User Device Tracker

Version 3.4
© 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

**Get Started with SolarWinds UDT** ................................................................. 5

- Introduction to UDT .......................................................................................... 6
- What SolarWinds User Device Tracker offers .................................................. 6
- What is a device? ............................................................................................... 6
- How does SolarWinds User Device Tracker work? ........................................... 7
- SNMP requirements for monitored devices ...................................................... 8

**Administer SolarWinds UDT** ........................................................................... 9

- Log into the web console .................................................................................... 9
- Discover and add network devices to UDT ....................................................... 11
- Advanced automatic import options .................................................................. 11
- Add Orion nodes to UDT .................................................................................... 12
  - Has a node been added to UDT? ..................................................................... 13
- Add Active Directory Controllers and users ...................................................... 14
  - Manage Active Directory domain controllers .............................................. 14
    - Add an Active Directory Domain Controller ......................................... 14
    - Edit an Active Directory domain controller ....................................... 15
    - Assign a credential to an Active Directory domain controller .......... 16
    - Delete an Active Directory Domain Controller .................................. 16
  - Manage Active Directory credentials .......................................................... 16
    - Add, edit or delete an Active Directory credential ...................................... 17
    - Domain controller configuration validation ............................................. 17
  - Set up polling of user data across domains ................................................. 18
    - Define credentials for polling across domains .................................... 18
- Rogue Devices, the White List, and the Watch List ........................................... 19
  - Manage the White List .................................................................................... 20
  - Ignoring devices .............................................................................................. 20
  - Add endpoints to the White List .................................................................... 20
Manage Watch List ........................................................................................................... 22
UDT Settings ................................................................................................................... 22
Port Management ........................................................................................................... 23
    Unmonitored nodes ................................................................................................... 23
    Monitored nodes ....................................................................................................... 24
    Ports ............................................................................................................................. 24
Manage Watch List ......................................................................................................... 24
Manage the White List ..................................................................................................... 25
    Ignoring devices ......................................................................................................... 25
Polling Interval ............................................................................................................... 26
    Polling Timeout Warning .......................................................................................... 26
Device Tracker Thresholds ............................................................................................... 26
Data Retention .................................................................................................................. 27
View UDT Job Status ...................................................................................................... 27
Advanced Configuration Settings for SolarWinds User Device Tracker ....................... 27

Solutions in SolarWinds UDT .......................................................................................... 29
Enable DNS resolution for wireless nodes ........................................................................ 30
Resolve IP address conflicts with IPAM and UDT integration ......................................... 30
Find the switch and port where a particular hostname, IP, or MAC address is or was connected ........................................................................................................... 33
Track status for a group of ports ...................................................................................... 34
Shut down a network device port ................................................................................... 35
Create and manage a watch list ...................................................................................... 36
Display rogue endpoint connections in real-time ......................................................... 36
Find wireless endpoint connections ............................................................................... 37
Find a user’s connections .............................................................................................. 38
Moving SolarWinds UDT to a new server ....................................................................... 38
Define credentials for polling across domains ............................................................. 39
Get Started with SolarWinds UDT

Welcome to the UDT Getting Started Guide. This guide will take you from installation to full implementation of UDT.

**Existing customers:** Access your licensed software from the [SolarWinds Customer Portal](#). If you need any implementation help, contact our [Support Geeks](#).

Read this [SolarWinds Customer Support](#) article to learn how to properly open a support case and get your case the right level of visibility.

**Evaluators:** Download your free 30-day evaluation [here](#). If you need assistance with your evaluation, contact [sales@solarwinds.com](mailto:sales@solarwinds.com).
Introduction to UDT

SolarWinds User Device Tracker (UDT) monitors the devices, ports, and users associated with your network. It lets you analyze port use and capacity, and be alerted to issues before or as soon as they occur, find where devices are connected in your network and get detailed information about capacity analysis.

UDT regularly polls switches and routers for information about what is connected to them. Based on this information, it creates a database of current and historical information about where a device has been connected.

UDT polls Active Directory domain controllers event logs for user login activity, and based on this provides current and historical views of endpoints to which users have been connected on the network.

| UDT cannot be used to monitor nodes that are monitored by the Orion Remote Collector. |

What SolarWinds User Device Tracker offers

SolarWinds UDT provides focused device and port monitoring for network engineers. SolarWinds UDT provides many features to help, including:

- Discover IPv4 and IPv6 devices
- Quickly find where a device or user is connected on the network
- Find out where a device or user has been connected in the past
- Find out what has been connected to a port over time
- Provides port capacity analysis for a switch (how many ports are being used, including both monitored and un-monitored ports)
- Provides global port capacity analysis for used/available ports and network capacity planning
- Configure a watchlist to track when specific devices appear on the network and alert when the devices appear
- Provides enhanced network topology mapping
- Generates predefined reports on connected devices, device capacity, and Active Directory users

What is a device?

A device is referenced by its MAC address, hostname, or IP Address. You can use SolarWinds UDT to search on this information to find where the device is currently connected to the network and where it has been connected in the past.
How does SolarWinds User Device Tracker work?

Using SNMP calls to your network framework, SolarWinds User Device Tracker uses SNMP calls to your network framework to provide real-time feedback on your monitored devices, users, and trends through statistics stored in the Orion Platform database. Keeping with the SolarWinds common components infrastructure, no agents are installed on your servers and there is no remote software to maintain. All calls are made in real time and displayed on a web console accessible from any supported browser.

The following diagram provides an overview of the current SolarWinds UDT architecture, including interactions among SolarWinds UDT components, the SolarWinds UDT database, Active Directory domain controllers, and the managed devices on your network.
SNMP requirements for monitored devices

SolarWinds UDT can monitor the performance of any SNMPv1, SNMPv2c, or SNMPv3 enabled device on your network. You may need to consult the device documentation or the device manufacturer for specific instructions when configuring SNMP.

- To properly monitor devices on your network, enable SNMP on all devices capable of SNMP communications.
- If SNMPv2c is enabled on a device you want to monitor, UDT will attempt to poll the device for performance information using SNMPv2c. If you only want to use SNMPv1, disable SNMPv2c on the device to be polled.
Administer SolarWinds UDT

This guide provides an overview of product features and related technologies for the SolarWinds Universal Device Tracker (UDT). In addition, it contains recommendations on best practices, tutorials for getting started, and troubleshooting information for common situations.

