



ForeScout

eyeExtend for ServiceNow

Configuration Guide

Version 2.2



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.Forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-05-29 13:53

Table of Contents

About ServiceNow Integration	5
Fore Scout App for Asset Management.....	5
Fore Scout App for IT Incidents	6
Fore Scout App for SOC Incidents	6
Use Cases	6
Asset Identification	6
Asset Inventory True-up.....	7
IT Service Management.....	7
Security Operations	8
Additional ServiceNow Documentation.....	8
About this Module	9
About Certification Compliance Mode	10
About Support for Dual Stack Environments.....	10
Concepts, Components, Considerations.....	10
Concepts	10
Components	12
Considerations	13
ServiceNow Instance Account.....	13
Upgrade from ServiceNow 1.x to 2.1 or 2.2.....	13
Upgrade from ServiceNow 2.0 to 2.1 or 2.2	14
Upgrade from ServiceNow 2.1 to 2.2.....	16
What to Do	16
Requirements.....	16
Fore Scout Requirements.....	17
Fore Scout eyeExtend (Extended Module) Licensing Requirements.....	17
Per-Appliance Licensing Mode	17
Flexx Licensing Mode	18
More License Information	19
ServiceNow Requirements	19
Install the Module	20
Start the Module	21
Configure the Module	21
Establish Connection to ServiceNow Instance	22
Edit ServiceNow Connection.....	26
Test ServiceNow Connection	27
Define General Settings	28
Define Outbound Mapping	29
Define ServiceNow Tables	32

Remove ServiceNow Tables	34
Define Host Properties	34
Define ServiceNow Lookup Properties.....	37
Verify the Configuration	40
Delete ServiceNow Instance	41
Remove ServiceNow Properties	41
Remove ServiceNow Tables	42
Remove ServiceNow Connection	43
Create ServiceNow Policies	43
Name the Policy	44
How Devices Are Detected and Handled	44
ServiceNow Policy Templates	45
Create an Add Asset Identification Information to CMDB Policy	47
Create an Update Asset Identification Information to CMDB Policy.....	53
Create an Assign to VLAN Stage 1 Policy	57
Create an Assign to VLAN Stage 2 Policy	62
Create a Switch Block Stage 1 Policy.....	65
Create a Switch Block Stage 2 Policy.....	70
Create a Switch Block Stage 3 Policy.....	73
Create a SecOps Ticketing Policy	77
Create Custom ServiceNow Policies	81
Policy Properties	82
Policy Actions	83
Add or Update Asset to CMDB	85
Create IT Incident	86
Create SOC Incident	88
Set Action Thresholds	89
Send Additional Properties.....	91
Work with Forescout eyeExtend for ServiceNow	98
Best Practices	98
Communication Thresholds	98
Appliance Sizing.....	99
Appliance Clustering	99
ServiceNow Tables	99
Additional Properties.....	100
General Guidance	100
Additional Forescout Documentation.....	100
Documentation Downloads	101
Documentation Portal	101
Forescout Help Tools.....	102

About ServiceNow Integration

Forescout eyeExtend for ServiceNow® enables the exchange of information between the Forescout platform and the ServiceNow cloud service as well as the integration of IT Service Management and Security Operations in ServiceNow. ServiceNow sends action requests to the Forescout platform and triggers policy actions.

With Forescout eyeExtend for ServiceNow, you can:

- Send selected tags to ServiceNow. You can configure and schedule mapping to the Configuration Management Database (CMDB).
- Import device properties and get real-time updates from ServiceNow.
- Create incidents in ServiceNow and receive real-time updates for them.
- Provide a Web service to ServiceNow to send action requests.

ServiceNow uses the Forescout policy engine to report incidents. It cooperates with the Forescout platform to take actions on devices and issue action requests in ServiceNow workflows and business rules.

The following are the scoped certified applications:

- [Forescout App for Asset Management](#)
- [Forescout App for IT Incidents](#)
- [Forescout App for SOC Incidents](#)

Forescout App for Asset Management

The Forescout App for Asset Management supports integration between the Forescout platform and ServiceNow. The Configuration Management Database (CMDB) is enriched and supplemented by the bi-directional data exchange between the Forescout platform and ServiceNow. Through adding or updating of device properties on ServiceNow's CMDB configuration item tables, the Forescout platform triggers the ServiceNow workflow by applying Forescout policies. These policies are based on the Forescout platform properties and the properties exchanged with the ServiceNow instance.

The data exchange is as follows:

- Identify devices on network segments using CounterACT® Appliance(s)
- Update ServiceNow tables with device properties captured by the Forescout platform
- Import device properties from ServiceNow of which the Forescout platform was not aware

The Forescout App for Asset Management also includes tables, import sets, and scripts needed by the Forescout App for IT Incidents and the Forescout App for SOC Incidents. These additional objects let the Forescout App for Asset Management push updates to the Forescout platform.

Forescout App for IT Incidents

The Forescout App for IT Incidents is for Information Technology (IT) personnel. The app lets you create IT service incidents in ServiceNow from the Forescout platform. The use case is available through a Forescout action.

The app also lets a ServiceNow user send action requests to the Forescout platform based on controls available in the Incident table.

The app contains a business rule to send information about an IT incident to the Forescout platform, in the event of an update. The information sent for an IT incident includes the incident number, category, subcategory, impact, urgency, priority, short description, and state.

This app is dependent on the Forescout App for Asset Management.

Forescout App for SOC Incidents

The Forescout App for SOC Incidents is for Security Operations Center (SOC) personnel. The app lets you create SOC incidents in ServiceNow from the Forescout platform. The use case is available through a Forescout action.

The app also lets a ServiceNow user send action requests to the Forescout platform based on controls available in the Security Incident table.

The app contains a business rule to send information about a SOC incident to the Forescout platform, in the event of an update. The information sent for a SOC incident includes the incident number, category, subcategory, business impact, priority, short description, and state.

This app is dependent on the Forescout App for Asset Management and the Security Incident Response plugin from ServiceNow.

Use Cases

This section describes important use cases supported by Forescout eyeExtend for ServiceNow. Be sure to review the [Best Practices](#).

To understand how this module helps you achieve these goals, see [About this Module](#).

- [Asset Identification](#)
- [Asset Inventory True-up](#)
- [IT Service Management](#)
- [Security Operations](#)

Asset Identification

ServiceNow's IT Asset Management and CMDB components are widely used. The Forescout asset identification and remediation functionality both benefit from each other's rich information.

Workflow

1. A device on the network is identified through admission events, and scanning activity by the Forescout platform, which captures additional properties. This device information is shared with ServiceNow.
2. ServiceNow adds this information in its repository and provides additional properties from its repository.
3. The Forescout platform adds these ServiceNow properties to its repository and leverages them for policy decisions.
4. Forescout and ServiceNow users view updated and correlated device information.

Asset Inventory True-up

The continuous monitoring function in the Forescout platform can play a role of “auditor” and help equalize and bring both the Forescout platform and the ServiceNow system up-to-date. The Forescout platform enriches asset attributes with additional context, such as the switch port to which the device is connected, VLAN information, network segment information, location, compliance status, and so on. The Forescout platform monitors and updates information in the asset inventory from the time a device enters the network until it leaves the network. The result is real-time asset monitoring and management that reduces the effort required to monitor and manage the assets and increases overall network asset compliance.

Workflow

1. A device’s information is captured upon scan activity.
2. The Forescout platform gets the device’s information from ServiceNow, points out discrepancies, and helps ServiceNow update its repository.
3. The Forescout platform can also verify if the device has the latest patches; if not, it can inform ServiceNow and take remediation actions.
4. Depending on the configuration, additional remediation actions may be taken.

For example, a software update is pushed out from ServiceNow and CMDB information is updated. The Forescout platform scans and finds that the device did not apply the update. The Forescout platform informs ServiceNow and a different pre-defined workflow is initiated, which updates or reissues the software update based on the Forescout policy.

IT Service Management

Actions in the Forescout platform, such as create an IT incident, result in incidents being created in ServiceNow.

Workflow

1. The Forescout user identifies an endpoint for which an IT incident must be created through a policy or manually.
2. The Forescout user triggers a Create IT Incident action from Forescout eyeExtend for ServiceNow.

3. An IT incident is added to the ServiceNow IT Incidents table, corresponding to the endpoint in the Forescout platform on which the Create IT Incident action was triggered.
4. ServiceNow sends the incident number, category, subcategory, impact, urgency, priority, short description, and state updates back to the Forescout platform.
5. The ServiceNow user creates an action request to the Forescout platform.

Security Operations

Actions in the Forescout platform, such as create a SOC incident, result in incidents being created in ServiceNow.

Workflow

1. The Forescout user identifies an endpoint for which a SOC incident must be created through a policy or manually.
2. The Forescout user triggers a Create SOC Incident action from Forescout eyeExtend for ServiceNow.
3. A SOC incident is added to the ServiceNow Security Incidents table, corresponding to the endpoint in the Forescout platform on which the Create SOC Incident action was triggered.
4. ServiceNow sends the incident number, category, subcategory, business impact, priority, short description, and state updates back to the Forescout platform.
5. The ServiceNow user creates an action request to the Forescout platform.

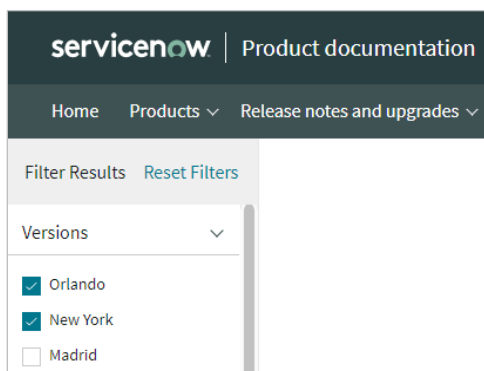
Additional ServiceNow Documentation

Refer to the following online documentation for more information about the ServiceNow solution:

- CMDB:
https://docs.servicenow.com/bundle/orlando-servicenow-platform/page/product/configuration-management/concept/c_ConfigurationManagementDatabase.html
- IT Service Management:
https://docs.servicenow.com/bundle/orlando-it-service-management/page/product/it-service-management/reference/r_ITServiceManagement.html
- Security Operations:
<https://docs.servicenow.com/bundle/orlando-security-management/page/product/security-operations/concept/security-operations-intro.html>

Or, refer to the following link and select the version:

<https://docs.servicenow.com/search?facetreset=yes&q=>



About this Module

The Forescout platform integrates with ServiceNow instances to provide complete visibility of assets. ServiceNow integration lets you send selected host information from the Forescout platform to ServiceNow instances and trigger Forescout platform actions based on properties.

Forescout eyeExtend for ServiceNow integrates the Forescout platform and ServiceNow so that you can:

- Use policies and actions provided by the eyeExtend module to update current asset information (such as switch port, open ports, or VLAN) to ServiceNow. See [ServiceNow Policy Templates](#).
- Use policy templates for action intents and ticketing. See [ServiceNow Policy Templates](#).

Forescout eyeExtend for ServiceNow and the Forescout App for Asset Management work together to support full functionality between the Forescout platform and ServiceNow. You must install and configure both components to work with the features described in this document. For example, Forescout policies and actions provided by the eyeExtend module are used to populate the import set table in the Forescout App for Asset Management with Forescout data, then the application transfers the data to ServiceNow CMDB.

In addition, there are Forescout apps for IT incidents and SOC incidents.

Read this document together with the installation and configuration guides for the *Forescout App for Asset Management*, *Forescout App for IT Incidents*, and *Forescout App for SOC Incidents*.

You must install and configure both the Forescout platform and ServiceNow to work with the features described in this document.

To access the Forescout Apps:

1. Go to <https://store.servicenow.com>.
2. Search for *Forescout App*. The following apps are available:
 - Forescout App for Asset Management
 - Forescout App for IT Incidents

- Forescout App for SOC Incidents
- 3. Select **More** to view the details of each app.
- 4. Select **Get** to download the Forescout apps you want.
- 5. Download and read the installation and configuration guides for each app you download. The guides are located under Supporting Links & Docs.

About Certification Compliance Mode

Forescout eyeExtend for ServiceNow supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

About Support for Dual Stack Environments

The Forescout platform detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, **IPv6 addresses are not yet supported by this eyeExtend module**. The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this eyeExtend module.

Concepts, Components, Considerations

This section provides a basic overview of the architecture of ServiceNow and the Forescout platform:

- [Concepts](#) – Basic integration concepts and deployment options.
- [Components](#) – Devices in your network that participate in the integration.
- [Considerations](#) – Setup details and common network structure issues to keep in mind when you implement this module.


Concepts

Integration lets you connect one or more CounterACT Appliances or Enterprise Managers to a unique ServiceNow instance. When multiple CounterACT Appliances are mapped to a single ServiceNow instance, they are grouped into a *connecting CounterACT Appliance cluster*. These devices handle communication between the ServiceNow instance and the rest of CounterACT Appliances in your environment. As part of the configuration, Forescout eyeExtend for ServiceNow lets you control the rate of insertion and update from the Forescout platform to the ServiceNow instance, thus avoiding the processing limit of ServiceNow.

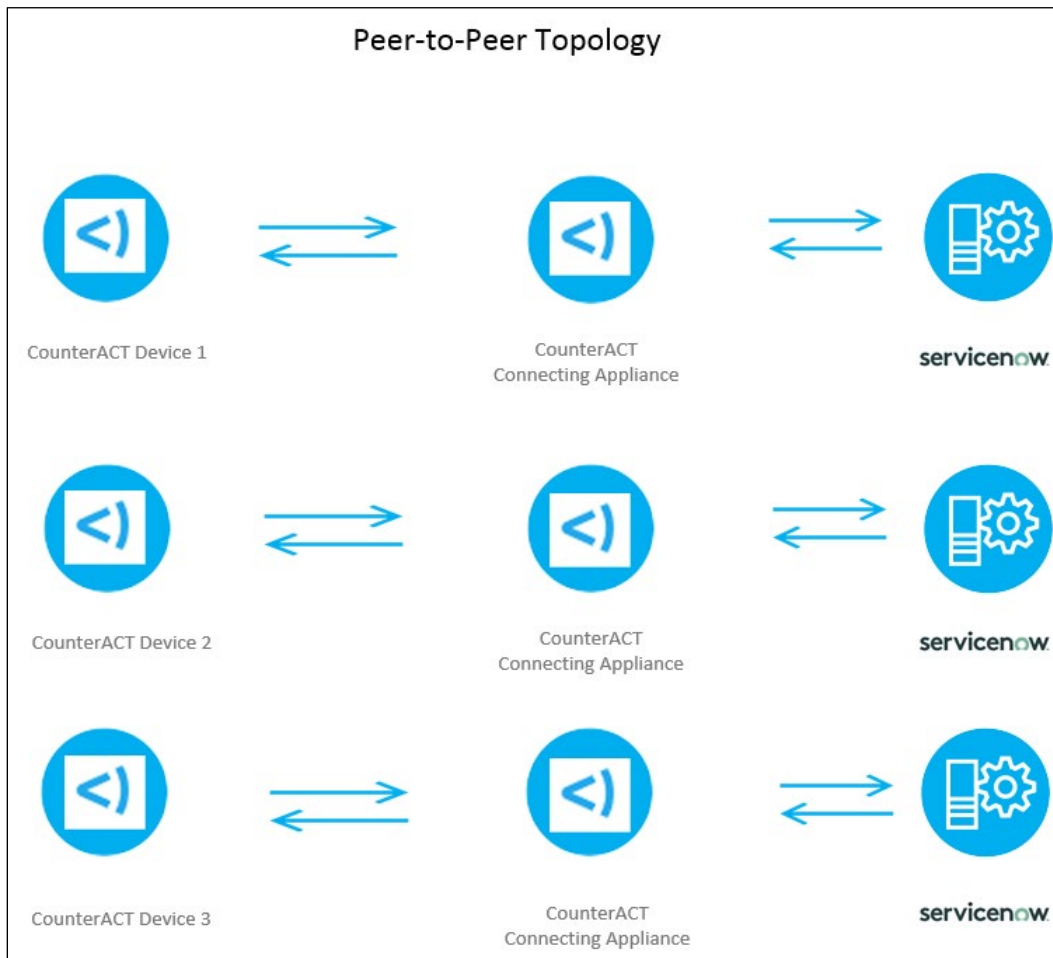
Typically, there is only one ServiceNow production instance per customer hosted in the cloud. CounterACT Appliances are connected to this ServiceNow instance using logical URL and user credentials.

