. Expand the nodes to verify your selection.

![List of Ports](image)

13. Click next until the Import Preview tab is displayed, and click Import.

![Network Sonar Results Wizard](image)

14. When the import is complete, go to My Dashboards > Home > Summary.
   - The nodes you selected are displayed in the All Nodes widget.
   - The Event Summary widget shows these nodes were added.

You can now [add these nodes to UDT for monitoring](#).
Select Orion Nodes for monitoring with UDT

Whether you are already monitoring nodes with the Orion platform or have just run a discovery job to find nodes specifically for UDT, you now need to select the nodes you want to monitor.

1. Click Settings > All Settings > UDT Settings.
2. Select Manage Ports.
3. From the Show dropdown, select Nodes.
4. From the Filter to dropdown, select UDT Unmonitored Nodes.
5. Select the nodes you want to monitor, and click Monitor Node with UDT.

To immediately start monitoring all ports, select UDT Monitored Nodes from the Filter to dropdown. Then select all ports, and Click Poll now.

6. Navigate to My Dashboards > Device Tracker > Device Tracker Summary. Within a few minutes the All UDT Nodes widget should start showing ports, as shown below.
Hover over a port to display a summary.

Click on a port to display its details page.
Select an Active Directory Domain Controller to track user logins

SolarWinds UDT lets you track Active Directory user who log in to your network, in addition to tracking devices. To do this, you must select an active directory domain controller to use with UDT.

1. Go to Settings > All Settings > UDT Settings.
2. Click Discover Active Directory Domain Controller.
3. Click Add Administrator Credential.
4. Select an existing credential, or create a new credential by entering a name for the credential, and the user name and password.
5. Click Test, and if the credential is valid, click Assign.
   The credential is added to the credential list.
6. Click Next to continue.
7. A list of available Active Directory Domain Controllers is displayed.
8. Select the Active Directory Domain Controller(s) you want to use to monitor user log ins, and click Import.
9. When the View Results tab is displayed, click OK, I'm Done.
    The All User Log Ins widget displays details of users currently logged in (including the credential just used to add the Active Directory Domain Controller).

<table>
<thead>
<tr>
<th>USER NAME</th>
<th>MOST RECENT LOG IN TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>lab.exc10\labuser</td>
<td>1/22/2018 11:01:44 AM</td>
</tr>
</tbody>
</table>

As time passes, this widget will show all users that have logged in after the controller was added. You can then use the search box to find a user you are interested in, and drill down to the user details page.
The Device Tracker Summary dashboard

Once you have imported the devices you want to monitored, and they have been polled, you can see the results on the Device Tracker Summary dashboard.


By default the summary dashboard displays the following widgets.

<table>
<thead>
<tr>
<th>Widget Title</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>All UDT Nodes</td>
<td>The list of all monitored nodes, initially grouped by vendor and status, showing status icon and node name for each. Expand a node to display the name and status of the ports on that node.</td>
</tr>
<tr>
<td></td>
<td>- Move the cursor over a node or port to display current information</td>
</tr>
<tr>
<td></td>
<td>- Click on a node or port to open the node or port details page</td>
</tr>
<tr>
<td>Total Ports Currently Used</td>
<td>A pie chart with the total number and percentage of used and free ports.</td>
</tr>
<tr>
<td>All User Log Ins</td>
<td>If you have added an Active Directory Domain Controller to UDT, this widget displays a list of users logged into the monitored network. Logins are listed from most to least recent.</td>
</tr>
<tr>
<td>Active Alerts</td>
<td>This shows any active alerts associated with UDT devices and ports.</td>
</tr>
<tr>
<td>Rogue Devices</td>
<td>The list of devices that are not on the White List of devices considered safe for your network.</td>
</tr>
<tr>
<td>Top 10 Nodes by Percent Ports Use</td>
<td>The ten nodes with the highest percent of ports used.</td>
</tr>
<tr>
<td></td>
<td>- Move the cursor over a node to display current information</td>
</tr>
<tr>
<td></td>
<td>- Click on a node to open the node or details page</td>
</tr>
<tr>
<td>Top 10 Access Points by Current # of Endpoints</td>
<td>The 10 wireless access points with the most current endpoint connections.</td>
</tr>
<tr>
<td></td>
<td>- Move the cursor over an access point to display current information</td>
</tr>
<tr>
<td></td>
<td>- Click on an access point to open the access point details page</td>
</tr>
<tr>
<td>Top 10 SSIDs by Current # of Endpoints</td>
<td>The 10 Service Set Identifiers (SSIDs) with the most current endpoint connections.</td>
</tr>
<tr>
<td></td>
<td>- Move the cursor over an SSID to display current information</td>
</tr>
<tr>
<td></td>
<td>- Click on an SSID to open the node or details page</td>
</tr>
<tr>
<td>Device Watch List</td>
<td>The items that have been added to the Device Watch List.</td>
</tr>
<tr>
<td>Ethernet Ports Used Over Time</td>
<td>A chart showing the percentage of Ethernet ports used.</td>
</tr>
<tr>
<td>Last 25 Events</td>
<td>A list of the last 25 events associated with UDT.</td>
</tr>
</tbody>
</table>
Rogue devices and setting up a White List of allowed devices

You could monitor every device on your network, but in most cases this is not necessary. There are usually devices that are never moved, and can be regarded as safe. UDT lets you create a list of these devices, referred to as the White List. Any device that connects to your network that is not on this list will appear in the Rogue Device widget, and will trigger the appropriate alert.