Browse through the links and information to learn about adding and monitoring storage devices, and much more.

Want more information?

- UDT Release Notes
- UDT Online Help
- All UDT Documentation

Log into the web console

If you added User Device Tracker (UDT) to an existing SolarWinds Orion platform installation, you will probably be familiar with the Web Console and will be able to immediately access UDT.

- Navigate to My Dashboards > Storage > Device Tracker Summary.

If you have installed UDT as a standalone product:

1. Launch the Web Console:
   - Click Start > All Programs > SolarWinds > Orion Web Console.
   
   or:

   - Open a web browser on your SolarWinds UDT server and enter http://ipAddress or http://hostname, where ipAddress is the IP address of your server and hostname is the host name of your server.
2. Enter a user name and password.

   The first time you log into UDT, and until you change the default Admin password, you can log in with the user name Admin and no password.

3. Click Login.

   The Orion Summary Home Dashboard is displayed.


   The User Device Tracker Summary is displayed.

The Web Console menus also provide access to the alerts, reports, and settings menus.
Discover and add network devices to UDT

When you have installed SolarWinds User Device Tracker (UDT), you need to identify the objects you want to monitor.

There are several ways to do this. If you have other SolarWinds Orion Platform products such as NPM installed and have already created a database of nodes for monitoring, you can go straight to Add Orion nodes to UDT.

If you have not yet created a database of network devices, see Discover your network with the Discovery wizard. You will then need to identify them for monitoring with UDT as described in Add Orion nodes to UDT.

Advanced automatic import options

As of UDT 3.4, you can automatically import UDT discovery results. When you select Import ports during Network discovery, you have the ability to adjust the automatic import of UDT discovery results with different filtering options, such as Port Status, Port Mode, or Hardware.

1. In the Orion Web Console, click Settings > Network Discovery.
2. Click Add New Discovery.
3. Proceed to the Monitoring Settings page.
4. Select Automatically monitor based on my defined monitoring settings > click Define Monitoring Settings.
5. Proceed to the Ports page.
6. Select Import ports.
   This option is disabled by default.
7. Select the individual check boxes under Status, Port Mode, Hardware according to your import preferences.
8. Optionally, set the Advanced filtering options.

![Choose What to Monitor](image)

9. Click Finish.

10. Proceed to the Discovery Scheduling page.

11. Select Frequency and select Yes, run the discovery now.

12. Click Discover.

   After the discovery finishes successfully, UDT ports are automatically imported and monitored according to your filters.

### Add Orion nodes to UDT

To select nodes that are currently in the Orion database so they can be monitored by UDT:

1. Go to Settings > All Settings.
2. Select UDT Settings in the Product Specific Settings section.
3. Select Manage Ports in the Port Management section.
4. Select Show Nodes, and Filter to: UDT Unmonitored Nodes.
5. Select the nodes to be monitored, and select Monitor Node with UDT.

![Port Management](image)

These ports will be imported to UDT in the next polling interval.

**Has a node been added to UDT?**

To check whether an Orion node has been successfully added to UDT, and to view all event notifications related to nodes importation, check the Last 25 Events widget on the Device Tracker Summary page.

<table>
<thead>
<tr>
<th>Notification</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports of the node [node name] have been imported. [Reason is stated if known].</td>
<td>Successful importation of a single node.</td>
</tr>
<tr>
<td>Ports of the node [node name] have not been imported. [Reason is stated if known].</td>
<td>Importation of a single node failed.</td>
</tr>
<tr>
<td>Some ports of node [node name] have been imported as unmonitored due to license limit.</td>
<td>Importation failed due to license limit of a single node.</td>
</tr>
<tr>
<td>Ports for [number of nodes] have been imported.</td>
<td>Successful importation of multiple nodes.</td>
</tr>
<tr>
<td>Ports for [number of nodes] have not been imported. [Reason is stated if known].</td>
<td>Failed general importation of multiple nodes.</td>
</tr>
<tr>
<td>Some ports for [number of nodes] have been imported as unmonitored due to license limit.</td>
<td>Importation due to license limit of a multiple nodes.</td>
</tr>
</tbody>
</table>

You can also see the complete list of monitored nodes as follows:

1. Go to Settings > All Settings.
2. Select UDT Settings in the Product Specific Settings section.
3. Select Manage Ports in the Port Management section.
4. Select Show Nodes and Filter to: UDT Monitored Nodes.
5. All monitored nodes are displayed. You can filter this list using the Group by dropdown, or use the Search box to find a specific node.
Add Active Directory Controllers and users

UDT can track user activity by reading the Active Directory domain controller event log.

Before you can add an Active Directory domain controller and begin tracking the user accounts associated with it, you must first create credentials for UDT to interact with it. UDT requires Event Log Reader permission on each Active Directory controller.

The following topics describe the process of adding an Active Directory domain controller to UDT, and using it to track the activity of Active Domain associated users on your network.

- **Manage an Active Directory Domain Controller**
- **Set Up Polling of User Data Across Domains**
- **Define Credentials for Polling Across Domains**
- **Manage Active Directory Credentials**

Manage Active Directory domain controllers

An Active Directory Domain Controller is a server running Windows Server with Active Directory domain services installed. Active Directory domain controllers are used in UDT to retrieve information about user activity on network devices.

The Manage Active Directory domain controllers page displays the Active Directory domain controllers currently set up for UDT, and enables you to do the following:

- **Add an Active Directory Domain Controller**
- **Edit an Active Directory domain controller**
- **Assign a credential to an Active Directory domain controller**
- **Delete an Active Directory Domain Controller**

Add an Active Directory Domain Controller

Add Active Directory Domain Controllers to your network to track Active Directory users when they log into your network.