Deployment Options

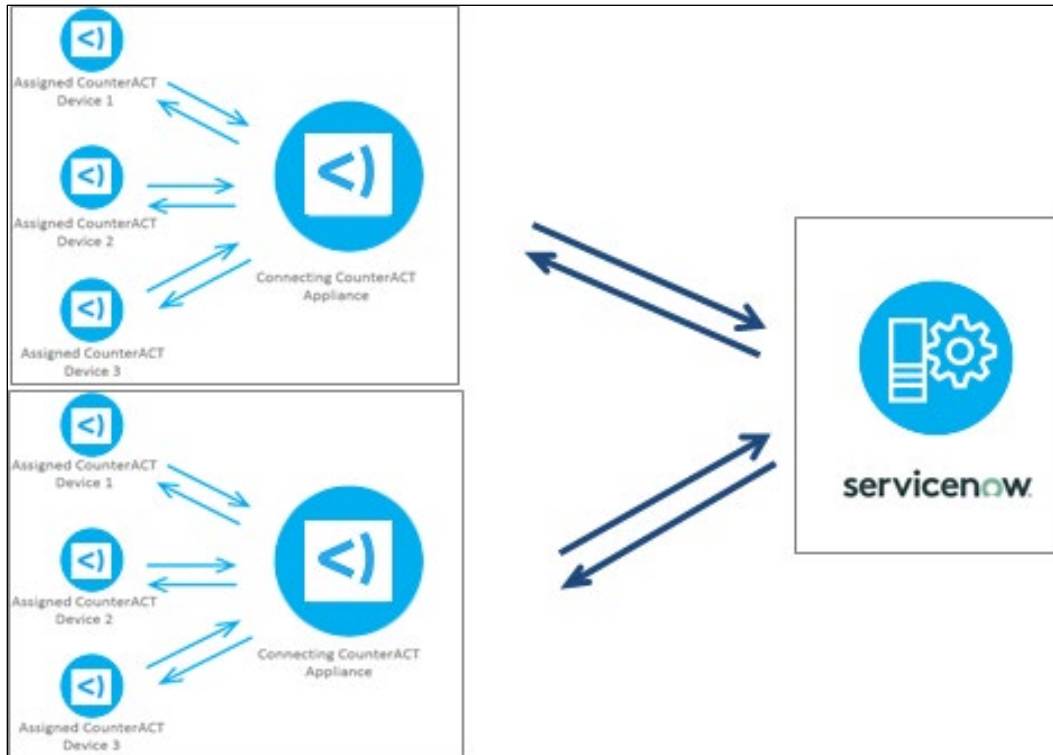
There are two topologies that can be used to set up multiple CounterACT Appliances to a ServiceNow instance. For both topologies, a single CounterACT Appliance can be assigned to only one ServiceNow instance.

 *The actual deployments can be designed to combine both topologies to meet particular network requirements.*

Peer-to-Peer: Each CounterACT Appliance communicates directly with a ServiceNow instance. This is a one-to-one relationship, where each CounterACT Appliance or Enterprise Manager initiates queries whenever required. This is often the topology for remote sites.



Appliance Proxy: One connecting CounterACT Appliance serves as a channel to a ServiceNow instance. The connecting CounterACT Appliance controls the number of requests to ensure more efficient traffic control and to avoid overloading the ServiceNow instance.



Components

- A **ServiceNow instance** is a cloud instance typically referenced by one logical URL per company (for example, mycompany.servicenow-instance.servicenow.com). The ServiceNow instance is already created and used by the company independent of the Forescout platform.
- A **CounterACT Connecting Appliance cluster** is a group of one or more CounterACT Appliances connecting to the ServiceNow instance through the logical URL associated with the ServiceNow instance. There may be more than one connecting Appliance cluster in a company, typically set up by geographical region, business unit, or functional separation.
- **CounterACT Appliances** manage or monitor devices based on the network segments assigned to a particular CounterACT Appliance. When these Appliances reach out to ServiceNow, they go through the CounterACT Connecting Appliance cluster(s).
- **Devices on the network** are the hardware assets whose information has to be exchanged between the Forescout platform and ServiceNow. The Forescout platform continuously monitors the devices – not just when they enter and leave the network.

In this context, when Forescout eyeExtend for ServiceNow is installed on CounterACT connecting Appliance clusters (each CounterACT Appliance individually), you can configure connection parameters to the ServiceNow instance. These connection parameters include logical URL (for example, mycompany.servicenow-instance.servicenow.com), user credentials (this user would have the right privileges/permissions to perform the necessary operations), proxy settings, and advanced settings.

Considerations

This section addresses any additional considerations for Forescout eyeExtend for ServiceNow.

Be sure to also review the [Best Practices](#).

ServiceNow Instance Account

Contact your ServiceNow administrator to get the username to connect to the ServiceNow instance. This is required to configure Forescout eyeExtend for ServiceNow. The user account should contain:

`x_ftpp_now_plat.integration`

To use IT Service Management, the user account should also contain:

`x_ftpp_incident_m.integration`

To use Security Operations, the user account should also contain:

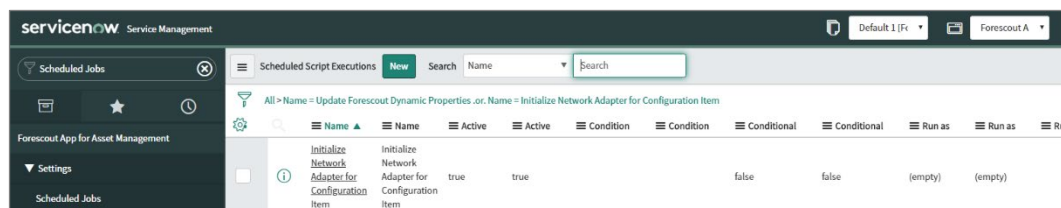
`x_ftpp_sec_inc_m.integration`

For instructions on creating user credentials, refer to the *Forescout App for Asset Management*, *Forescout App for IT Incidents*, and *Forescout App for SOC Incidents* installation and configuration guides.

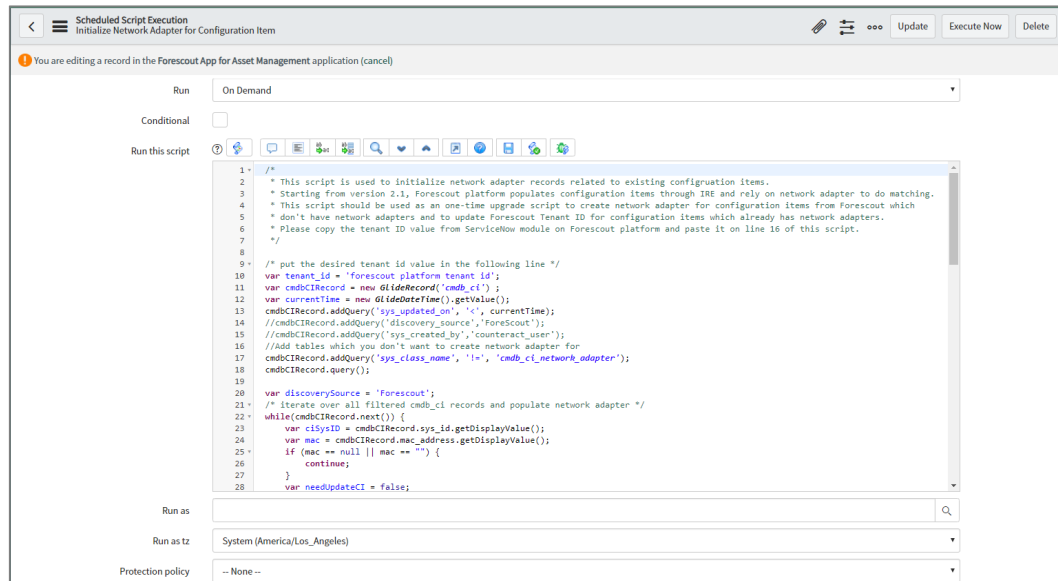
Upgrade from ServiceNow 1.x to 2.1 or 2.2

If you previously installed ServiceNow 1.x, you can upgrade to 2.1 or 2.2. After the upgrade:

- On the Forescout platform, stop policies.
- On ServiceNow, install the Forescout App for Asset Management 2.1. You can leave the 1.x Forescout App for CMDB installed or you can uninstall it.
- If there are assets populated in CMDB:
 - Go to **Forescout App for Asset Management > Scheduled Jobs**.
 - Select Initialize Network Adaptor for Configuration Item.



- Edit the **Run this script** section by adding any necessary queries after line 13 and replacing 'forescout platform tenant id' in line 10 with the Tenant ID displayed in **Options > ServiceNow > General Settings**.
- In **Run as**, select an appropriate user that will be populated to the **Created by** or **Updated by** column if the script creates or updates a record in ServiceNow.



- Select **Update** and **Execute Now**.
- On ServiceNow, add a new role for the user **x_ftpp_now_plat.integration**. Refer to the *Forescout App for Asset Management* installation and configuration guide for managing users.
- On the Forescout platform, edit the actions in the 1.x policies as follows:
 - Replace the **Add Asset to CMDB (Deprecated)** action with the **Add Asset to CMDB** action.
 - Replace the **Update Asset to CMDB (Deprecated)** action with the **Update Asset to CMDB** action.

Optional Upgrade Steps

Refer to the following sections in the *Forescout App for Asset Management* installation and configuration guide for optional upgrade steps:

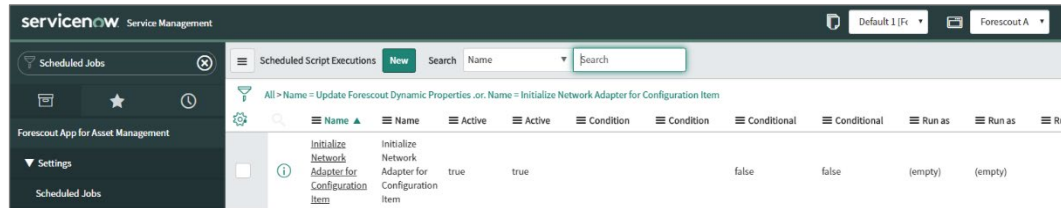
- Modify Forescout Classification Mapping table
- Modify Forescout CI Transform Map

Upgrade from ServiceNow 2.0 to 2.1 or 2.2

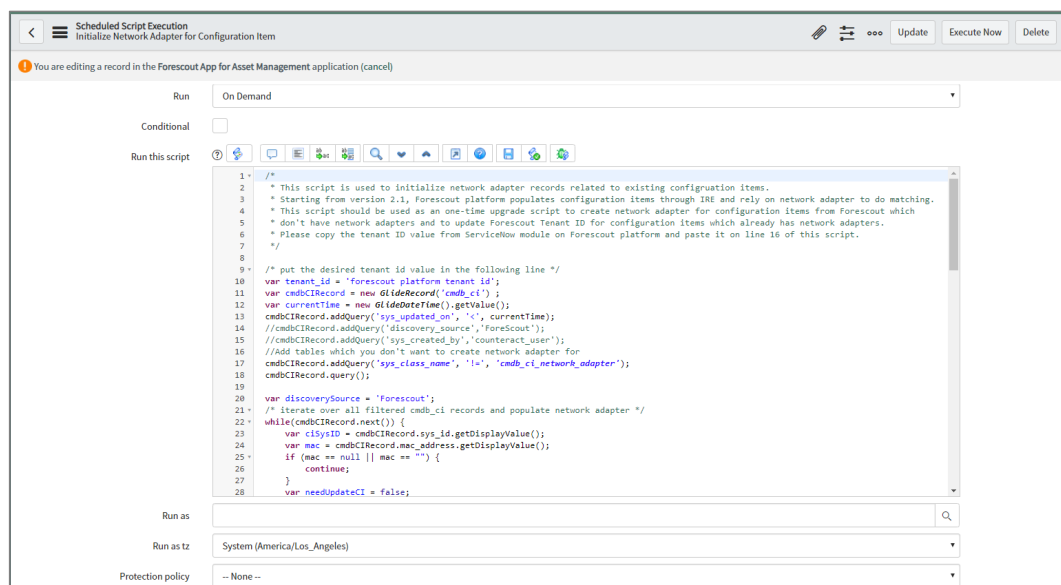
If you previously installed ServiceNow 2.0, you can upgrade to 2.1 or 2.2.

- On the Forescout platform, stop policies.
- On ServiceNow, upgrade to the Forescout App for Asset Management 2.1.

- If there are assets populated in CMDB:
 - Go to **Forescout App for Asset Management > Scheduled Jobs**.
 - Select Initialize Network Adaptor for Configuration Item.



- Edit the **Run this script** section by adding any necessary queries after line 13 and replacing 'forescout platform tenant id' in line 10 with the Tenant ID displayed in **Options > ServiceNow > General Settings**.
- In **Run as**, select an appropriate user that will be populated to the **Created by** or **Updated by** column if the script creates or updates a record in ServiceNow.



- Select **Update** and **Execute Now**.
- On ServiceNow, create a choice for discovery source and modify CI identifiers. Refer to the *Forescout App for Asset Management* installation and configuration guide for details.
- On the Forescout platform, edit the actions in the ServiceNow 2.0 policies as follows:
 - For the Add Asset to CMDB action, there are two more options for the Properties Mapping parameter: {vendor_classification} to Vendor and Model(vendor_classification) and {os_classification} to Operating System(os_classification). Select these options based on your use case.

- For the Update Asset to CMDB action, there are two more options for the Properties Mapping parameter: {vendor_classification} to Vendor and Model(vendor_classification) and {os_classification} to Operating System(os_classification). Select these options based on your use case.

Optional Upgrade Steps

Refer to the following sections in the *Forescout App for Asset Management* installation and configuration guide for optional upgrade steps:

- Modify Forescout Classification Mapping table
- Modify Forescout CI Transform Map

Upgrade from ServiceNow 2.1 to 2.2

You can upgrade from ServiceNow 2.1 to 2.2 without any additional steps.

What to Do

Perform the following steps to set up this integration:

1. Verify that requirements are met. See [Requirements](#) for details.
2. Review the [Best Practices](#).
3. On the ServiceNow instance, download and install the Forescout App for Asset Management. Refer to the *Forescout App for Asset Management* installation and configuration guide.
4. Optionally, download and install the Forescout App for IT Incidents and/or the Forescout App for SOC Incidents. Refer to the *Forescout App for IT Incidents* or *Forescout App for SOC Incidents* installation and configuration guides.
5. On the Forescout platform, download and install the Forescout eyeExtend for ServiceNow product from the Forescout website: updates.forescout.com. See [Install the Module](#) for details.
6. Define a target ServiceNow instance. Assign CounterACT Appliances to it. See [Establish Connection to ServiceNow Instance](#) for details.
7. Create policies for the Forescout platform to update ServiceNow assets. See [ServiceNow Policy Templates](#).
8. When the configurations have been tested and the policies created, you are ready to start [Work with Forescout eyeExtend for ServiceNow](#).

Requirements

Verify that the following requirements are met:

- [Forescout Requirements](#)
- [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#)
- [ServiceNow Requirements](#)

Forescout Requirements

The module requires the following Forescout releases and other components:

- Forescout version 8.1 or 8.2.
- A module license for Forescout eyeExtend for ServiceNow. See [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#).

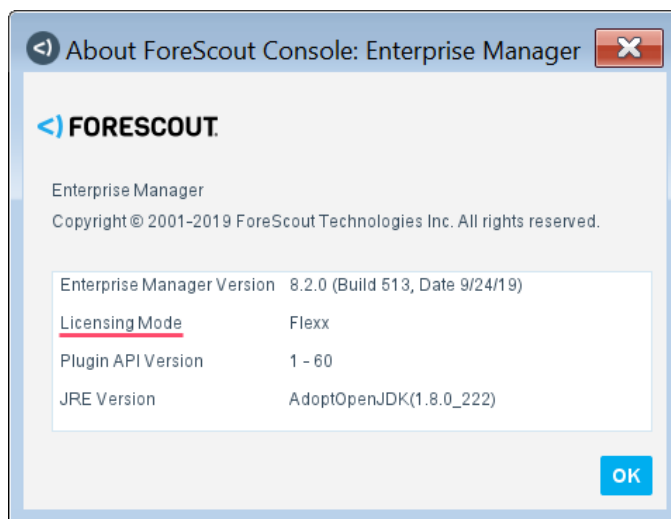
Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend product requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- [Per-Appliance Licensing Mode](#)
- [Flexx Licensing Mode](#)

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.




Per-Appliance Licensing Mode

When installing the module, you are provided with a 90-day demo license.

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your Forescout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

To continue working with the module after the demo period expires, you must purchase a permanent module license.