To set up the white list, add rules that identify the devices to be included. You can identify individual devices by hostname, IP address, or MAC address. You can identify groups of devices using subnets, address ranges, or pattern matching.

By default, UDT is set up with three rules that add all devices to the White List, meaning that there are no rogue devices.

If a White List has not been set up and the three default rules are in place, the Rogue Devices widget looks like this:

The three default rules are:

- Any hostname is safe
- Any IP address is safe
- Any MAC address is safe

**IP addresses or MAC addresses?**

A MAC (Machine Access Control) address is given to a network adapter when it is manufactured; it is unique, and cannot be altered.

An IP (Internet Protocol) addresses not usually assigned to a computer, or other device, until it is added to a network. If it is taken away from the network, and then returned, it will receive whatever IP address is available, unless an IP address is reserved. This can be done using SolarWinds Orion IP Address Manager.
These rules use pattern matching. The pattern used for each is the wildcard character, *, which means any hostname, IP or MAC address encountered is added to the White List.

To set up your own White List:

1. Go to the My Dashboard > Device Tracker > Device Tracker Summary dashboard.
2. On the Rogue Devices widget, click Create White List.
3. Choose the selection method for your first rule. You can:
   - Select Device, and add individual Hostnames, IP Addresses or MAC Addresses.
   - Select IP Range, and add the start and end IP addresses of one or more ranges.
   - Select MAC range, and add the start and end MAC addresses of one or more ranges.
   - Select Subnets, and add the Subnet Address and Subnet Mask for each subnet.
   - Select Custom, and enter the required pattern or patterns, refering to the examples displayed.
4. Click Next.
   The devices that this rule regards as safe is listed.
5. Enter a name, and optional description for this rule, and click Next.
6. Click Add New to add another rule.
7. When you have set up your rules, delete or disable the three default rules.
8. Go to My Dashboards > Device Tracker > Device Tracker Summary. The Rogue Devices widget now shows any devices connected to the network that do not meet the rules you created.

For more on setting up your white list, see the Whitelisting FAQ.

What to do about rogue devices

When a device appears on the rogue device list, it is up to you to decide if it is legitimate or if it needs to be investigated.
In the first instance above, we see that a Windows device with a MAC address of 00:15:5D:43:06:42 has been added to the network.

The device name column may show the IP address, the MAC address or the DNS address.

**If you can tell from this information that it is safe to ignore the device:**

1. Click Safe device, add it to white list.
   
   The Add devices to the white list page is opened for this device.

2. Click Next. On this screen you can enter a name and an optional description for this device.

3. Click Finish.

**If you want more information before deciding:**

1. Click the device name.

   ![Device Tracker Endpoint Details](image)

   The Device Tracker Endpoint Details page is displayed. Here you can see network connection details, the Hostname, IP address, Mac Address, Vendor and other information for the endpoint.

2. To monitor this endpoint as a node, click Start monitoring as a node. This opens the Add Node page.

   For further information, see [Add a single node for monitoring](#).

**If you want to put this device on the watch list:**

1. Copy the MAC Address.

2. Go to the Device Tracker Summary dashboard.

3. Click Manage List on the Device Watch List widget.

4. Click Add Device/User.

5. Paste or enter the MAC address into the MAC Address field, enter a name and description for this device, and click OK.

**If you want further information on the port to which the device is connected:**
1. On the Endpoint Details page, click Node Port or SSID.
   The Port Details page is displayed showing port details and history.

2. If you have read/write credentials for the node on which this port is located, you can shut the port down by clicking Shutdown.
The Watch List

Whereas the White List contains devices that are permitted on your network and do not need to be monitored, the Watch List contains devices you want to investigate further.

The Watch List is mostly created as you decide which of the devices that appear on the Rogue Device list should be put on the white list and which should be watched.

2. On the Rogue Devices list click Watch this device next to the device you want to add to the watch list.
3. The Manage Watch List page is displayed. Click Next to add the device to the White List.
4. If you want to identify this device and add a description explaining why you added it to the White List, select the checkbox and click Edit.

Manually adding a device to the Watch List

If you know the MAC Address for a device you want to watch, you can manually add it to the watch list:

2. Click Manage List on the Device Watch List widget on the Device Tracker Summary page.
3. Click Add Device/User.
4. Enter the MAC Address.
5. Optionally, you can add a Name and Description for this device to remind you why it is being monitored.

The Device Watch List widget

The Device Watch List widget is displayed on the Device Tracker Summary dashboard, and shows the status and other information about all devices.