1. Go to Settings > All Settings, and click UDT Settings in the Product Specific Settings section.
2. Click Discover Active Directory Domain Controller in the Track Users and Endpoints.
   The Device Tracker Discovery page is displayed.
3. Click Add Administrator Credential.
4. Create the appropriate credential for UDT to use with this Active Directory domain controller.
   For information on credentials see **Manage Active Directory credentials**.
5. Click Test, and if the credentials are verified click Assign. The credential is added to the list.
6. Click Next.
7. The Discovering DC popup is displayed, and the network is scanned for Domain Controllers.
   The Active Directory domain controllers on the network are listed.
8. Select the controller to use, and click Import.
9. Click OK, I'm Done.
10. The Welcome to Discovery Central page is displayed. This shows all discoveries including UDT ports and domain controllers.

What am I testing against?

Active Directory credentials are used to discover domain controllers. Each credential in the list is used to contact Active Directories for the corresponding domain. Essentially, you should create a separate credential for each domain.

For example, if you define three credentials:
   - alpha.local\administrator
   - beta.local\Joe.Frazier
   - zeta.local\Muhammad.Ali

Each would be used in turn to contact their relevant domain controllers. More specifically, "administrator" would be used to discover domain controllers on "alpha.local"; "Joe.Frazier" would be used to contact domain controllers on "beta.local"; and "Muhammad.Ali" would be used to contact domain controllers on "zeta.local".

For purposes of discovering AD domain controllers, the AD account must be a member of the domain; and for purposes of polling for user login data, the AD account must at least be a member of Event Log Readers if not a group with greater permissions.

Edit an Active Directory domain controller

You can edit Active Directory domain controller settings such as the controller name, IP address, default view, polling settings, custom properties, and alert thresholds using the Edit Properties page.

1. Go to Settings > All Settings, and click UDT Settings in the Product Specific Settings section.
2. Click Manage Active Directory Domain Controller in the Track Users and Endpoints section.
3. Select the Active Directory Domain Controller, and click Edit.
   The Edit Properties page for this controller is displayed.

   For further information on using this Edit Properties page, see Edit node properties.

   Settings specific to Active Directory domain controllers are shown near the bottom of the Edit Properties page.
Assign a credential to an Active Directory domain controller

A credential is simply a username and password, that can be accessed by a unique name. This saves you having to enter the username and password each time you use a device. After you have set up a credential when adding a Active Directory domain controller, or have created it using Manage Active Directory credentials, you can apply it to multiple controllers.

1. Go to Settings > All Settings, and click UDT Settings in the Product Specific Settings section.
2. Click Manage Active Directory Domain Controller in the Track Users and Endpoints section.
3. Select one or more Active Directory domain controllers in the list.
4. Click Assign security log access credentials.
5. Select or create the required credential, and click OK.

Delete an Active Directory Domain Controller

1. Go to Settings > All Settings, and click UDT Settings in the Product Specific Settings section.
2. Click Manage Active Directory Domain Controller in the Track Users and Endpoints section.
3. Select one or more Active Directory domain controllers in the list.
4. Click Delete.
   a. To delete the controller from UDT, select Delete node and data from UDT only.
   b. To delete the controller for all SolarWinds products, select Delete node from all modules.
5. Click Delete to confirm.

Manage Active Directory credentials

Active Directory credentials are required for the Active Directory domain controllers you add to UDT. These can be set up and edited on the Manage Active Directory Administrator Credentials page, or created when you add a controller.
This topic covers how to add, edit, and delete Active Directory credentials, and the possible scenarios that may result when UDT attempts to validate these credentials.

The domain credential used by UDT for communications with the Domain Controller should have the following permission:

- Event Log Readers

The domain credentials should also have access to the following WMI namespaces:

- CIMV2
- directory
- RSOP

Add, edit or delete an Active Directory credential

1. Go to Settings > All Settings, and click UDT Settings in the Product Specific Settings section.
2. Click Add, Edit or Delete UDT Credentials in the UDT section.
3. To add a credential:
   a. Click Add UDT Credential.
   b. Enter a name to identify this credential. For example, if this credential were the one that you want UDT to use in retrieving event log data from an Active Directory domain controller, you might call it Event Log Reader.
   c. Enter the User Name (Domain\Username) to use with this credential.
   d. Enter and confirm the password, then click OK.
4. To edit a credential:
   a. Select the credential, and click Edit Credential.
   b. Amend the User Name and Password as required, and click OK.
5. To delete a credential.
   You cannot delete a credential if it is currently associated with one or more domain controllers. You can check if a credential is currently assigned by referring to the Assigned to DC(s) column in the credentials list.
   Select the credential, and click Delete.
6. Click OK to confirm the deletion.

Domain controller configuration validation

Domain controller configuration validation is performed in UDT on the following pages:
- Add Node
- Manage Active Directory Domain Controller
- Device Tracker Discovery

The following scenarios may be encountered.

<table>
<thead>
<tr>
<th>Event Notification Displayed</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMI service is not running</td>
<td>WMI services is not running on the Domain Controller.</td>
</tr>
<tr>
<td>WMI service is running but</td>
<td>UDT credential does not have rights to the required WMI namespaces (CIMV2, directory and RSOP).</td>
</tr>
<tr>
<td>user does not have enough</td>
<td></td>
</tr>
<tr>
<td>permissions</td>
<td></td>
</tr>
<tr>
<td>2 connection error</td>
<td>If the audit account log-on event is configured to the state &quot;No Auditing&quot; or &quot;Failure&quot; and the UDT credential does not have event log read access.</td>
</tr>
<tr>
<td>1 connection error</td>
<td>The audit account log-on event is configured as expected but the UDT credential does not have event log read access, or:</td>
</tr>
<tr>
<td></td>
<td>The audit account log-on event is not configured but the UDT credentials have event log read access.</td>
</tr>
<tr>
<td>Successful</td>
<td>If everything is set up as expected.</td>
</tr>
<tr>
<td>Test Failed</td>
<td>If the supplied credentials are wrong.</td>
</tr>
</tbody>
</table>

Set up polling of user data across domains

Enabling UDT to poll user data, essentially by retrieving event log data, on an AD domain controller outside the local domain of the UDT server requires setup both in UDT and the AD domain controller. UDT supports the following methods for getting event log data from another domain:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eventing6</td>
<td>This is the preferred method, and depends on the AD domain controller running Windows Server 2008 or later.</td>
</tr>
<tr>
<td>WMI</td>
<td>This method is supported across Windows platforms</td>
</tr>
</tbody>
</table>

UDT collects user information through a scheduled job (REL).