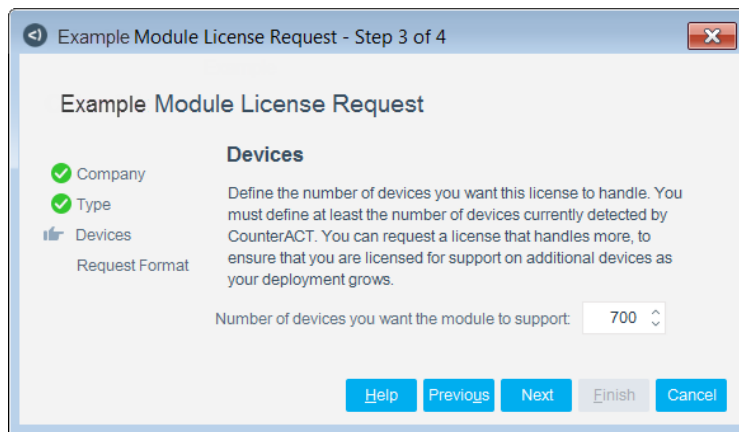
Demo license extension requests and permanent license requests are made from the Console.

 This module may have been previously packaged as a component of an Integration Module which contained additional modules. If you already installed this module as a component of an Integration Module, you can continue to use it as such. Refer to the section about module packaging in the Forescout Administration Guide for more information.

Requesting a License

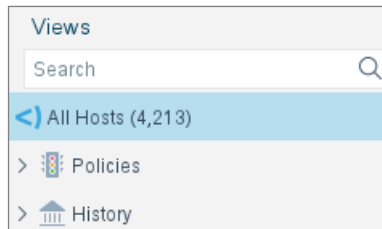
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by the Forescout platform. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

Enter this number in the **Devices** pane of the Module License Request wizard, in the Console Modules pane.



To view the number of currently detected devices:


1. Select the **Home** tab.
2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.



Flexx Licensing Mode


When you set up your Forescout deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including eyeExtend products. After the initial license file has been activated, you can update the file to add additional eyeExtend licenses or change endpoint capacity for

existing eyeExtend products. For more information on obtaining eyeExtend licenses, contact your Forescout sales representative.

 *No demo license is automatically installed during system installation.*

License entitlements are managed in the [Forescout Customer Portal](#). After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

Each eyeExtend license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each eyeExtend license varies by module but does not exceed the capacity of the Forescout eyeSight license.

 *Integration Modules, which package together groups of related licensed modules, are not supported when operating in Flexx Licensing Mode. Only eyeExtend products, packaging individual licensed modules are supported. The Open Integration Module is an eyeExtend product even though it packages more than one module.*

More License Information

For more information on eyeExtend (Extended Module) licenses:

- **Per-Appliance Licensing.** Refer to the *Forescout Administration Guide*.
- **Flexx Licensing.** Refer to the *Flexx Licensing How-to Guide*.

You can also contact your Forescout sales representative for more information.

ServiceNow Requirements

- ServiceNow Cloud Service version New York or Orlando.
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).
- Verify connectivity between the CounterACT Appliance and the target ServiceNow servers on the configured HTTPS port.

 *HTTPS is always assumed for this connection.*





- If traffic from the ServiceNow cloud instance to the Forescout platform is not allowed in a corporate firewall, a MID Server is required. Otherwise, the Forescout platform is not able to receive real-time ServiceNow properties updates, IT/SOC incidents updates, or Forescout action requests on IT/SOC incidents.

Install the Module

To install the module:

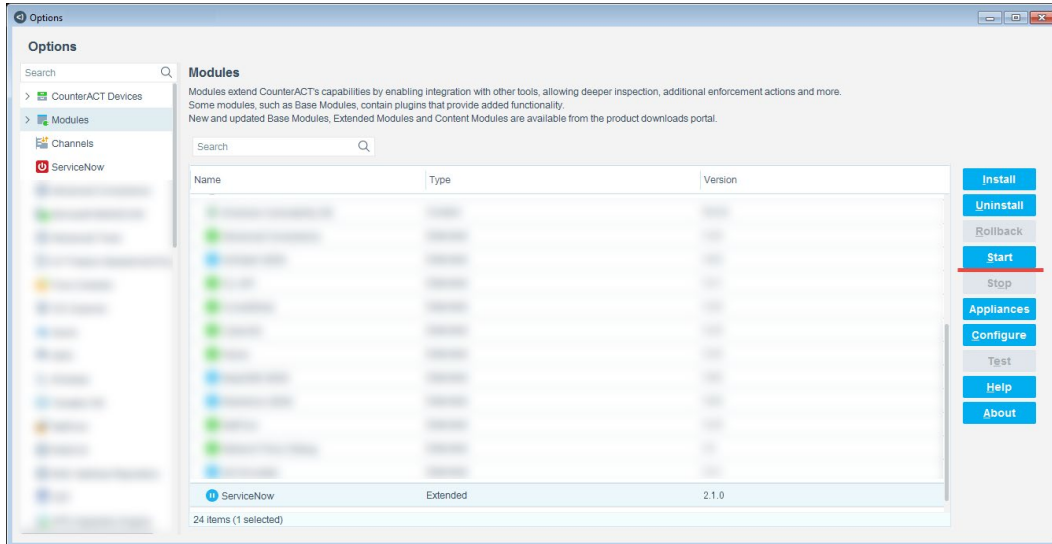
1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
 - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
 - [Customer Portal, Downloads Page](#) - **Flexx Licensing Mode**

To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download the module `.fpi` file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module `.fpi` file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.
 -  *The installation begins immediately after selecting Install and cannot be interrupted or canceled.*
 -  *In modules that contain more than one component, the installation proceeds automatically one component at a time.*
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.
 -  *Some components are not automatically started following installation.*
 -  *This module interacts with the Forescout App for Asset Management. If you install only this module, you can send information from the Forescout platform to ServiceNow. However, you must install and configure both components to work with all the features described in this document, including bidirectional interaction with ServiceNow Cloud Service.*

Start the Module

When Forescout eyeExtend for ServiceNow is initially installed, the recommendation is to start the module on the Enterprise Manager for the purpose of generating the necessary IDs, such as Tenant ID and authorization tokens. In addition, start Forescout eyeExtend for ServiceNow on the Appliances that manage the hosts and the connecting Appliance configured in the module configuration.



Configure the Module

Configure the module to ensure that the Forescout platform can communicate with the ServiceNow instance.

Perform this procedure after Forescout eyeExtend for ServiceNow is installed on your targeted CounterACT Appliance.

To complete the configuration of some of these connections, you must perform the following configuration steps on the ServiceNow instance:

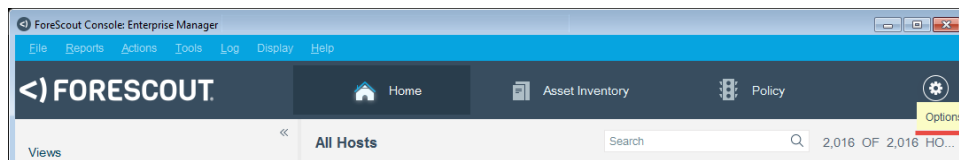
1. Set up a [ServiceNow Instance Account](#)
2. [Establish Connection to ServiceNow Instance](#)
3. [Define General Settings](#)
4. [Define Outbound Mapping](#)
5. [Define ServiceNow Tables](#)
6. [Define Host Properties](#)
7. [Define ServiceNow Lookup Properties](#)
8. [Verify the Configuration](#)

Establish Connection to ServiceNow Instance

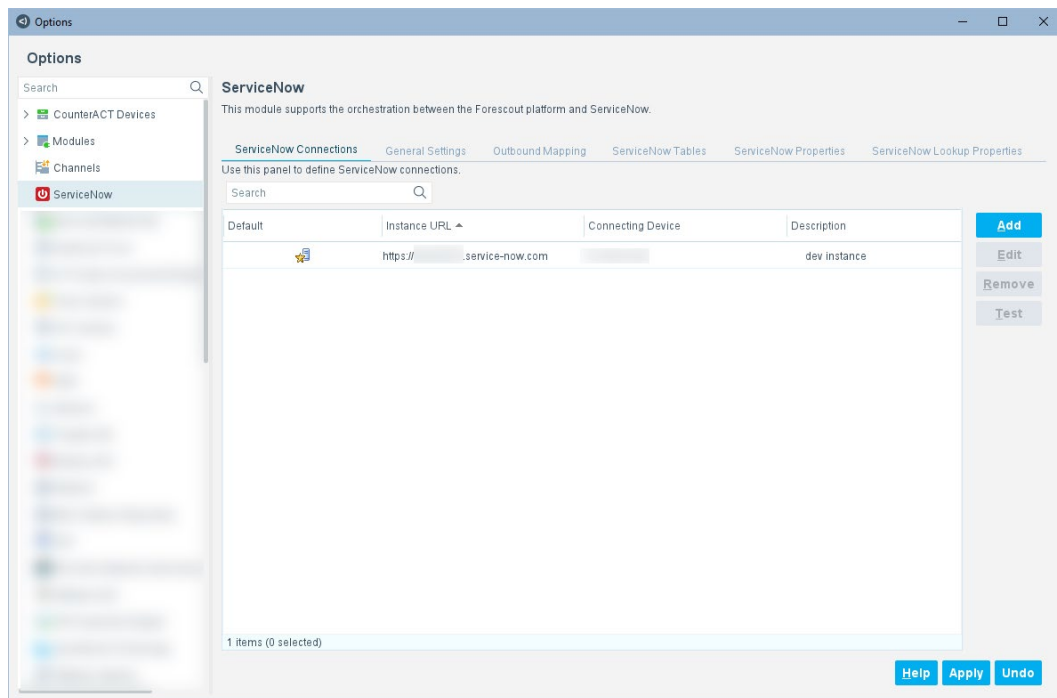
You need to map your CounterACT Appliance to a ServiceNow instance to ensure that the Forescout platform can communicate with the ServiceNow instance.

To add a ServiceNow connection:

1. In the Console, select **Options** from the Tools menu.



2. From the Options pane, select **ServiceNow**.



3. In the ServiceNow Connections tab, select **Add**.

4. Configure the connection as follows:

Instance URL	Enter the URL for your online ServiceNow account, followed by the port number. The port number is optional. If no port number is provided, the Forescout platform uses port 443. For example: servicenow.com:443.
Username	Enter the username used to access ServiceNow Cloud Service.
Password	Enter the password used to access ServiceNow Cloud Service. ServiceNow password restrictions will apply.
Verify Password	Re-enter the password to verify it.
Validate Server Certificate	<p>Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend module communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:</p> <ul style="list-style-type: none"> Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance <p>Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the <i>Forescout Administration Guide</i>.</p>
Description	(Optional) Enter text that describes the ServiceNow connection, such as a nickname. This is helpful if you have more than one ServiceNow connection.

5. Select **Next**.

6. Configure the CounterACT device assignment as follows:

Connecting CounterACT Device	<p>In an environment where more than one CounterACT device is assigned to a single ServiceNow instance, the connecting CounterACT Appliance functions as a middleman between the ServiceNow instance and the CounterACT Appliance. The connecting CounterACT Appliance forwards all queries and requests to and from the ServiceNow instance.</p> <p>Select the IP address of the connecting CounterACT device.</p>
Assign specific devices	<p>This CounterACT Appliance is assigned to a ServiceNow instance, but it does not communicate with it directly. All communication between the ServiceNow instance and its assigned CounterACT Appliance is handled by the connecting CounterACT Appliance defined for the ServiceNow instance. All the IP addresses handled by an assigned Appliance must also be handled by the ServiceNow instance the Appliance is assigned to.</p> <ol style="list-style-type: none"> 1. Select Available Devices and then select an item in the Available Devices list. 2. Select Add. The selected device will send its requests to the ServiceNow server through the connecting Appliance.
Assign all devices by default	<p>This is the connecting Appliance that CounterACT Appliances are assigned to by default if they are not explicitly assigned to another connection Appliance.</p> <p>Select Assign all devices by default to make this connecting Appliance the middleman for all CounterACT Appliances not assigned to another connecting device.</p>

For more information, see [Deployment Options](#).

7. Select **Next.**

Add ServiceNow Connection

ServiceNow Connection
Assign CounterACT Devices
Proxy
Advanced Settings

Proxy
Proxy servers are for handling communications between ServiceNow and the connecting CounterACT device. If your environment routes Internet communications through proxy servers, select Use Proxy Server and specify login information.

Use Proxy Server ☐

Proxy Server

Proxy Server Port

Proxy Server Username

Proxy Server Password

Verify Password

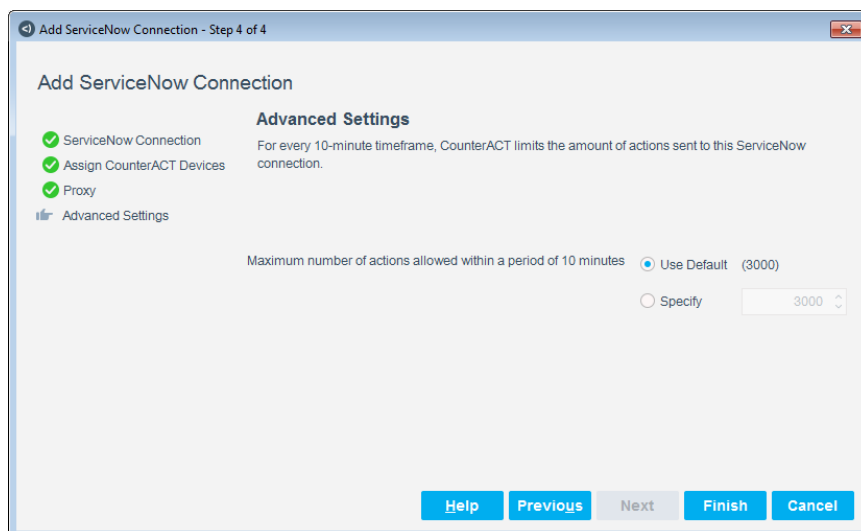
Help Previous Next Finish Cancel

8. (Optional) Configure a proxy server.

To use a proxy server with Basic Authentication, you must provide the proxy server's credentials.

Use Proxy Server	If your environment routes Internet communications through proxy servers, select this option.
Proxy Server	Enter the Fully Qualified Domain Name (FQDN) of the proxy server or the IPv4 address.
Proxy Server Port	Select the port number of the proxy server.
Proxy Server Username	Enter the administrator username used to access the proxy server.
Proxy Server Password	Enter the administrator password used to access the proxy server.
Verify Password	Re-enter the administrator password to verify it.

9. Select **Next**.



10. Configure the advanced settings as follows:

Maximum number of actions allowed within a period of 10 minutes

The Forescout platform limits the number of actions sent to this ServiceNow instance. Rate limiting prevents the ServiceNow instance from becoming inundated.

- Select **Use Default** to use the default setting of 3,000 action items per 10-minute timeframe.
- Select **Specify** and set the number of action items per 10-minute timeframe.

11. Select **Finish**. The server is displayed in the ServiceNow pane.

The best practice is to perform a **Test** after setting up a connection. See [Test ServiceNow Connection](#).

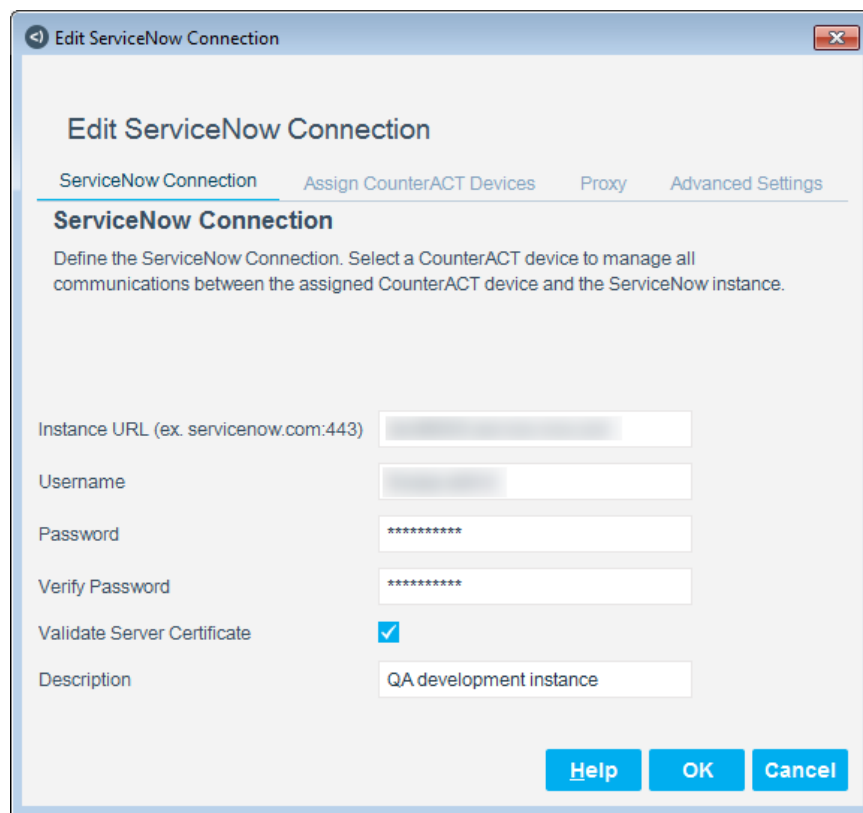
Edit ServiceNow Connection

You can change the connecting device or assign a different CounterACT Appliance to the connecting device.