Further information about a watched device can be displayed by moving the cursor over the device status or Name.
Click on the device status or Name to show all Endpoint details page.
Locate network devices

One of the most powerful, but simple-to-use tools in UDT is Search. Use it to quickly locate devices and users logins on your network by name, address, or vendor.

You can use wildcards if you only have partial information or want to find a range of devices.

1. On any UDT page, go to the Search Device Tracker field in the upper right corner.
2. Click on the down arrow to open the search menu.
3. Select which identifier you want to use for your search.
4. If you use multiple identifiers, this will result in a slower search, possibly with many unwanted results.

Enter all or part of the identifier, using the wildcard (*), if required.

If you are searching on vendor, you do not need to use wildcards.

For example, if you are searching on IP Address, MAC address, hostname and Vendor:

10* will find:

- 10.1.0.100 (IP address)

*10 will find:

- 0.0.0.10 (IP address)
- 10.1.0.124 (IP address)
- 00:0C:30:10:BD:10 (MAC address)

*de* will find:

- 00:10:18:14:C7:DE (MAC address)
- lab-apm-demo (hostname)
- Brocade Communications (Vendor)
If more than one result is returned, they are listed on the Device Tracker Search Result. If only one result is returned, the details page is displayed.
UDT Alerts

When a rogue device or a device on the watch list is detected, UDT triggers an alert. Alerts are customizable and can generate a variety of actions, such as sending an email, executing an external page, or playing a sound.

UDT comes with several out-of-the-box alerts. These are enabled by default, so if rogue hostnames, IP or MAC addresses are detected, alerts are displayed in the All Active Alerts widget on the Orion Summary Home and the Active Alerts Device Tracker Dashboards.

The example below shows that a device using the rogue IP address of 10.199.xx.xxx triggered an alert 3 hours and 1 minute ago.

You can customize alerts by changing the action associated with it. These actions include:

- Send emails or messages
- Execute programs and scripts
- Create ServiceNow Incidents
- Log entries in logs or text files
- Create custom properties

You can customize emails to contain information about the condition that triggered the alert, or select who receives the email depending on time or date.

Alerts can be escalated if not responded to within a set period.

To see more information about an alert, click on the alert name. This opens the Active Alert Details page, where you can:

- View more information on the alert
- Acknowledge the alert
- Edit or turn off the alert

For complete information on creating alerts, and customizing actions for your specific environment, see Use alerts to monitor your environment in the Orion Platform Administrator Guide.
Configure a UDT alert

The preconfigured UDT alerts cover all rogue IP addresses, all rogue MAC address, and all rogue hostnames. To create alerts for specific ranges of rogue addresses that trigger different actions, you can customize these or you can create new alerts.

This example shows you how to duplicate a preconfigured alert, and configure it to be triggered if the IP address of the rogue device is in a specific range.

1. Go to Alerts & Activity > Alerts and click Manage Alerts in the upper-right corner.
2. On the Manage Alerts page:

   1. Select Object Type from the Group By drop-down.
   2. Select Rogue IP Address.
   3. Check the Alert me when a rogue IP address appears on network alert.
   4. Click Duplicate and Edit.

3. On the Properties tab, edit the alert name and description, and click Next.

   The trigger condition tab is displayed.

   This shows the condition that triggers the alert. In this case, it is triggered whenever the Rogue field is equal to Yes. To change this so that it is only triggered if the IP address is in a specified range, we need to add the lower and upper limits of that range.
4. On the Trigger Condition tab:

   ![Trigger Condition Table]

1. Click the plus icon and select Add Single Value Comparison.
2. Select IP Address from the second drop-down.
3. Select Is greater or equal to than from the third drop-down.
4. Select the first IP address in the required range.

5. Repeat these actions, but select Is less than or equal to and the last IP address in the required range.


7. Select Send an Email/Page, and click Configure Action.

8. Enter a name for the action, and enter the recipients for this email alert.
10. Complete the other configuration sections, and click Next.

   For more information on setting up email alerts, see Send an email or page in the Orion Platform Administrator Guide.

11. On the Summary tab, review the settings for this alert.

12. Review the message above the Submit button.

   The message shows how many objects trigger this alert. In this case three devices have been detected using IP addresses in the specified range. When you click Submit, the specified recipient receives an email for each address.
UDT reports

Out-of-the-box, there are eleven UDT-specific reports available. These will start to show data and be ready to print as soon as devices start being monitored.

To view or print a UDT report:

1. Go to Reports > All Reports.
2. Select Product from the Group By drop-down.
3. Select UDT reports from the list.
4. Click on the required report.
5. Click Printable version if required.

For information on scheduling reports, see Schedule reports from the Schedule Manager in the Orion Platform Administrator Guide.

You can change both the layout and the content of UDT reports. See Manage reports in the Orion Web Console in the Orion Platform Administrator Guide for more information.
What next?

This Getting Started Guide is intended to get you up and running with UDT, and to start seeing real results almost immediately. The next step is to scale up your UDT monitoring to cover your whole environment, fine tune your whitelist, and set up the alerts and reports for your specific needs. To aid you on your journey, SolarWinds provides:

- Online help
- Administrator Guide
- Knowledge Base
- The THWACK community