Define credentials for polling across domains

For purposes of retrieving user log data from AD domain controllers, the AD account that UDT uses must be a member of the relevant domain must at least be a member of Event Log Readers if not a group with greater permissions.

See [Securing a Remote WMI Connection](https://docs.microsoft.com) (© Microsoft 2018, available from https://docs.microsoft.com, obtained 12/18/2018) for instructions to make the account a member of Event Log Readers and make it capable of accessing relevant WMI namespaces.
Keep in mind these requirements when you set up your credentials for accessing an AD domain controller outside the local UDT server domain:

- The UDT user account must be a member of the target domain.
- The UDT user account must either be a member of the Administrators group on the target domain controller or a limited account with privileges to access the remote security event log and directory service on the remote domain controller. If UDT is using a limited account the account must be a member of these groups:
  - Domain Users
  - Distributed COM Users
  - Event Log Readers
  - Remote Desktop Users
- The domain credentials should also have access to the following WMI namespaces:
  - CIMV2
  - directory
  - RSOP

For information on setting namespace security, see Setting Namespace Security with the WMI Control (© Microsoft 2018, available from https://docs.microsoft.com, obtained 12/18/2018).

Rogue Devices, the White List, and the Watch List

SolarWinds User Device Tracker (UDT) enables you to quickly detect devices that are accessing your network that should not be or that you want to investigate further. You can mark those that are allowed access or ignore them completely.

**Rogue devices:** Devices that are expected to be accessing your network. They are on neither the Watch nor the White lists. This usually means they have not been encountered before and you will have to determine whether they are to be permitted access or not.

**Watched devices:** Devices you want to monitor.

**Safe devices:** Devices for which access to the network has been approved. A device is marked as safe by adding it to the white list.

**White list:** The list of devices that have been approved to access your network. This list can contain specific devices or rules that define devices.

The white list is actually two lists:

- **Included list:** The devices on this list comply to one or more rule determining they belong on the network. Devices in this list are considered safe devices.
- **Ignored list:** These devices are ignored by UDT and all related data is ignored.

**Watch list:** The list of watched devices that are on the network, showing current connection details.
Manage the White List

The UDT White List enables you to specify which endpoints on your network you regard as safe. Using this list UDT can immediately detect endpoints that are therefore not considered safe, and display these on the Rogue Devices widget.

Simple rules determine which endpoints are included in the White List.

When you first launch UDT, the Rogue Devices widget displays a Create White List button. Click this to open the Add endpoints to the White List page.

The Manage White list page is displayed when you click on the Manage List link on the Rogue Device widget. By default UDT has the following three rules set up:

- Any Hostname
- Any IP Address
- Any MAC Address

This means that all hostnames, IP Addresses and MAC addresses are considered safe and included in the White List. No endpoints appear on Rogue Devices widget.

UDT treats an endpoint's MAC address, IP address, and hostname as separate objects. Depending on white list inclusion rules, one or more of those objects could possibly appear in the Rogue Devices widget at the same time.

On this page you can edit, disable, enable, and delete rules.

Click Add new to open the Add endpoints to the White List page and create new rules.

Ignoring devices

The White List also enables you to tell UDT which endpoints on your network to ignore altogether. Any endpoint that you want UDT to ignore becomes completely invisible to all its widgets.

Click the Ignored tab to display the rules for ignoring endpoints.

The rules for ignoring endpoints are identical to those used to Add endpoints to the White List.

Add endpoints to the White List

UDT uses inclusion rules to determine whether endpoints connected to monitored devices are safe or unsafe. A rule will specify the address, hostname or subnet to be included. The following selection methods can be used in a rule.

<table>
<thead>
<tr>
<th>SELECTION METHOD</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Individual hostnames, IP Address or MAC Address</td>
</tr>
<tr>
<td><strong>SELECTION METHOD</strong></td>
<td><strong>EXAMPLE</strong></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IP range</td>
<td>A range of IP addresses (IP4 or IP6)</td>
</tr>
<tr>
<td>MAC range</td>
<td>A range of MAC addresses</td>
</tr>
<tr>
<td>Subnet</td>
<td>a logical subdivision of IP addresses</td>
</tr>
<tr>
<td>Custom</td>
<td>Any hostname, IP or MAC address that contains a specific pattern</td>
</tr>
</tbody>
</table>

A rule can consist of multiple instances of the same selection method.

Follow these steps to add endpoints to the White List by adding rules.

1. Click Manage List on the Rogue Device widget on the Device Tracker Summary view. The existing inclusion rules are displayed.
2. Click Add New on the Included tab.
3. Click a Selection Method, and add the appropriate information:
   - **Device**: Select the target (Hostname, IP Address or MAC Address), and enter the appropriate string. Click Add More to add another device, as needed.
   - **IP Range or MAC Range**: Enter the Start address and End address of the range. Click Add More to add another range, as needed.
   - **Subnet**: Click the plus icon (+) and, in the Add New Subnet popup, enter the Subnet Address and Subnet Mask. Then click Add. Add further subnets, if required.
   - **Custom**: Select a target and enter appropriate patterns, using asterisks (*) as wildcards as required. Enter each one on a separate line.
4. Click Next.
5. Optionally, enter a name and description for this rule.
6. Click Finish.

Once a rule has been created you can:
- Edit it, and change the parameters.
- Disable it, so it is not applied until it is enabled again.
- Delete it.
Manage Watch List

The Watch List enables you to create a list of devices and users to be able to see where they are located on your network. This list is displayed in the Device Watch List widget on the Device Tracker Summary page. Click Update All to refresh the list with current information.

To add a device or user to the Manage Watch List:

2. Click Add Device/User.
3. Enter the MAC Address, IP Address or Hostname (if watching a device), or the username (if watching a user).
4. Optionally, you can add a Name and Description for this device to remind you why it is being monitored.

Devices can also be added to the watch list by clicking Watch this device on the Rogue Devices widget.

UDT Settings

To access the UDT Settings, navigate to Settings > All Settings > UDT Settings.