To edit a ServiceNow connection:

1. In the Modules pane, select **ServiceNow**. The ServiceNow pane opens.

2. In the ServiceNow pane, select the instance and select **Edit**.



The screenshot shows a dialog box titled "Edit ServiceNow Connection" with a close button (X) in the top right corner. The dialog has four tabs: "ServiceNow Connection" (selected), "Assign CounterACT Devices", "Proxy", and "Advanced Settings". Under the "ServiceNow Connection" tab, there is a heading "ServiceNow Connection" followed by a description: "Define the ServiceNow Connection. Select a CounterACT device to manage all communications between the assigned CounterACT device and the ServiceNow instance." Below this, there are several input fields: "Instance URL (ex. servicenow.com:443)", "Username", "Password", and "Verify Password" (all masked with asterisks). There is a checkbox for "Validate Server Certificate" which is checked. A "Description" field contains the text "QA development instance". At the bottom right, there are three buttons: "Help", "OK", and "Cancel".

3. Edit the parameters in the ServiceNow Connection, Assign CounterACT Devices, Proxy, and Advanced Settings tabs.
4. Select **OK** to save your changes.

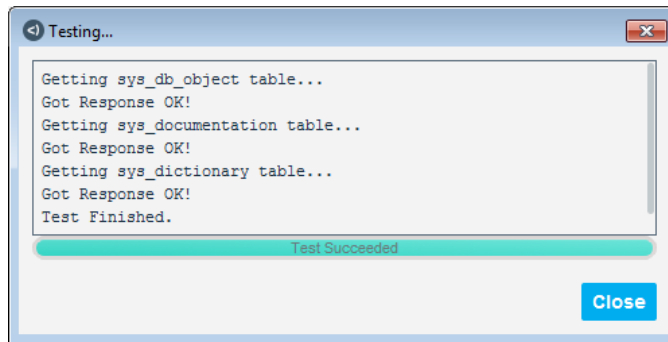
Test ServiceNow Connection

Testing the ServiceNow connection retrieves table and column information.

To test a ServiceNow connection:

1. In the Modules pane, select **ServiceNow**. The ServiceNow pane opens to the ServiceNow Connections tab.

2. Select the connection and select **Test**.



3. The status of the test is displayed. If the test failed, check your configurations and re-test. If the test passed, repeat step [2](#) for any additional connections.
4. Select **Close**.

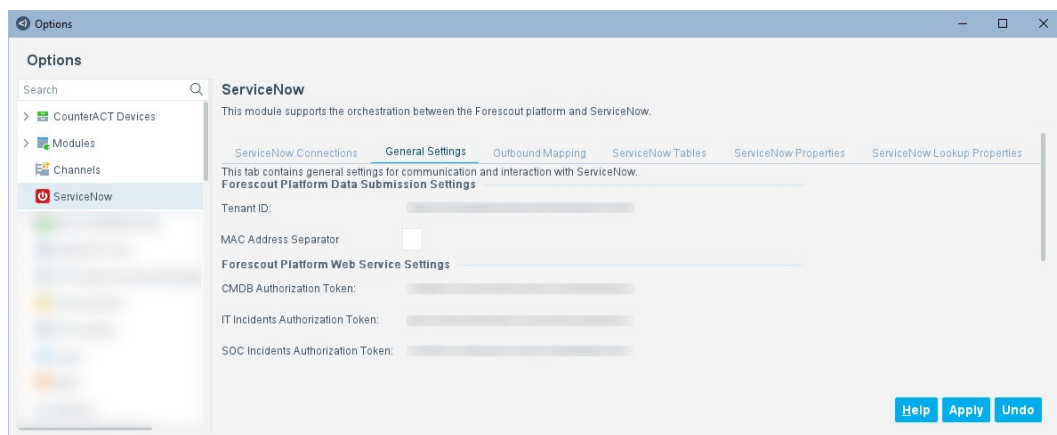
Define General Settings

Use general settings for communication and interaction with ServiceNow and to change default mappings.

After an initial installation, the Tenant ID and tokens are not available until you start Forescout eyeExtend for ServiceNow.

To define General Settings:

1. Select **Options** and select **ServiceNow**.
2. In the ServiceNow pane, select the General Settings tab.




3. Configure the general settings as follows:

Forescout Platform Data Submission Settings	<p>The settings are as follows:</p> <ul style="list-style-type: none"> ▪ Tenant ID: A unique tenant ID included in the messages the Forescout platform sends to ServiceNow. ▪ MAC Address Separator: Enter a character to use as a MAC address separator, such as a colon or a dash. The separator character is inserted between MAC addresses in both inbound and outbound requests. By default, MAC addresses from the Forescout platform do not have a separator. If MAC addresses from other sources are displayed in ServiceNow with a separator, you can configure this option for consistency.
Forescout Platform Web Service Settings	<p>The following three tokens are generated after the Forescout platform is installed and started:</p> <ul style="list-style-type: none"> ▪ CMDB Authorization Token ▪ IT Incidents Authorization Token ▪ SOC Incidents Authorization Token

4. Select **Apply**.

Define Outbound Mapping

Use outbound mapping to define the mapping between Forescout host properties and the ServiceNow database table. You can add or edit mappings. The Forescout CI Staging Table contains a default mapping that you can edit.

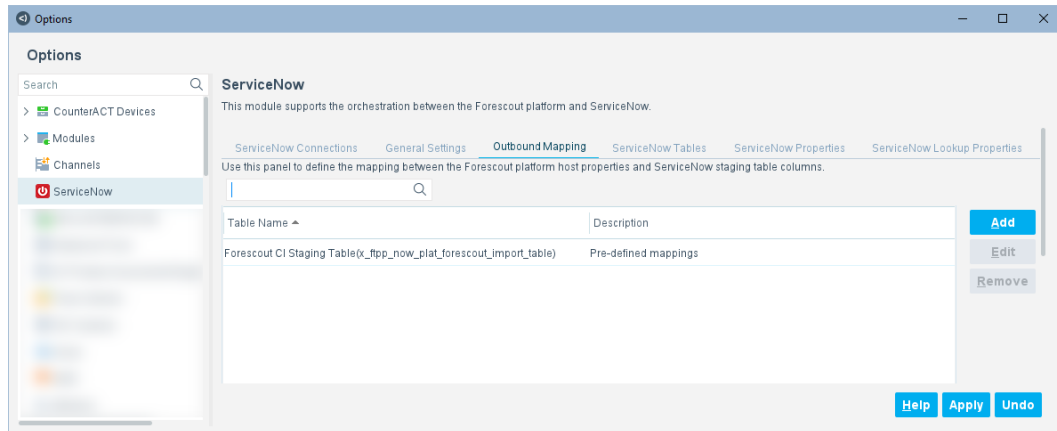
 *If there are existing policies using the Add Asset to CMDB action or the Update Asset to CMDB action, the newly configured mapping will not be selected in the policy actions. Update the existing actions when you add new fields to the outbound mapping.*

To send additional properties to ServiceNow (those not included in the pre-loaded Outbound Mapping configuration), see [Send Additional Properties](#).

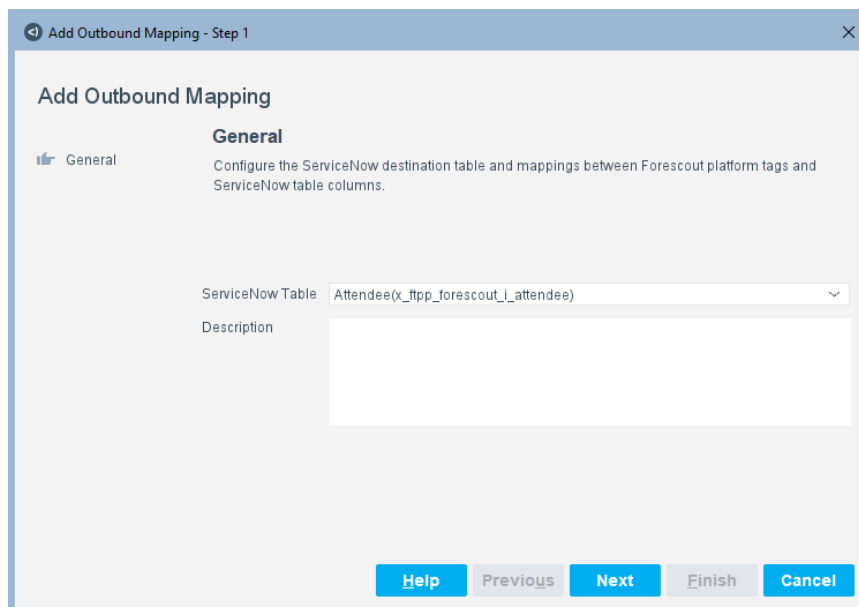
In the following procedure, you select the destination table, then add the mapping by selecting the Forescout Platform Tag as the source and the ServiceNow column as the destination.

To define Outbound Mapping:

1. Select **Options** and select **ServiceNow**.
2. In the ServiceNow pane, select the Outbound Mapping tab.



3. Select a ServiceNow database table name and select **Add**.



4. From the **ServiceNow Table** drop-down menu, select a ServiceNow database table. Optionally, add a description.


5. Select **Next**.

The screenshot shows a dialog box titled "Add Outbound Mapping - Step 2 of 2". Inside, there's a section "Add Outbound Mapping" with two tabs: "General" (selected) and "Map Data". Under "Map Data", the instruction says "Map the Forescout platform tag value to the ServiceNow column." Below this is a search bar and a table with two columns: "Forescout Platform Tag" and "ServiceNow Column". To the right of the table are buttons "Add", "Edit", and "Remove". At the bottom of the dialog are buttons "Help", "Previous", "Next", "Finish", and "Cancel".

6. Select **Add**.

The screenshot shows a dialog box titled "Add Mapping". It has two input fields: "Forescout Platform Tag" and "ServiceNow Column". To the right of each field is a "Browse" button. At the bottom of the dialog are "OK" and "Cancel" buttons.

7. Select **Browse** and select the Forescout Platform Tag (the property) and the ServiceNow column to which to map. Select **OK**.
8. Repeat steps [6](#) and [7](#) for each property.
9. In the Add Outbound Mapping pane, select **Finish**.

 *The newly created mapping will not be selected in the existing policy or the policy template. You need to select it in the policy.*

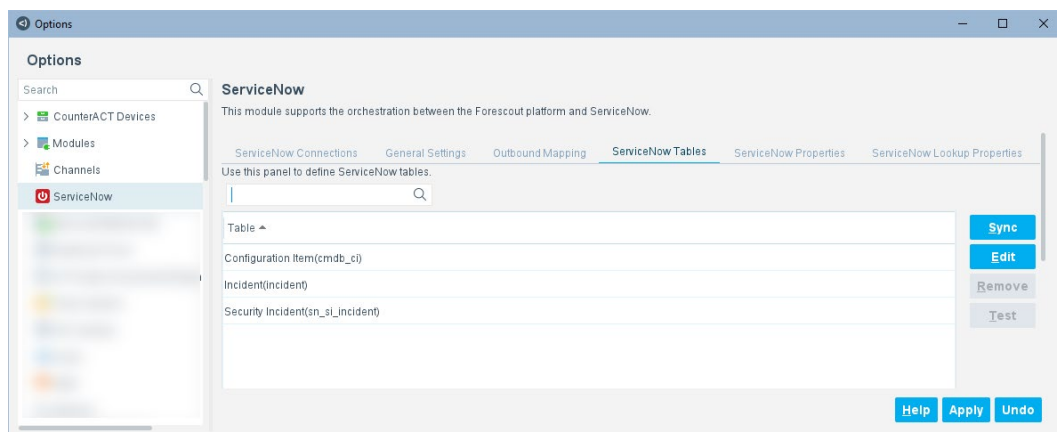
Define ServiceNow Tables

The Configuration Management Database (CMDB) is enriched and supplemented by the bi-directional data exchange between the Forescout platform and ServiceNow. The ServiceNow table definitions are optional and are used to bring properties from ServiceNow to the Forescout platform. You can create policies based on the Forescout platform properties exchanged with the ServiceNow instance. The workflow is as follows:

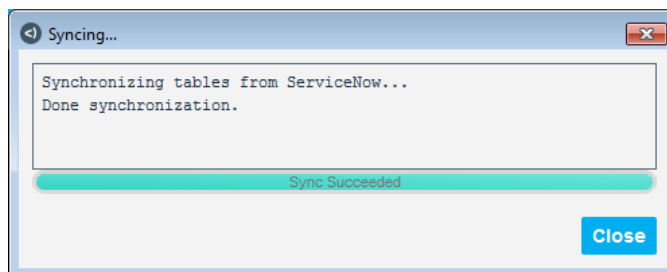
- Add host properties in the Forescout platform with values from ServiceNow table records.
- Use these properties as dynamic properties in policy decisions through custom policies. When data is updated in ServiceNow, it is sent to the Forescout platform.

To add ServiceNow tables:

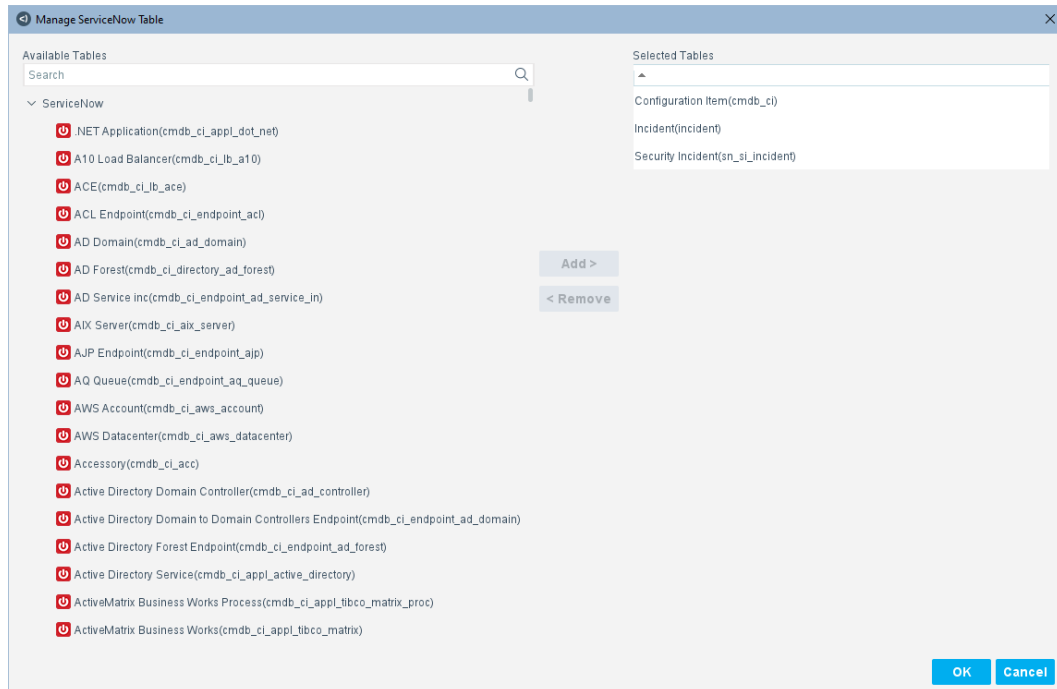
1. Select **Options** and select **ServiceNow**.
2. In the ServiceNow pane, select the ServiceNow Tables tab.