<table>
<thead>
<tr>
<th>SECTION</th>
<th>SETTINGS/LINKS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Management</td>
<td>Discover Ports</td>
<td>Add, manage, configure and delete ports.</td>
</tr>
<tr>
<td></td>
<td>Manage Ports</td>
<td></td>
</tr>
<tr>
<td>Track Users and EndPoints</td>
<td>Add Active Directory Domain Controller</td>
<td>Monitor Active Directory users and keep an eye on network users.</td>
</tr>
<tr>
<td></td>
<td>Manage Active Directory Domain Controller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage Watch List</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage White List</td>
<td></td>
</tr>
</tbody>
</table>
## Port Management

The Port Management page is used to manage and monitor nodes and ports.

To access the Port Management page, either:

- Click Manage Ports on the All UDT Nodes widget on the Device Tracker Summery view.
- Navigate to Settings > All Settings > UDT Settings, and select Manage Ports.

You can add a node at any time by clicking **Add Node**.

Select Port Discovery to access the [Orion Discovery Central](https://your Orion Discovery Central).

### Unmonitored nodes

1. Select Show Nodes and Filter to: UDT Unmonitored Nodes.
2. Select a node. The following options can then be selected:

### License Summary

- **UDT License Summary**
  - This link takes you to your [SolarWinds license details page](https://yourSolarWinds license details page), that shows license details for all your SolarWinds Orion products including UDT. This includes the UDT version, type of license, and allowed number of monitored ports and current number of monitored ports.

### Thwack Community

- **UDT thwack Forum**
  - This link takes you to the [SolarWinds Thwack UDT forum](https://yourSolarWinds Thwack UDT forum).

### UDT Credentials

- **Add, edit or delete UDT Credentials**
  - Create, edit and delete Active Directory Administrator Credentials.

<table>
<thead>
<tr>
<th>Section</th>
<th>Settings/Links</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDT Settings</td>
<td><strong>Polling intervals</strong></td>
<td>SolarWinds User Device Tracker comes configured to produce the best results in most network environments.</td>
</tr>
<tr>
<td></td>
<td><strong>Data Retention</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Thresholds</strong></td>
<td>However, in some environments you may find you need to adjust settings such as polling frequency, job timeouts, data retention, warning thresholds, and monitored port types to suit your monitoring requirements.</td>
</tr>
<tr>
<td></td>
<td><strong>View UDT Job Status</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Advance Settings</strong></td>
<td></td>
</tr>
<tr>
<td>License Summary</td>
<td><strong>UDT License Summary</strong></td>
<td></td>
</tr>
<tr>
<td>Thwack Community</td>
<td><strong>UDT thwack Forum</strong></td>
<td></td>
</tr>
<tr>
<td>UDT Credentials</td>
<td><strong>Add, edit or delete UDT Credentials</strong></td>
<td></td>
</tr>
</tbody>
</table>
- **Edit properties:** Click to open the [Edit Properties](#) page, where you can edit the polling details, custom properties, alert thresholds and other information for the selected node.
- **Unmanage:** Click to suspend polling and statistics collection for a specified period. During this period the node status will be "Node status is Unmanaged".
- **Rerunage:** Click to immediately resume polling and statistics collection.
- **Monitor node with UDT:** Click to monitor any ports on this node from the next poll. The node will now be displayed in the Monitored nodes list.
- **Delete:** Delete the selected node.

## Monitored nodes

1. Select Show Nodes and Filter to: UDT Monitored Nodes.
2. Select a node. Expand to show ports. The following options can then be selected:
   - **Edit properties:** Click to open the [Edit Properties](#) page, where you can edit the polling details, custom properties, alert thresholds and other information for the selected node.
   - **Unmanage:** Click to suspend polling and statistics collection for a specified period. During this period the node status will be "Node status is Unmanaged".
   - **Rerunage:** Click to immediately resume polling and statistics collection.
   - **Poll now:** Click to immediately initiate polling for the selected device.
   - **Delete:** Delete the selected node.

## Ports

*To shutdown or turn on a port you must have Read/Write Credentials for this node*

1. Select Show Ports
2. Select a port. The following options can then be selected:
   - **Unmonitor:** Click to stop monitoring a monitored port.
   - **Monitor:** Click to monitor an unmonitored port.
   - **Shutdown:** Click to shutdown the selected port.
   - **Turn on:** Click to turn on the selected port.
   - **Delete:** Delete the selected port.

## Manage Watch List

The Watch List enables you to create a list of devices and users to be able to see where they are located on your network. This list is displayed in the [Device Watch List](#) widget on the [Device Tracker Summary](#) page.

Click **Update All** to refresh the list with current information.

To add a device or user to the Manage Watch List:

2. Click Add Device/User.

3. Enter the MAC Address, IP Address or Hostname (if watching a device), or the username (if watching a user).

4. Optionally, you can add a Name and Description for this device to remind you why it is being monitored.

Devices can also be added to the watch list by clicking Watch this device on the Rogue Devices widget.

Manage the White List

The UDT White List enables you to specify which endpoints on your network you regard as safe. Using this list UDT can immediately detect endpoints that are therefore not considered safe, and display these on the Rogue Devices widget.

Simple rules determine which endpoints are included in the White List.

- Any Hostname
- Any IP Address
- Any MAC Address

This means that all hostnames, IP Addresses and MAC addresses are considered safe and included in the White List. No endpoints appear on Rogue Devices widget.

UDT treats an endpoint's MAC address, IP address, and hostname as separate objects. Depending on white list inclusion rules, one or more of those objects could possibly appear in the Rogue Devices widget at the same time.

On this page you can edit, disable, enable, and delete rules.

Click Add new to open the Add endpoints to the White List page and create new rules.

Ignoring devices

The White List also enables you to tell UDT which endpoints on your network to ignore altogether. Any endpoint that you want UDT to ignore becomes completely invisible to all its widgets.

Click the Ignored tab to display the rules for ignoring endpoints.

The rules for ignoring endpoints are identical to those used to Add endpoints to the White List.
Polling Interval

This page, accessible by clicking Polling Interval on the UDT Settings page, allows you to configure the polling interval.