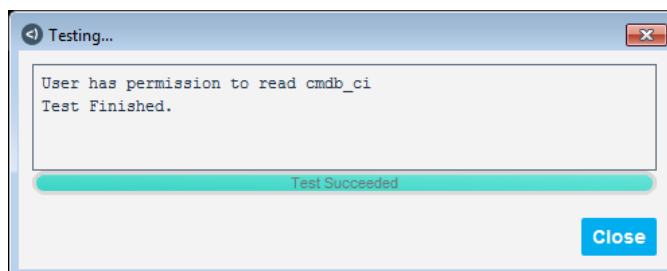
3. Select **Sync**. The tables from ServiceNow are synchronized.



4. Select **Edit**. The Forescout platform connects with the ServiceNow server and pulls in the available tables. These tables are displayed in the Manage ServiceNow Table dialog box.



5. In the Manage ServiceNow Table dialog box, you determine which ServiceNow tables you want to be able to view in the Forescout platform.
 - Select a table in the Available Tables field and then select **Add**. The table is added to the Selected Tables list. These tables will be imported into the Forescout platform.
 - To remove a table, select the table in the Selected Tables list and then select **Remove**. The table returns to the Available Tables list.
6. Select **OK**.
7. In the ServiceNow Tables tab, select a table and select **Test**. The Forescout platform checks if the user has read permission to that table.



8. Select **Close**.

Remove ServiceNow Tables

Sometimes, you might need to remove the ServiceNow tables. For example, when you no longer need to get any column values in that table, you can remove it, or when you change to using another ServiceNow instance, you need to remove the tables, select **Sync**, and add the tables again.

To remove ServiceNow Tables:

1. In the Console, select **Options** from the Tools menu.
2. In the left pane, select **ServiceNow**, and in the right pane, select the ServiceNow Tables tab.
3. Select one or more ServiceNow tables and then select **Remove**.

 *You cannot remove tables that are used by properties.*

4. When prompted for confirmation, select **OK**.

Define Host Properties

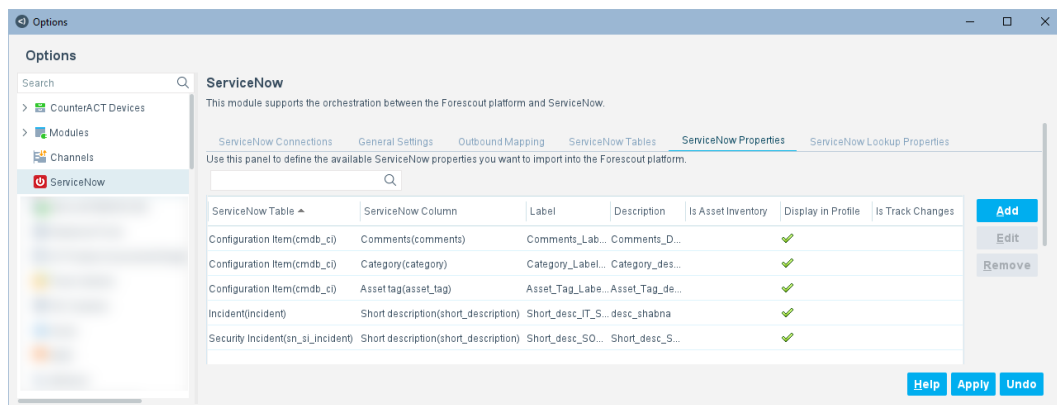
Host properties are information stored in the Forescout platform for each device identified on the network. When you work with Forescout eyeExtend for ServiceNow, you create new host properties to hold data extracted by querying the ServiceNow instance. This makes retrieved data available for use in Forescout policies.

You can create single-value properties, for example, a string property that contains the GUID of the device, or composite properties, for example, a location that contains a city and state.

Track Changes properties let you define policy conditions that identify changes in the values of custom properties. You can define track changes properties for single-value, list, or Record Exists properties that you create.

To define host properties:

1. In the ServiceNow pane, select the ServiceNow Properties tab.



2. Select **Add**.

Add Property - Step 1

Add Property

General
Define the Forescout platform host properties that hold data from external servers.

ServiceNow Table: Configuration Item(cmdb_ci)

ServiceNow Column: Location(location)

Label: Location

Tag: snow_location

Description: Location data from Snow

☐ Single property ☒ Composite property

The property is a custom table that combines several retrieved columns.

Search: []

Field Name	Type	ServiceNow Column
No items to display		

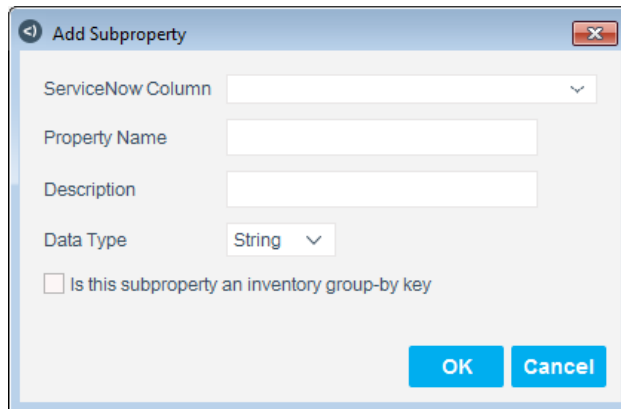
Buttons: Add, Edit, Remove, Up, Down

Buttons: Help, Previous, Next, Finish, Cancel

3. Configure the general settings as follows:

ServiceNow Table	Select a ServiceNow table.
ServiceNow Column	Select the column name within the selected ServiceNow table.
Label	Create a name to refer to the name of the ServiceNow column.
Tag	Enter a tag, which is a unique text string using ASCII characters. The Forescout platform references the property using this unique identification string.
Description	(Optional) Insert text, for example, the nickname of the host property you are creating.
Single property	Select this option to define a single property, which is a property that contains one value. Then, select String , Integer , Boolean , or Date from the Type drop-down menu.
Composite property	Select this option to define a composite property, which contains a custom table that combines several retrieved columns. It can be a group of all available types.

4. If you select **Composite property**, select **Add** to load the column list.



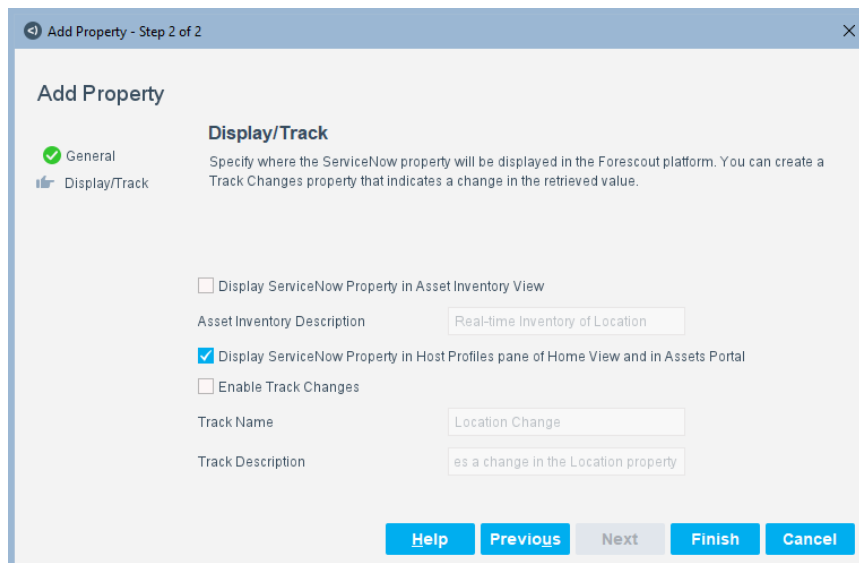
The 'Add Subproperty' dialog box contains the following fields and controls:

- ServiceNow Column:** A dropdown menu.
- Property Name:** A text input field.
- Description:** A text input field.
- Data Type:** A dropdown menu with 'String' selected.
- Is this subproperty an inventory group-by key:** An unchecked checkbox.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

5. Configure the sub-properties as follows:

ServiceNow Column	Select a ServiceNow column.
Property Name	Enter a name for the property.
Description	(Optional) Enter a description for the property.
Data Type	Select a data type (String , Integer , Boolean , or Date).
Is this subproperty an asset inventory group-by key	Select this option if this sub-property is used to generate asset inventory counts.

6. Select **OK**.
7. In the General pane, select **Next**.



The 'Add Property - Step 2 of 2' dialog box shows the 'Display/Track' configuration for a property. It includes the following elements:

- General:** Indicated by a green checkmark icon.
- Display/Track:** Indicated by a thumbs-up icon. The description states: 'Specify where the ServiceNow property will be displayed in the Forescout platform. You can create a Track Changes property that indicates a change in the retrieved value.'
- Display ServiceNow Property in Asset Inventory View:** An unchecked checkbox.
- Asset Inventory Description:** A text input field containing 'Real-time Inventory of Location'.
- Display ServiceNow Property in Host Profiles pane of Home View and in Assets Portal:** A checked checkbox.
- Enable Track Changes:** An unchecked checkbox.
- Track Name:** A text input field containing 'Location Change'.
- Track Description:** A text input field containing 'es a change in the Location property'.
- Buttons:** 'Help', 'Previous', 'Next', 'Finish', and 'Cancel' buttons at the bottom.

8. Configure the following properties:

Display ServiceNow Property in Asset Inventory View	Select this option to display this property in the Console Asset Inventory tab.
Asset Inventory Description	Enter a description of the property you want to display in the Console Asset Inventory. This description is displayed only if Display ServiceNow Property in Asset Inventory View is selected.
Display ServiceNow Property in Host Profiles Pane of Home View and in Assets Portal	Select this option to list this property in the Profiles tab of the Home view and in the Assets Portal.
Enable Track Changes	<p>The Track Changes properties let you define policy conditions that identify changes in the value of the custom properties you define. You can define track changes properties for single-value, list, or Record Exists properties.</p> <p>Select Enable Track Changes to create a second, parallel change property under the Track Changes folder of the Properties tree. Use the change property in policies to identify changes in the property values retrieved from the ServiceNow instance. This is applicable to single-value and list properties only.</p>
Track Name	The name of the item you want to track. The text entered in the Label field in the General pane populates this field and cannot be edited.
Track Description	The description of the item you want to track. The text entered in the Tag field in the General pane populates this field and cannot be edited.

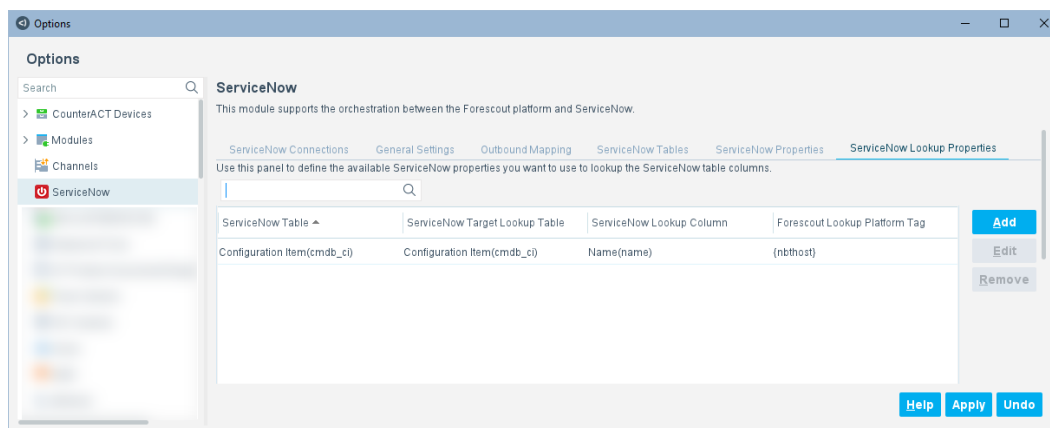
9. Select **Finish**. The property is added to the table in the Property tab.
10. Repeat steps 2 to 9 for every host property you want to create and use.
11. In the ServiceNow pane, select **Apply**. The Forescout platform saves the configuration, updates the internal database, and restarts Forescout eyeExtend for ServiceNow. It may take 1-2 minutes for the changes to take effect.
12. (Optional) Refer to *Forescout App for Asset Management* to create cross-scope access to allow the Forescout app to read the ServiceNow table in scripts.

Define ServiceNow Lookup Properties

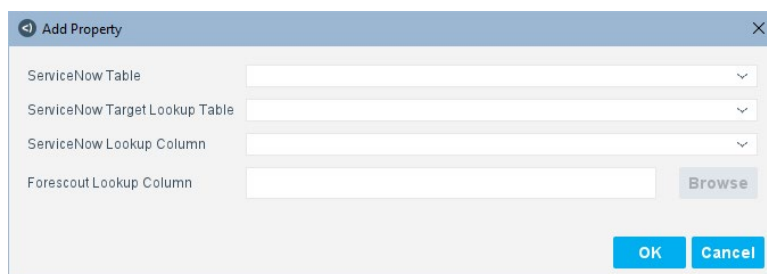
Use ServiceNow lookup properties to configure user-defined fields to query CMDB tables. Define the lookup table and lookup column using the ServiceNow Lookup Properties tab. You can use custom columns as a key to look up data from cmdb_ci tables.

To define lookup properties:

1. In the ServiceNow pane, select the ServiceNow Lookup Properties tab.



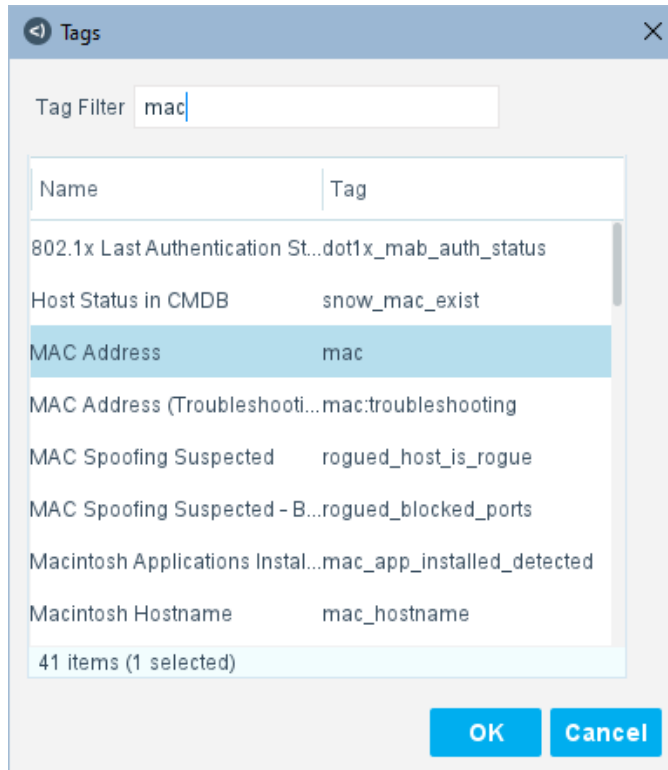
2. Select **Add**.



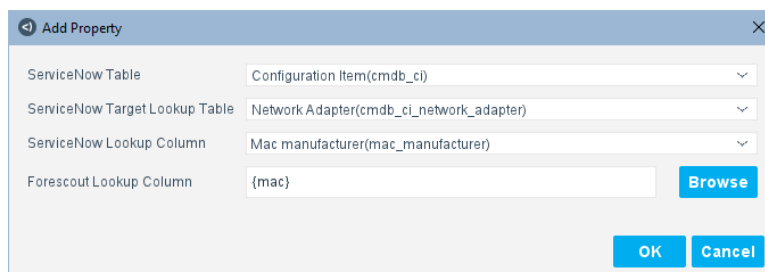
3. Configure the settings as follows:

ServiceNow Table	<p>Select from the list of tables defined in the ServiceNow Tables tab. Examples: Security Incident(sn_si_incident), Incident(incident), Configuration Item(cmdb_ci).</p> <p>Once you select a ServiceNow Table, the lists for ServiceNow Target Lookup Table and ServiceNow Lookup Column are initially populated.</p>
ServiceNow Target Lookup Table	<p>For the selected ServiceNow Table, select a target lookup table for which to query. In many cases, it is same as the ServiceNow Table.</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ Select Configuration Item if you want to query based on Name ▪ Select Network Adapter if you want to query based on IP address or MAC address
ServiceNow Lookup Column	<p>For the selected ServiceNow Target Lookup Table, select a ServiceNow lookup column from the list.</p>
Forescout Lookup Column	<p>Enter the Forescout lookup column or select Browse to search for a Forescout column. See step 4.</p> <p>This column is related to the ServiceNow Lookup Column.</p>

4. To browse for a column on the Forescout platform, select the **Browse** button. Type in a filter such as mac, then select the column name, such as MAC Address.