The defaults for all intervals is 30 minutes.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Default Poll Interval</td>
<td>The frequency of polling for layer 2 devices, such as switches.</td>
</tr>
<tr>
<td>Layer 3 Default Poll Interval</td>
<td>The frequency of polling for layer 3 devices, such as routers.</td>
</tr>
<tr>
<td>Domain controller Default Poll</td>
<td>The frequency of polling Active Directory domain controllers for user login information.</td>
</tr>
<tr>
<td>Interval</td>
<td></td>
</tr>
</tbody>
</table>

Polling Timeout Warning

SolarWinds recommends monitoring a maximum of 3,000 devices with a single UDT poller. If many of your devices require monitoring at both Layer 2 and Layer 3 of the network stack, the maximum device limit that a single UDT poller can service within the polling interval (by default, 30 minutes) may be lower.

For example, if you use the default polling interval (30 minutes), you are managing 2,000 devices on a server with the recommended minimum hardware widgets, and 1,000 devices require polling at both L2 and L3, the polling cycle may complete before 1,000 jobs are even started. As a result, those unstarted jobs are queued for the next polling interval. However, in the meantime, the jobs currently running, having started, continue to be processed until finished, which may be sometime after 30 minutes—let's say 35 minutes.

35 minutes after the previous polling cycle, the next cycle begins and the jobs queued from the previous cycle are processed. And this staggered pattern of accumulating data is likely to become the norm, potentially producing issues with the timeliness of data seen in Web Console widgets and reports.

There are three options:

- Increase server hardware components so that the existing polling workload finishes within the set interval.
- Install an additional UDT poller on a separate server machine, and distribute work across the two pollers. For more information, see “Additional Polling Engine and Web Console
- Increase the polling intervals, with the risk that the data gathered for devices polled early in the cycle might become stale by the time the cycle finishes.

Device Tracker Thresholds

This page lets you to define what you want to be regarded as high and warning levels of port utilization. This is the percentage of available ports. This is used in reports and widgets such as the Top Nodes by Percentage Port Used.
Data Retention

This page, accessible by clicking Data Retention on the UDT Settings page, enables you to configure UDT data retention settings.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
<th>DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>History Retention</td>
<td>The number of days for which port activity is retained.</td>
<td>30</td>
</tr>
<tr>
<td>Detailed Statics</td>
<td>The number of days after which detailed statistics are summarized into hourly statistics.</td>
<td>7</td>
</tr>
<tr>
<td>Hourly Statistics</td>
<td>The number of days after which hourly statistics are summarized into daily statistics.</td>
<td>30</td>
</tr>
<tr>
<td>Daily Statistics</td>
<td>The number of days after which daily statistics are deleted.</td>
<td>365</td>
</tr>
</tbody>
</table>

View UDT Job Status

This page displays the UDT Job Status information including the following:

- Node ID
- Engine
- IP Address
- Node Caption
- Job Type
- Node Unmanaged
- Polling Disabled
- Polling Interval
- Scan Duration
- Averaging Factor
- Last Run
- Last Successful Scan
- Last Result
- Next Run
- Poll Now

Click Poll Now to poll a specific node.

Advanced Configuration Settings for SolarWinds User Device Tracker

The Device Tracker Advanced Settings page provides information on the advanced settings available for tuning the behavior of SolarWinds UDT.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD User Update Interval</td>
<td>This frequency that UDT will update Active Directory user information.</td>
</tr>
<tr>
<td>SNMP Timeout</td>
<td>How long UDT will wait for a response to a single SNMP request.</td>
</tr>
<tr>
<td>Port Discovery Job Timeout</td>
<td>How long UDT will wait for a Port Discovery Job to complete.</td>
</tr>
<tr>
<td>Layer 3 Discovery Job Timeout</td>
<td>How long UDT will wait for a Layer 3 discovery job to complete.</td>
</tr>
<tr>
<td>Layer 2 Job Timeout</td>
<td>How long UDT will wait for a Layer 2 job to complete.</td>
</tr>
<tr>
<td>Layer 3 Job Timeout</td>
<td>How long UDT will wait for a Layer 3 job to complete.</td>
</tr>
<tr>
<td>DNS Job Timeout</td>
<td>How long UDT will wait for a DNS job to complete.</td>
</tr>
<tr>
<td>DNS Cache Positive TTL</td>
<td>How long resolved hostnames will be cached.</td>
</tr>
<tr>
<td>DNS Cache Negative TTL</td>
<td>How long unresolved hostnames will be cached.</td>
</tr>
<tr>
<td>SNMP Pacing Delay</td>
<td>How long UDT will wait for between subsequent SNMP requests.</td>
</tr>
<tr>
<td>Monitored Port Types</td>
<td>Check all the Port Types that will be discoverable by UDT.</td>
</tr>
<tr>
<td>Search Results Row Limit</td>
<td>The maximum number of rows per table returned by UDT in the search results page.</td>
</tr>
<tr>
<td>MAC-Notification processing interval</td>
<td>The frequency that UDT will process MAC notification traps.</td>
</tr>
</tbody>
</table>
Solutions in SolarWinds UDT

The following sections provide instructions for accomplishing necessary tasks with UDT based on different scenarios:

- Enable DNS resolution for wireless nodes
- Resolve IP address conflicts with IPAM and UDT
- Find the switch and port where a particular hostname, IP, or MAC address is/was connected
- Track status for a group of ports
- Shut down a network device port
- Create and manage a watch list
- Show rogue endpoint connections in real-time
- Find wireless endpoint connections
- Find a user's connections
- Move SolarWinds UDT to a new server
- Define credentials for polling across domains
Enable DNS resolution for wireless nodes

UDT uses the Orion Platform wireless component to manage wireless devices. By default, the wireless component does not resolve a wireless node's IP address into a hostname. To enable this to do so, adjust the SolarWinds.Wireless.Collector.dll.config file as follows:

1. Open SolarWinds.Wireless.Collector.dll.config. By default this is located in the C:\Program Files\SolarWinds\Orion\Wireless directory.
2. Change the value of:
   <add key="RDNSTimeout" value="0" />
   to:
   <add key="RDNSTimeout" value="1" />
3. Save the change and restart the Orion Web Console.