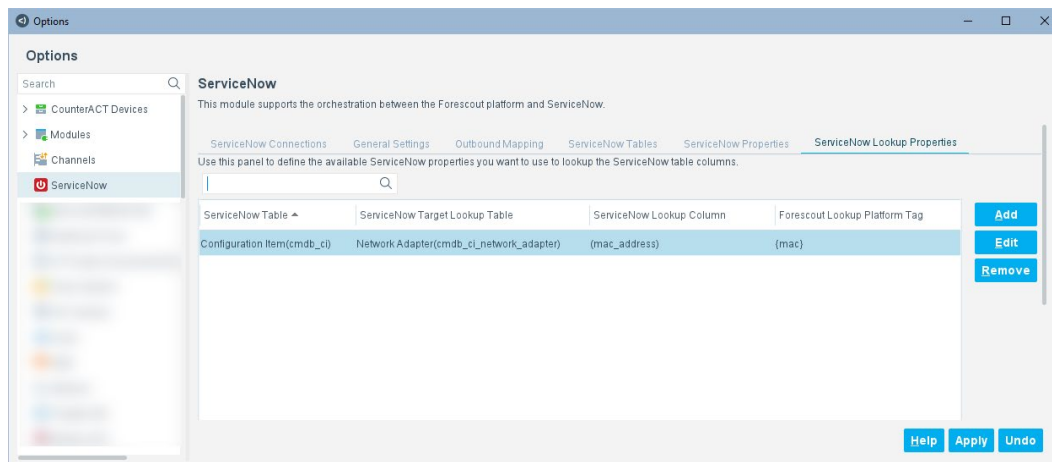


5. Select **OK** in the Tags dialog box.



If the lookup property is not defined for any of the tables listed in the Add Property dialog box, by default, the MAC address is used as the lookup.

6. Select **OK** in the Add Property dialog box.



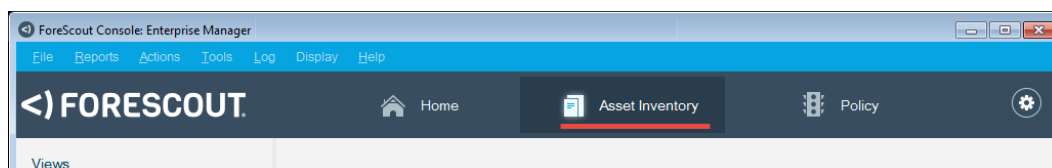
7. Select **Apply** in the ServiceNow pane.

Verify the Configuration

After configuring ForeScout eyeExtend for ServiceNow, verify that the asset information is displayed.

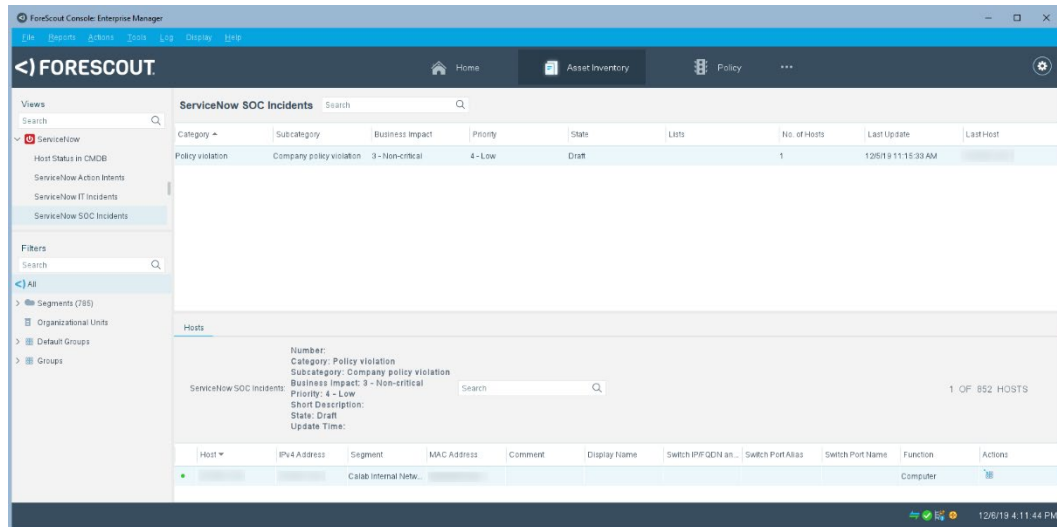
To verify the configuration:

1. In the Console, select the Asset Inventory tab.



*If you did not select **Display ServiceNow Property in Asset Inventory View** when you configured the properties, your ServiceNow properties are not displayed in the Views pane of the Asset Inventory tab.*

2. In the Views pane, expand the **ServiceNow** folder and select an item in the list to view its properties.



3. Select a row in the upper pane to view additional information in the lower pane.

Delete ServiceNow Instance

If you have multiple connecting Appliances configured to the ServiceNow instance, and one or more of them are no longer of use, they can be removed.

For example, the ServiceNow instance is connecting to Appliance A, with Appliances B and C also assigned to Appliance A. The instance is also connecting to Appliance D, with Appliance E and F also assigned to Appliance D. Later, when you want to assign Appliance D, E, and F to use Appliance A to communicate with the instance as well, you can remove the instance configuration that is connecting to Appliance D, and edit the first configuration to assign Appliances D, E, and F to Appliance A.

The process for deleting a ServiceNow Instance is as follows:

- [Remove ServiceNow Properties](#) associated with the ServiceNow tables.
- [Remove ServiceNow Tables](#).
- [Remove ServiceNow Connection](#).

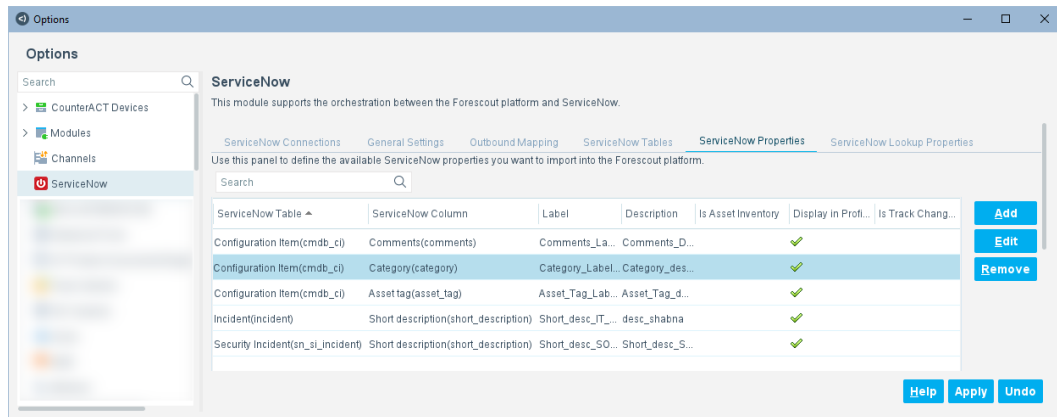
Remove ServiceNow Properties

You need to remove the ServiceNow properties before you can remove the ServiceNow tables.

To remove ServiceNow properties:

1. In the Console, select **Options** from the **Tools** menu.
2. Select **ServiceNow**. The ServiceNow pane opens to the ServiceNow Connections tab.

3. Select the ServiceNow Properties tab.
4. Select a property and then select **Remove**.



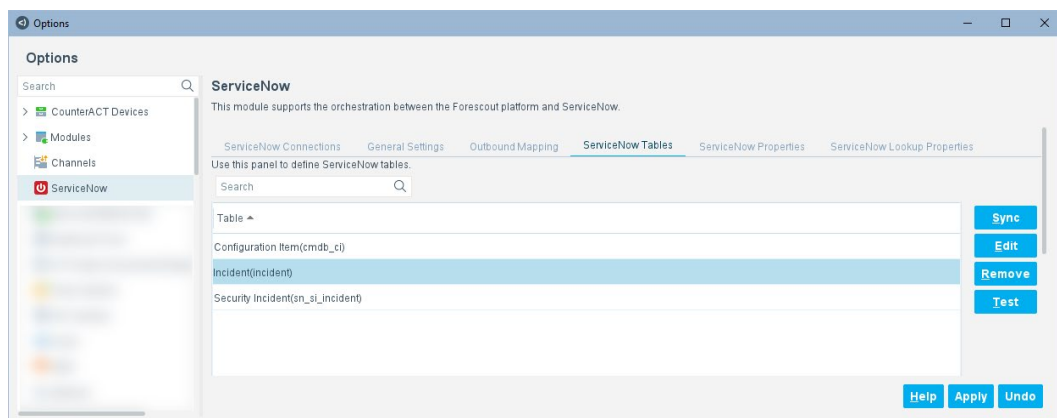
5. Select **OK**.
6. Repeat steps 3 to 5 for other properties, as necessary.
7. In the ServiceNow dialog box, select **Apply**.

Remove ServiceNow Tables

After you delete the ServiceNow properties, you can remove the ServiceNow tables from the Forescout platform.

To remove a ServiceNow table:

1. In the Console, select **Options** from the **Tools** menu.
2. Select **ServiceNow**. The ServiceNow pane opens to the ServiceNow Connections tab.
3. Select the ServiceNow Tables tab.
4. Select a table and then select **Remove**.



5. Select **OK**.
6. Repeat steps 3 to 5 for other tables, as necessary.

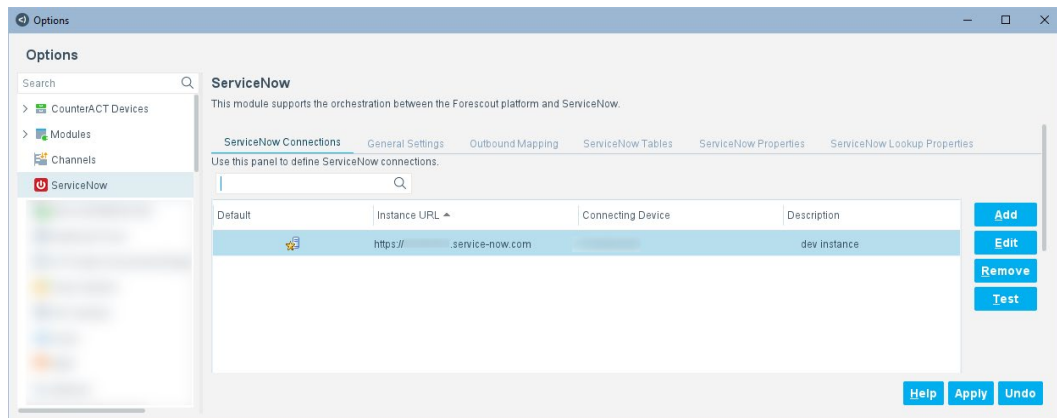
7. In the ServiceNow pane, select **Apply**.

Remove ServiceNow Connection

After you delete the ServiceNow tables, you can remove the ServiceNow instance from the Forescout platform.

To remove a ServiceNow instance:

1. In the Console, select **Options** from the **Tools** menu.
2. Select **ServiceNow**. The ServiceNow pane opens to the ServiceNow Connections tab.
3. Select an instance name and then select **Remove**.



4. Select **OK**.
5. In the ServiceNow pane, select **Apply**.

Create ServiceNow Policies

Forescout policies use a wide range of host conditions to trigger various management and remediation actions. When the conditions of the policy are met, the actions are implemented. With Forescout eyeExtend for ServiceNow, policies can include adding and updating ServiceNow tables as an action.

This section describes how to use ServiceNow policy templates to create policies to detect, manage, and remediate devices in a ServiceNow environment. Refer to the following sections:

- [Name the Policy](#)
- [How Devices Are Detected and Handled](#)
- [ServiceNow Policy Templates](#)
- [Create an Add Asset Identification Information to CMDB Policy](#)
- [Create an Update Asset Identification Information to CMDB Policy](#)
- [Create an Assign to VLAN Stage 1 Policy](#)

- [Create an Assign to VLAN Stage 2 Policy](#)
- [Create a Switch Block Stage 1 Policy](#)
- [Create a Switch Block Stage 2 Policy](#)
- [Create a Switch Block Stage 3 Policy](#)
- [Create a SecOps Ticketing Policy](#)

Name the Policy

Policy names appear in the Policy Manager, the Views pane, NAC Reports, and in other features. Precise names make working with policies and reports more efficient.

Define a unique name for the policy and enter a description. Some best practices are as follows:

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as `My_Compliance_Policy`.
- Use a descriptive name that indicates what your policy verifies and the actions to be taken.
- Ensure that the name indicates whether the policy criteria must be met or not met.
- Avoid having another policy with a similar name.

How Devices Are Detected and Handled

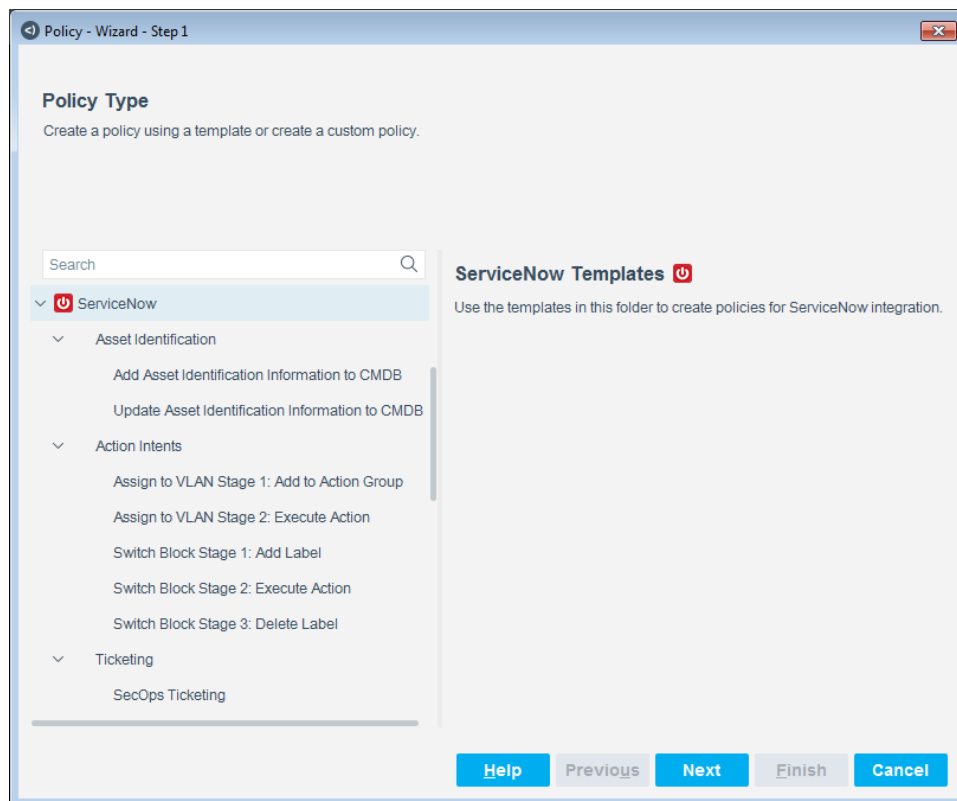
Policy rules instruct the Forescout platform how to detect and handle devices defined in the policy scope.

Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with hosts after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the host. If the host does not match the requirements of the sub-rule, it is inspected by the next rule.

ServiceNow Policy Templates

Forescout eyeExtend for ServiceNow provides policy templates for asset identification, action intents, and ticketing.



Asset Identification Templates

The following asset identification templates are provided:

Add Asset Identification Information to CMDB	<p>This policy template adds assets not found in the CMDB.</p> <p>The asset existence check compares the MAC address identified by the Forescout platform to the information in the CMDB. If the asset does not exist, the selected properties are added in the CMDB.</p> <p>The set of properties per device type is defined in the Forescout App for Asset Management.</p>
Update Asset Identification Information to CMDB	<p>This policy template updates asset properties in the CMDB, as captured by the Forescout platform.</p> <p>The asset existence check compares the MAC address identified by the Forescout platform to the information in the CMDB. If the asset exists and its property value has changed, the selected properties are updated in the CMDB.</p> <p>The set of properties per device type is defined in the Forescout App for Asset Management.</p>

Action Intents Templates

The following action intents templates are provided:

Assign to VLAN Stage 1: Add to Action group	<p>This policy template shows how to handle action requests from ServiceNow using groups. This template represents one such action, Add to Group.</p> <ul style="list-style-type: none"> ▪ The main rule captures all ServiceNow Add to Group action requests within the last hour. ▪ The first sub-rule adds an endpoint to the Assign to VLAN Action group when an Add to Group request is received from ServiceNow with an Action Parameter 1 value of VLAN. The endpoint is part of the group for one hour (by default). ▪ The second sub-rule is a catch-all, which covers other endpoints that do not match the above action request within the last hour (by default).
Assign to VLAN Stage 2: Execute Action	<p>This policy template shows how to execute the action request from ServiceNow using groups. This policy template represents one such action, Add to Group with an Action Parameter 1 value of VLAN.</p> <ul style="list-style-type: none"> ▪ The main rule looks for endpoints that belong to a specific action group. The condition is re-evaluated every eight hours (by default). ▪ The action assigns the filtered endpoints to the Guest VLAN.
Switch Block Stage 1: Add Label	<p>This policy template shows how to handle action requests from ServiceNow using labels. This policy template represents one such action, Add Label.</p> <ul style="list-style-type: none"> ▪ The main rule captures all ServiceNow Add Label action requests. ▪ The first sub-rule assigns a Switch Block label when an Add Label request is received from ServiceNow with an Action Parameter 1 value of Switch Block (by default). ▪ The second sub-rule is a catch-all, which covers other endpoints that do not match the above action request (by default).
Switch Block 2: Execute Action	<p>This policy template shows how to execute the action request from ServiceNow using labels. This template represents one such action, Add Label with an Action Parameter 1 value of Switch Block.</p> <ul style="list-style-type: none"> ▪ The main rule looks for endpoints with a specific assigned label. The condition is re-evaluated every eight hours (by default). ▪ The action executes the Switch Block action on the filtered endpoints.
Switch Block 3: Delete Label	<p>This policy template deletes the Switch Block label added by the Switch Block Stage 1: Add Label policy in order to undo the Switch Block action applied to the corresponding endpoints.</p>


Ticketing Template

The following ticketing template is provided:

SecOps Ticketing	<p>This policy template creates SOC incidents for any endpoint that is not compliant.</p>
-------------------------	---

Create an Add Asset Identification Information to CMDB Policy

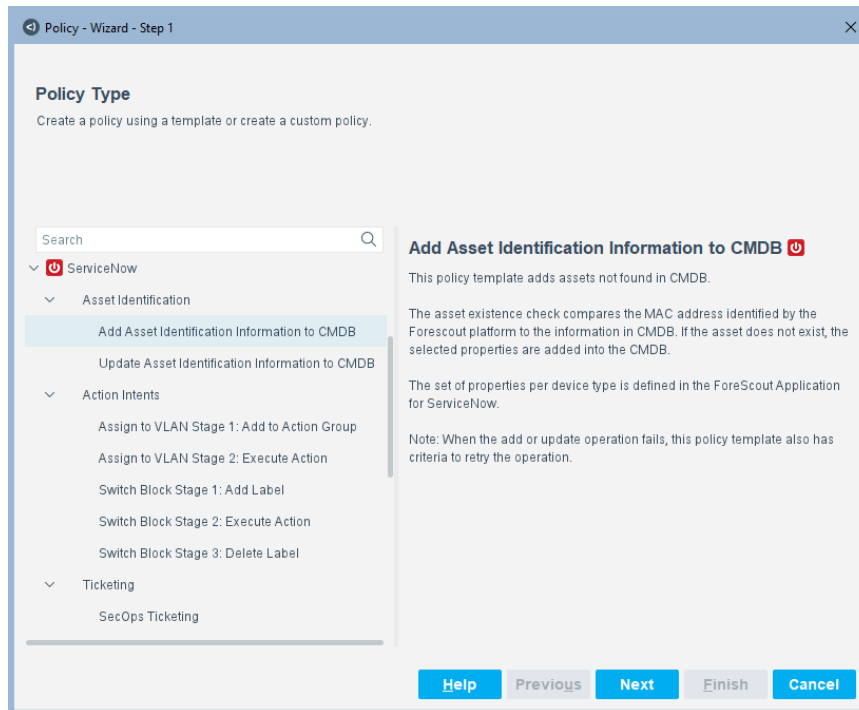
Use the Add Asset Identification Information to CMDB template to create policies that add assets not found in the CMDB. For example, if endpoint information is not in the CMDB, the Forescout platform will send it.

 *When the add or update operation fails, this policy template has criteria to retry the operation.*

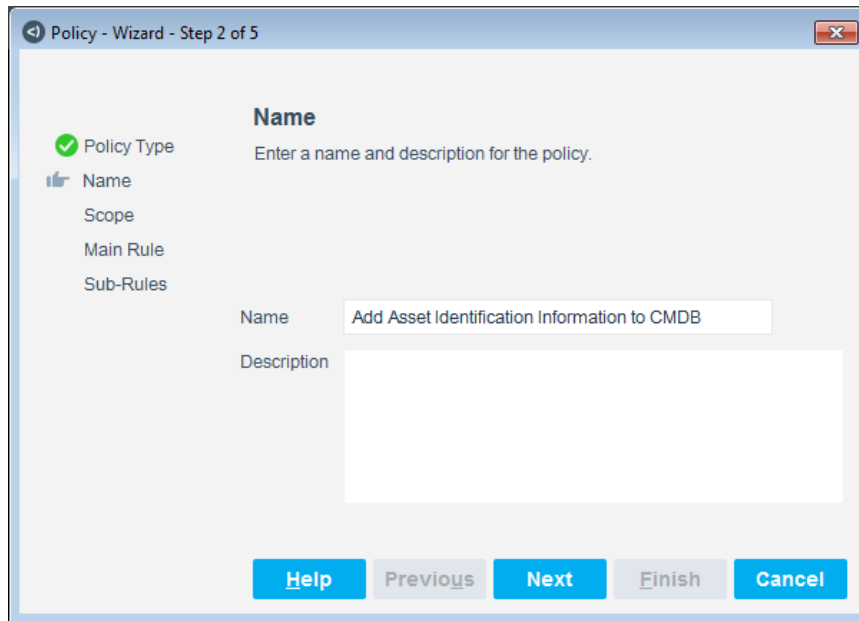
The policy adds the ServiceNow record based on your mapping of the Forescout properties to the ServiceNow tables.

To create the policy:

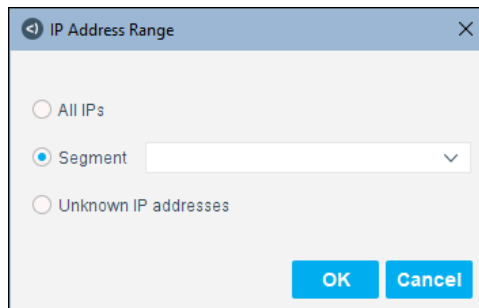
1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **ServiceNow** folder and select **Add Asset Identification Information to CMDB**.



4. Select **Next**.



5. Define a unique name for the policy and enter a description.
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The range is displayed in the Scope pane.

9. Select **Next**.

The main rule of this policy detects admission events, including:

- 802.1x admission event
- Authentication via CounterACT HTTP Login action
- AWS EC2 New Endpoint
- DHCP Request
- External host became internal
- External SecureConnector Connected
- Host Connected to a Switch Port
- IP Address Change
- Linux SecureConnector Connected
- Login to an authentication server
- Macintosh SecureConnector Connected
- New Host
- New IPv6 Address
- New VPN User
- Offline host became online
- Property administrative deletion event

- SecureConnector Connected
- VMware vSphere New Endpoint
- Windows CE HP SecureConnector Connected
- Wireless Host Connected
- WLAN lightweight AP connected

Policy - Wizard - Step 4 of 5

Main Rule

Use this screen to review policy sub-rule definitions.

Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria

Admission - DHCP Request New Host Offline host became online External host ...

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
No items to display		

Buttons: Help, Previous, Next, Finish, Cancel

10.The Condition Criteria section is populated by default. To add a condition, select **Add** in the Condition section. See [Policy Properties](#).

11.To add an action, select **Add** in the Actions section. See [Policy Actions](#).

12. Select **Next**.

Policy - Wizard - Step 5 of 5

Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Exceptions	Actions
1	Add Device to CMDB	Host Status in CMDB: Does Not Exist in CMDB AND Function: ...		
2	Last Add Attempt Failed	Host Status in CMDB: Last Add Action Failed		
3	Last Update Attempt Failed	Host Status in CMDB: Last Update Action Failed		
4	Reevaluate Device State	No Conditions		

Add
Edit
Remove
Duplicate
Up
Down

Help **Previous** **Next** **Finish** **Cancel**

- 13.** The sub-rules of the Add Asset Identification Information to CMDB policy list the items the Forescout platform is to check when applying the Main Rule. Double-click the Add Device to CMDB sub-rule to open it.

Policy: 'Add Asset Identification Information to CMDB1'-->Sub-Rule: 'Add Device to CMDB' - [X]

Name
 Name: Add Device to CMDB [Edit]
 Description: None.

Condition
 A host matches this rule if it meets the following condition:
 All criteria are True [v] [Add]
 Criteria:
 Host Status in CMDB - Does Not Exist in CMDB [Edit]
 Function - Information Technology > Networking > NAT Information Technology... [Remove]

Actions
 Actions are applied to hosts matching the above condition.

Ena...	Action	Details
<input checked="" type="checkbox"/>	Add Asset to CMDB	Add Asset to CMDB. Schedule: Star...

 [Add] [Edit] [Remove]


Advanced
 Recheck match: Every 8 hours, All admissions [Edit]
 Exceptions: None.

[Help] [OK] [Cancel]

- 14.** To add a condition, select **Add** in the Condition section. See [Policy Properties](#).
- 15.** To add an action, select **Add** in the Actions section. See [Policy Actions](#).
- 16.** Select **OK**. In the Policy dialog box, select **OK**.
- 17.** Repeat steps [13](#) to [16](#) to make changes to other sub-rules.
- 18.** In the Sub-Rules pane of the Policy Wizard, select **Finish**.
- 19.** In the Console, select **Apply** to save the policy.

Create an Update Asset Identification Information to CMDB Policy

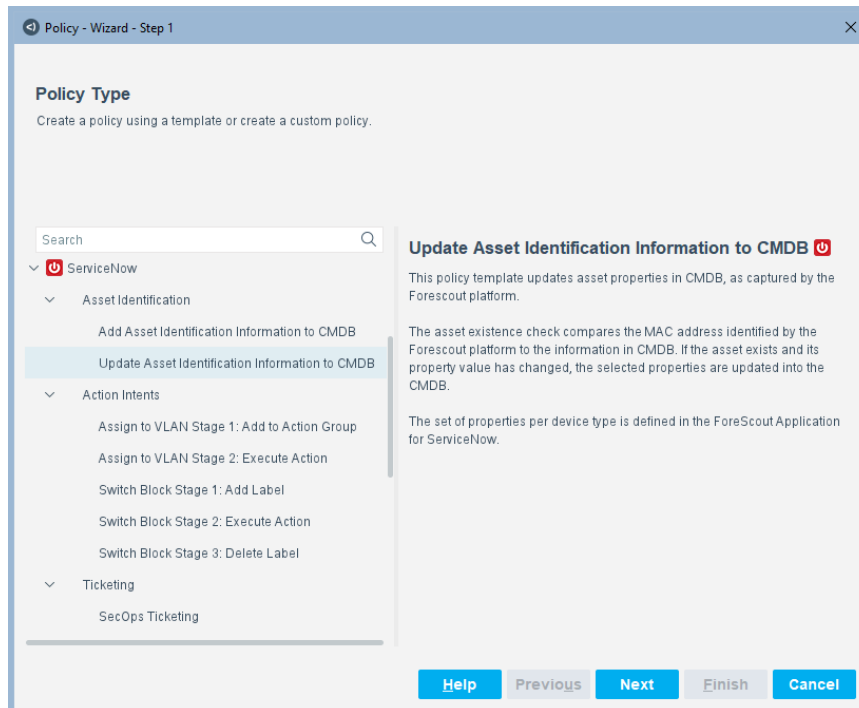
Use the Update Asset Identification Information to CMDB template to create policies that update existing asset properties in the CMDB, as captured by the Forescout platform, such as an update to endpoint information.

 *When the add or update operation fails, this policy template has criteria to retry the operation.*

The policy updates the ServiceNow record based on your mapping of the Forescout properties to the ServiceNow tables.

To create the policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **ServiceNow** folder and select **Update Asset Identification Information to CMDB**.



4. Select **Next**.

Policy - Wizard - Step 2 of 5

Name
Enter a name and description for the policy.

Policy Type (Completed)
Name (Current)
 Scope
 Main Rule
 Sub-Rules

Name: Update Asset Identification Information to CMDB
 Description: [Empty text area]

Buttons: Help, Previous, Next, Finish, Cancel

5. Define a unique name for the policy and enter a description.
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.

IP Address Range

☐ All IPs
☒ Segment [Dropdown]
☐ Unknown IP addresses

Buttons: OK, Cancel

The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The range is displayed in the Scope pane.

9. Select **Next**. The main rule of this policy detects admission events, by default there are no rules in this pane. However, you can add a rule, such as Host Status in CMDB.

Policy - Wizard - Step 4 of 5

Main Rule

Use this screen to review policy sub-rule definitions.

Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Policy Type
Name
Scope
Main Rule
Sub-Rules

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria

No items to display

Add
Edit
Remove

Actions

Actions are applied to hosts matching the above condition.

Enable Action Details

No items to display

Add
Edit
Remove

Help Previous Next Finish Cancel

10. To add a condition, select **Add** in the Condition section. See [Policy Properties](#).
11. To add an action, select **Add** in the Actions section. See [Policy Actions](#).

- 12.** Select **Next**. The sub-rules of the Update Asset Identification Information to CMDB policy list the items the Forescout platform is to check when applying the Main Rule.

The screenshot shows the 'Policy - Wizard - Step 5 of 5' window. On the left, a sidebar lists the steps: Policy Type, Name, Scope, Main Rule, and Sub-Rules (which is selected). The main area is titled 'Sub-Rules' and contains the following text: 'Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.'

Below the text is a table with the following columns: Name, Conditions, Exceptions, and Actions.

	Name	Conditions	Exceptions	Actions
1	Update Asset to CMDB	(Device interfaces on the host: Device interface...		

To the right of the table are buttons: Add, Edit, Remove, Duplicate, Up, and Down. At the bottom of the window are buttons: Help, Previous, Next, Finish, and Cancel.

13. Double-click the Update Asset to CMDB sub-rule to open it.

The screenshot shows a configuration window titled "Policy: 'Update Asset Identification Information to CMDB1'-->Sub-Rule: 'Update Asset to CMDB'". The window is divided into several sections:

- Name:** "Update Asset to CMDB". Description: "None". An "Edit" button is present.
- Condition:** "A host matches this rule if it meets the following condition:". Below this is an "Advanced view" dropdown and a table of conditions.

Not	(Criteria)	And/Or
<input type="checkbox"/>	(Device interfaces on the host - Device interface ...)	OR
<input type="checkbox"/>	(DHCP Server Change - Change: From: Any val...)	OR
<input type="checkbox"/>	(DNS Name Change - Change: From: Any value...)	OR
<input type="checkbox"/>	(Linux Manageable (SSH Direct Access) Chang...)	OR

 To the right of the table are buttons: "Add", "Edit", "Remove", "Up", and "Down".
- Actions:** "Actions are applied to hosts matching the above condition:". Below this is a table of actions.

Ena...	Action	Details
<input checked="" type="checkbox"/>	Update Asset to CMDB	Update Asset to CMDB. Schedule: ...

 To the right of the table are buttons: "Add", "Edit", and "Remove".
- Advanced:** "Recheck match" is set to "Every 8 hours, All admissions". "Exceptions" is set to "None". An "Edit" button is present.

At the bottom of the window are buttons: "Help", "OK", and "Cancel".