See also: Manage the UDT White List

Resolve IP address conflicts with IPAM and UDT integration

Integration with UDT and IPAM is available with UDT v 3.2 and IPAM v 4.3 or higher. If you are running both products, the built-in integration provides a view of end-to-end mapping of an IP address to any connected user/device, along with the device port and connection details in the same window. If you are running UDT v 3.2 and IPAM v 4.3 or higher, no actions are needed for integrating the two products: IPAM will automatically detect if UDT is installed and add UDT users and switch port columns to your IP address view.

The following screen shot shows the display presented in the IPAM Manage Subnets & IP Address widget when IPAM and UDT are integrated.

Integrating IPAM with UDT can help you troubleshoot in the following ways:
• Find out which user or device is accessing a particular IP address
• Drill down to get network connection history for an IP address
• Show port and user information related to an IP address or host DNS assignment
• View port usage and capacity on every switch
• Detect endpoint devices having IP address conflicts
• Shutdown a port through the web interface

Address conflicts are shown in the IP Address Conflicts widget on the IP Address Manager dashboard.

<table>
<thead>
<tr>
<th>IP ADDRESS Conflicts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP ADDRESS</strong></td>
</tr>
<tr>
<td>10.129.21.12</td>
</tr>
</tbody>
</table>
1. Click on the IP Address to display more information about the conflict.

   ![IP Address Conflict Details](image)

   **CONFLICT STATUS:** Active
   **CONFLICT TYPE:** Scope Overlap
   **CONFLICT DETECTED:** 2 day(s) ago (29 Aug 2018 01:23:35 AM)
   **RECOMMENDED ACTION:** Release and renew the IP address on one of the endpoints.
   - OR Change the IP address of the less critical endpoint to “static” assignment, resize the DHCP scopes so they don’t overlap, then reset the device to “dynamic” assignment.
   - OR Shut down the switch port for the less critical endpoint, resize the DHCP scopes so they don’t overlap, then re-enable the switch port.

   **ASSIGNED DEVICE** | **CONFLICTING DEVICE**
   --- | ---
   IP ASSIGNMENT: Dynamic | Dynamic
   MAC: 00-50-BA-F7-1D-24 | 00-40-52-F3-6D-D9
   SCOPE: WEST0021: Users-1stFl | WEST0021: Users-1stFl
   on WEST00501v | on WEST0052v
   UDT MOST RECENT HOSTNAME: Clark4-nb.demo.lab | wcix9-nb.demo.lab
   UDT NODE PORT/SSID: G2/0/20 | G3/0/20
   Shutdown | Shutdown

   **UDT Last 10 History Events**

<table>
<thead>
<tr>
<th>TIME</th>
<th>MAC ADDRESS/USER NAME</th>
<th>NODE PORT/SSID</th>
<th>NODE/ACCESS POINT</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/28/2018 2:23:35 AM</td>
<td>DEMO.LAB\Aaron.Clark logged on</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. If you need to resolve the conflict immediately, click on the node port. The UTP Port Details page is displayed.
3. Click Shutdown in the Port Details widget.

Find the switch and port where a particular hostname, IP, or MAC address is or was connected

Suppose you need to find the switch and port where a particular hostname, IP, or MAC address is now or has been connected to respond to a security or network problem.

From the Device Tracker Summary page:

1. Click the dropdown button after the search box in the upper right, and select the identifying method to be used for the search.

You can select multiple methods, although this will slow down your search.

MAC addresses can be entered with or without formatting.

2. Enter the identifier. You can enter the full name or address of the item, or use asterisks as wildcards.

An asterisk can be substituted anywhere in the search for one or more characters. For example:
laptop-01* will find laptop-011, and laptop-01223
3. Press Enter or click the search button to begin the search.

4. If a single result is returned, the details page for the item is displayed.
   If multiple results are returned, click on the required result to display the details page.

![Device Tracker Endpoint Details](image)

**Track status for a group of ports**

Suppose you want to track port usage for all of your Cisco devices. You need to create an Orion Platform group containing the relevant ports, and select that group in UDT widgets.

**Create a group**

1. From the Web Console, go to Settings > All Settings.
2. Click Manage Groups in the Node & Group Management section.
3. Click Add New Group.
4. Enter a name for the group (for example, "Cisco Ports"), and expand Advanced.
5. Select the status rollup mode:
   - To roll up the worst status of the group members, select Show Worst Status.
   - To roll up the best status of the group members, select Show Best Status.
   - To display a warning status if the group members have a mixture of different statuses, select Mixed Status shows warning.
6. Click Next.
7. Click Add dynamic query.
8. Enter a Dynamic query object name.
9. Select Port from the Orion Object drop-down list.
10. Click Add Condition and build the following condition using the three drop-down lists: Port Operational Status is 1.

This condition limits the group membership to operational ports.

11. Click Add Condition again and build a second condition: Node Vendor is Cisco.

This condition limits the group membership to ports on Cisco devices.

12. Click Preview to verify that the dynamic query is selecting the intended objects, and if so click Save.

13. Click Create Group.

This group is now available for you to use in a UDT port widget.

Add the group to the Device Tracking Summary view

1. In the UDT Summary view, click Customize Page.
2. Click Add Widget, select Group By Feature, and drag UDT Ports in Use Overview to the required position.
3. Click Done Adding Widgets, and click Done Editing.
4. Click Edit in the new UDT Ports in Use Overview widget.
5. Enter an appropriate title (for example, "Cisco Ports Usage").
6. Select the group you created.
7. Click Submit.

The chart now shows you the percentage of usage for all grouped ports on your Cisco devices.

**Shut down a network device port**

Suppose UDT lists an endpoint on your network as rogue, and you want to shut down access for it while you investigate.

1. In the Rogue Devices widget, click the rogue device name.
   The Device Tracker Endpoint Details page is displayed.
2. In the Current Network Connections widget, click the node port or SSID.
   The Device Tracker Port or SSID Details page is displayed.
3. In the Port Details widget, click the Shutdown button.
Create and manage a watch list

Create a watch list to alert you when specific IP or MAC addresses, hosts, or users connect to the network.

This procedure assumes you have already discovered the appropriate nodes and ports, and have added an Active Directory domain controller and appropriate credentials for UDT to use in retrieving user information.

- For information on discovery, see Discover and add network devices.
- For information on adding a domain controller and credentials, see Add Active Directory Controllers and users.

2. Click Add Device/User.
3. Select the object type (MAC address, IP address, hostname, or username) and enter a valid string.
4. Optionally, give this item a name and description.
5. Click OK.
6. Repeat 1-5 for all objects you want to be added to the Watch List.
7. Return to the Device Tracker Summary page. The Device Watch List will now show information about these devices if they have been attached to the network.

If a device is not found, a message saying that it "has never been seen" is displayed.

Display rogue endpoint connections in real-time

Suppose you have a White List set up, but you want real-time or near real-time alerts for when a rogue device connects to the network.

To do this, set up your devices to send connection-related traps to the UDT server. UDT checks the database for trap-related information at a set interval. If an endpoint connects to a UDT device, and the endpoint is not on the White List, UDT posts an alert in the web console.

The following instructions are for Cisco devices only.

You can remove device configurations by running a given command with 'no' in front of it. For example:

```
no set logging server ip_address
```

removes that target from the remote logging stream.

To enable your Cisco devices to send trap messages:
1. Open a command line in config mode on each device.
2. Execute the commands from the examples below, changing the IP address to match your UDT server:
   - Traps (IOS)
     ```
     snmp-server host ip_address public config
     snmp trap mac-notification change added
     snmp trap mac-notification change removed
     ```
   - Traps (CatOS)
     ```
     set snmp trap ip_address public config
     snmp trap mac-notification change added
     snmp trap mac-notification change removed
     ```
3. From the Web Console, go to Settings > All Settings.
4. Select UDT Settings in the Product Specific Settings section.
5. Click Advanced Settings in the UDT Settings section.
6. Change the value for MAC-Notification Processing Interval to the frequency that you want UDT to check for new trap messages. The default is 120 seconds.
7. Click Save.
8. To verify your setup, connect a device to the network that is not on the UDT White List.
9. Wait for the time set in Step 6 to elapsed, and check the Active Alerts and All Triggered Alerts widgets for an entry that shows the MAC address of the device you just connected.

Find wireless endpoint connections

To find the endpoints currently connected to the wireless network through a particular SSID:
1. From the SolarWinds Orion Summary Dashboard, drill down to the relevant node (wireless controller) in the All Nodes list.
2. In the Node Details view, click on the relevant SSID in the All Access Points and SSIDs widget. The SSID Details view is displayed.
   - The Current Endpoint Connections widget shows the endpoints currently connected to the wireless network through this SSID.
   - The All Endpoint Connections shows all endpoints that have connected via the SSID showing the connection period.
   - If you do not see an endpoint that you expect to see, you can search for it by IP address, hostname, or MAC address in either the Current Endpoint Connections or the All Endpoint Connections widget.
3. Click any endpoint to display its Endpoint Details page.
Find a user’s connections

To find all the endpoints where a specific user is or has been connected to the network:

1. On any UDT page, click on the menu button ▼ by the search box, and ensure only User Name is selected.
2. Enter the user name, and click the search button to begin the search.

If successful, the Device Tracker User Details page is displayed for the user, showing the user's connections in the All Endpoint Log Ins widget.

Moving SolarWinds UDT to a new server

SolarWinds UDT encrypts your sensitive data with a security certificate. To grant a new server access to this encrypted data, you must replicate the original security certificate to the new server.

If you do not replicate the original certificate, SolarWinds UDT on the new server cannot access any credentials used by your component monitors, and all of those component monitors will fail.

To replicate the original certificate:

**STEP 1: Export the credential from the original server:**

1. From the Windows Start Menu, select Run, type MMC, and click OK.
   The Microsoft Management Console is displayed.
2. From the File menu, select Add/Remove Snap-in, and click Add.
3. Select Certificates from the Available Snap-ins column, and click Add.
4. Select Computer account, and click Next.
5. Select Local computer, and click Finish, then click OK.
   The Microsoft Management Console is displayed.
6. Expand the Certificates (Local Computer) group in the middle column.
7. Expand the Personal group, and then expand the Certificates group.
8. Right-click SolarWinds Job Scheduler, and click All Tasks > Export.
10. Select Yes, export the private key, click Next, and click Next again.
11. Type and confirm a password for this private key, and click Next.
12. Specify the file name you want to give the certificate, click Next, and then click Finish.
   The certificate is saved with a .pfx file name extension.

**STEP 2: Copy the .pfx certificate file to the new server.**

**STEP 3: Import the certificate to the new server:**

1. From the Windows Start Menu, select Run, type MMC, and click OK.
   The Microsoft Management Console is displayed.
2. From the File menu, select Add/Remove Snap-in, and click Add.
3. Select Certificates from the Available Snap-ins column, and click Add.
4. Select Computer account, and click Next.
5. Select Local computer, and click Finish, then click OK.
   The Microsoft Management Console is displayed.
6. Expand the Certificates (Local Computer) group in the middle column.
7. Expand the Personal group, and then expand the Certificates group.
8. If there is a SolarWinds Job Scheduler Engine item in the list, right-click SolarWinds Job Scheduler Engine and select Delete.
9. Right-click the Certificates / Personal / Certificates node in the left column, and click on All Tasks > Import.
10. Click Next in the Certificate Import Wizard.
11. Navigate to the .pfx certificate file you copied to the server, and click Next.
12. Enter the password for the private key, check Mark this key as exportable, and click Next.
13. Select Place all certificates in the following store, and then select Personal as the Certificate Store.
14. Click Next, and click Finish. A message is displayed saying the import was successful.

**Define credentials for polling across domains**

Keep in mind these requirements when you set up your credentials for accessing an AD domain controller outside the local UDT server domain:

- The UDT user account must be a member of the target domain.
- The UDT user account must either be a member of the Administrators group on the target domain controller or a limited account with privileges to access the remote security event log and directory service on the remote domain controller. If UDT is using a limited account the account must be a member of these groups:
  - Domain Users
  - Distributed COM Users
  - Event Log Readers
Remote Desktop Users

- The domain credentials should also have access to the WMI namespaces listed below:
  - CIMV2
  - directory
  - RSOP

You can use these instructions (© Microsoft 2018, available at https://docs.microsoft.com, obtained December 19, 2018) to give the account the relevant privileges.

See also: Set up polling of user data across domains.