14. To add a condition, select **Add** in the Condition section. See [Policy Properties](#).

15. To add an action, select **Add** in the Actions section. See [Policy Actions](#).

16. Select **OK**. In the Policy dialog box, select **OK**.

17. In the Sub-Rules pane of the Policy Wizard, select **Finish**.

18. In the Console, select **Apply** to save the policy.

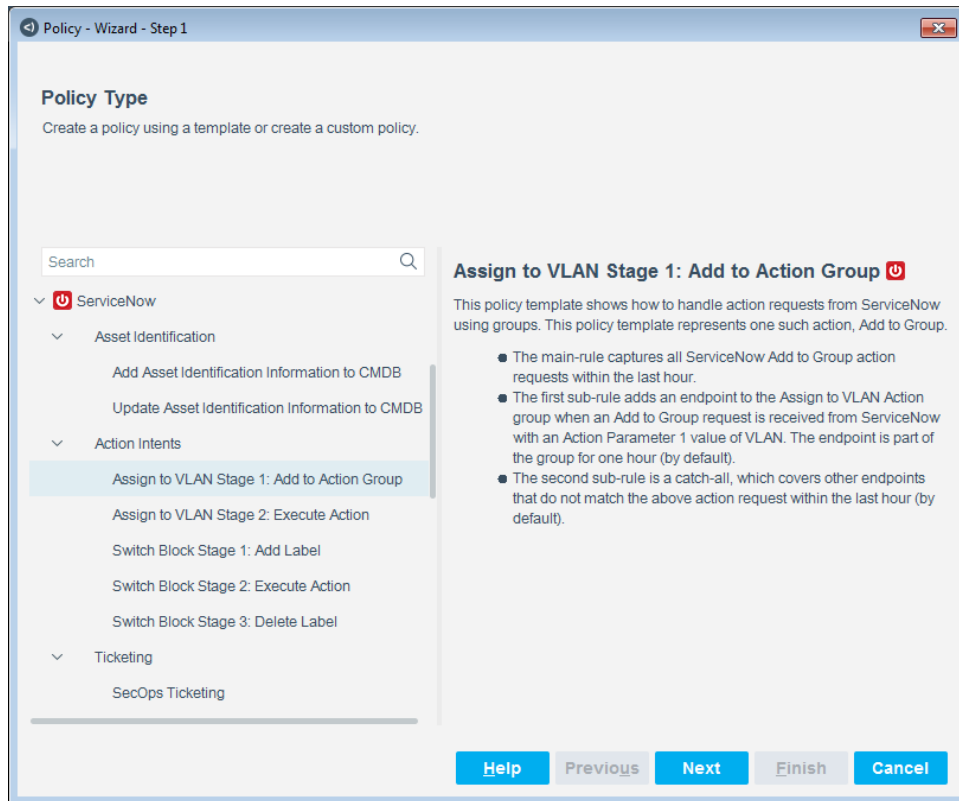
Create an Assign to VLAN Stage 1 Policy

Use the Assign to VLAN Stage 1: Add to Action group template to create policies that handle action requests from ServiceNow using groups. This template represents one such action, Add to Group.

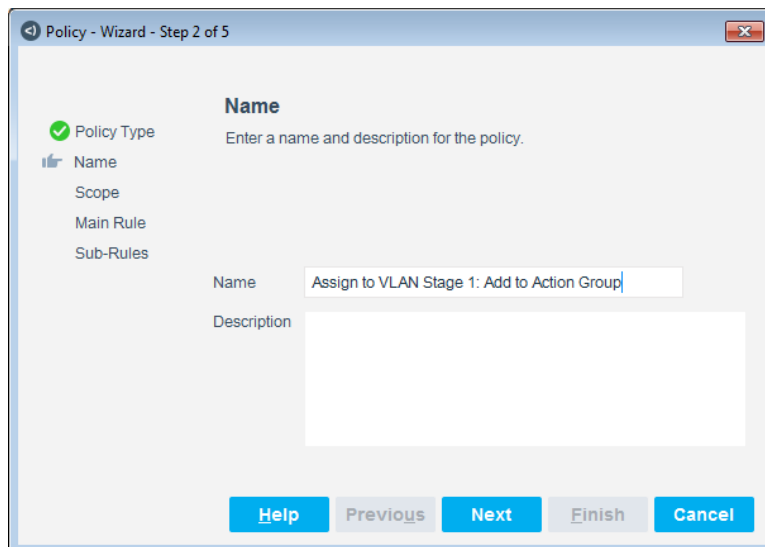
To create the policy:

1. Log in to the Console and select **Policy**.

2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **ServiceNow** folder and select **Assign to VLAN Stage 1: Add to Action group**.

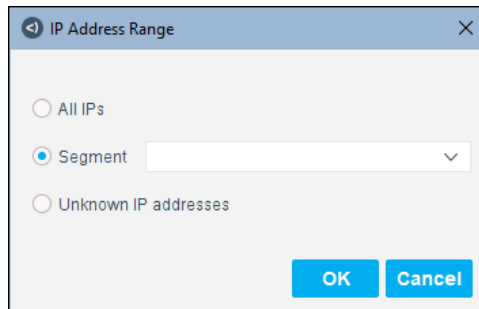


4. Select **Next**.



5. Define a unique name for the policy and enter a description.
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.

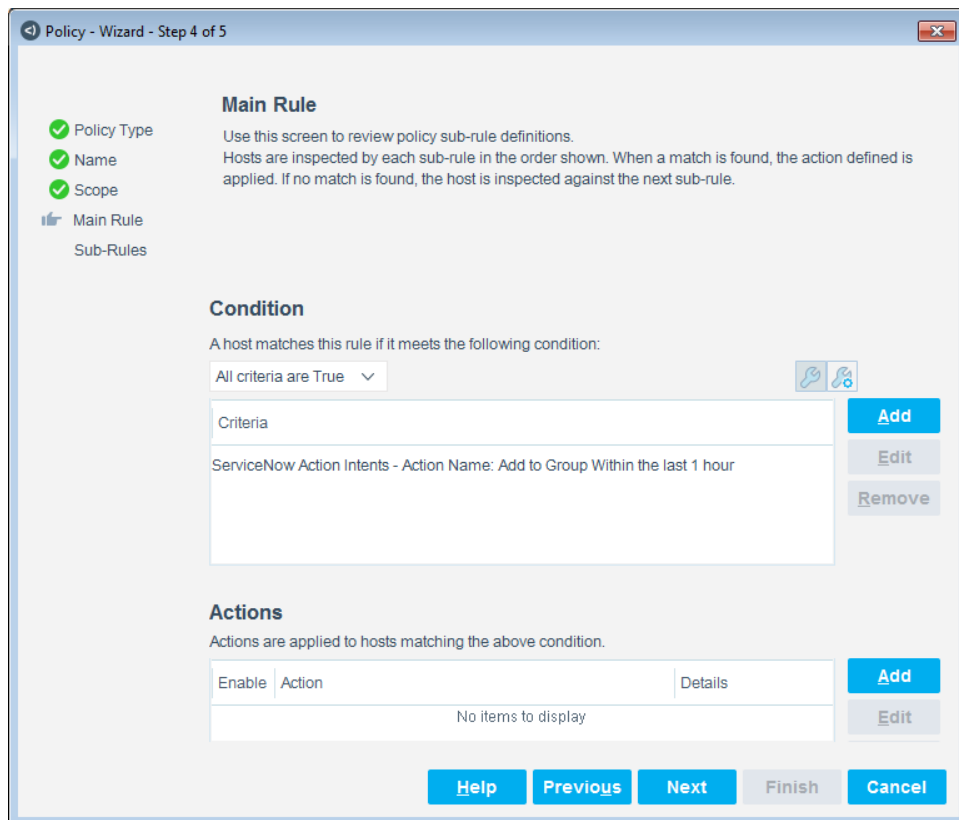
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The IP Address Range dialog box has a title bar with a back arrow, "IP Address Range", and a close button. It contains three radio button options: "All IPs", "Segment" (which is selected), and "Unknown IP addresses". The "Segment" option has a dropdown menu next to it. At the bottom right are "OK" and "Cancel" buttons.

The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
 - **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
 - **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The range is displayed in the Scope pane.
 9. Select **Next**. The main rule filters out all endpoints for which an action intent has been received with an Add to Group action in the last hour.



The "Policy - Wizard - Step 4 of 5" window shows the configuration for a main rule. On the left, a sidebar indicates that "Policy Type", "Name", and "Scope" are completed (checked), and "Main Rule" is the current step. The main area is titled "Main Rule" and includes a description: "Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule."

The "Condition" section states: "A host matches this rule if it meets the following condition:". Below this is a dropdown menu set to "All criteria are True". A list of criteria is shown, with one entry: "ServiceNow Action Intents - Action Name: Add to Group Within the last 1 hour". To the right of the list are "Add", "Edit", and "Remove" buttons.

The "Actions" section states: "Actions are applied to hosts matching the above condition:". Below this is a table with columns "Enable", "Action", and "Details". The table is currently empty, showing "No items to display". To the right of the table are "Add" and "Edit" buttons.

At the bottom of the window are navigation buttons: "Help", "Previous", "Next", "Finish", and "Cancel".

10. To add a condition, select **Add** in the Condition section. See [Policy Properties](#).
11. To add an action, select **Add** in the Actions section. See [Policy Actions](#).
12. Select **Next**. The sub-rules of the policy list the items the Forescout platform is to check when applying the Main Rule.

Policy - Wizard - Step 5 of 5

Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Exceptions	Actions
1	Assign to VLAN Action Group	ServiceNow Action Intents: Action ...		
2	All other endpoints	No Conditions		

Add **Edit** **Remove** **Duplicate** **Up** **Down**

Help **Previous** **Next** **Finish** **Cancel**

13. Double-click the Assign to VLAN Action Group sub-rule to open it.

Name
Name: Assign to VLAN Action Group
Description: None. Edit

Condition
A host matches this rule if it meets the following condition:
All criteria are True + -
Criteria
ServiceNow Action Intents - Action Name: Add to Group Action Parameter 1: ... Add Edit Remove

Actions
Actions are applied to hosts matching the above condition.

Enable	Action	Details
<input checked="" type="checkbox"/>	Add to Group	Add to Group. Schedule: Start=immediate...

Add Edit Remove

Advanced
Recheck match: Every 8 hours, All admissions
Exceptions: None. Edit

Help OK Cancel

The Assign to VLAN Action Group sub-rule filters out endpoints for which a ServiceNow action intent for an Add to Group action has been received with Action Parameter 1 value of VLAN within the last hour. If the sub-rule condition has been met, the filtered endpoints are added to the group Assign to VLAN Action. The All other endpoints sub-rule acts as a catch-all that will contain all endpoints not matching the Assign to VLAN Action Group sub-rule.

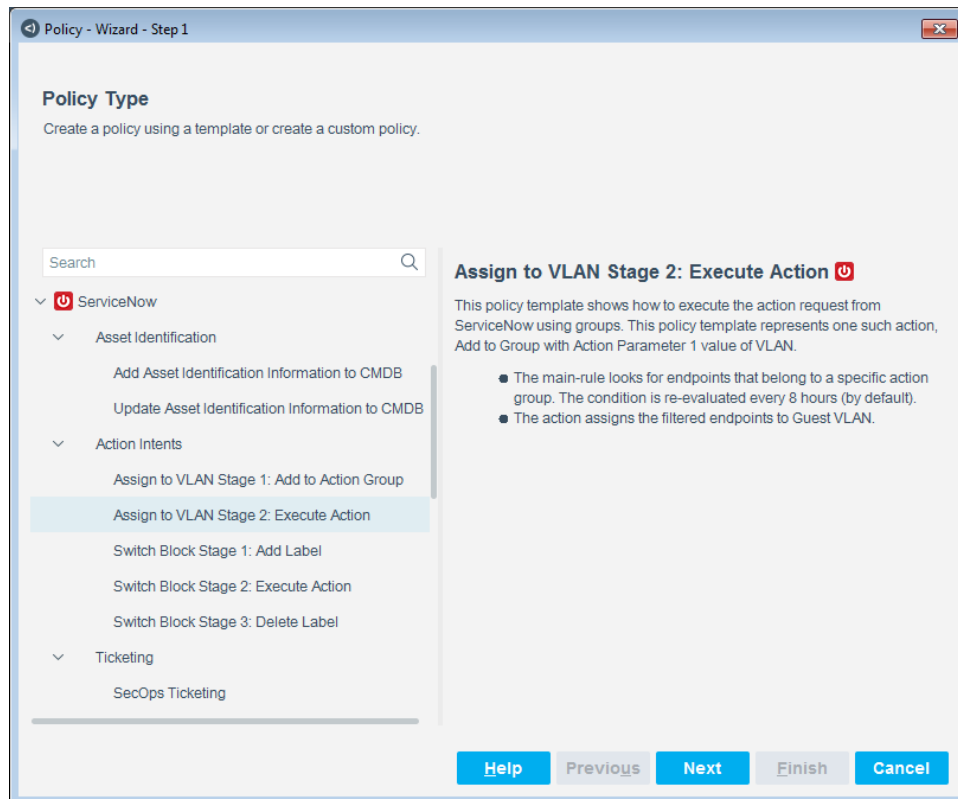
- 14.** To add a condition, select **Add** in the Condition section. See [Policy Properties](#).
- 15.** To add an action, select **Add** in the Actions section. See [Policy Actions](#).
- 16.** Select **OK** in each dialog box you open. In the Policy dialog box, select **OK**.
- 17.** In the Sub-Rules pane of the Policy Wizard, select **Finish**.
- 18.** In the Console, select **Apply** to save the policy.

Create an Assign to VLAN Stage 2 Policy

Use the Assign to VLAN Stage 2: Execute Action template to create policies that execute action requests from ServiceNow using groups. This template represents one such action, Add to Group with an Action Parameter 1 value of VLAN.

To create the policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens. Expand the **ServiceNow** folder and select **Assign to VLAN Stage 2: Execute Action**.



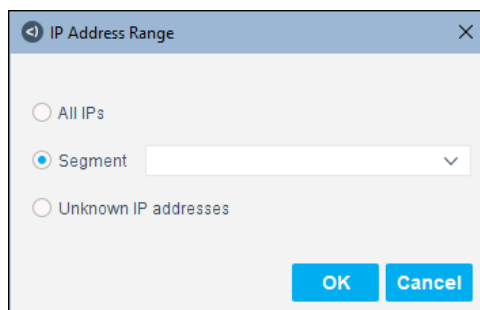
3. Select **Next**.



4. Define a unique name for the policy and enter a description.

5. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.

6. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

7. Select **OK**. The range is displayed in the Scope pane.

8. Select **Next**. The main rule filters out all endpoints that are members of the group, Assign to VLAN Action. The Assign to VLAN in the Actions section is not enabled by default but can be used to assign the filtered endpoints to Guest VLAN.

Policy - Wizard - Step 4 of 5

Main Rule
Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition
A host matches this rule if it meets the following condition:
All criteria are True

Criteria
Member of Group - Assign to VLAN Action

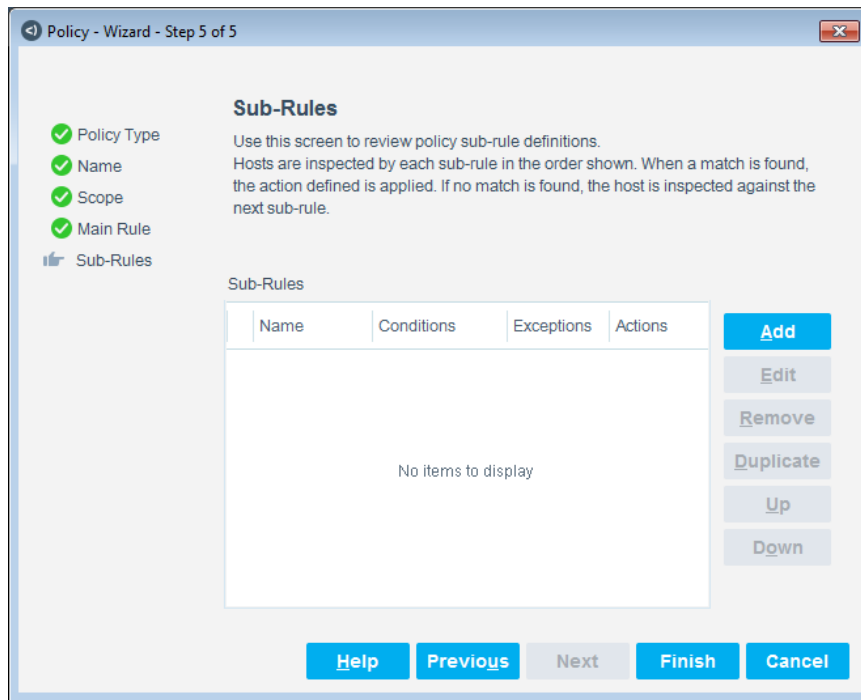
Actions
Actions are applied to hosts matching the above condition.

Enable	Action	Details
<input type="checkbox"/>	Assign to VLAN	Assign to VLAN. Schedule: Start=immed...

Buttons: Help, Previous, Next, Finish, Cancel

9. To add a condition, select **Add** in the Condition section. See [Policy Properties](#).
10. To add an action, select **Add** in the Actions section. See [Policy Actions](#).
11. Select **OK** in each dialog box you open.

- 12.** In the Main Rule pane, select **Next**. The sub-rules of the policy list the items the Forescout platform is to check when applying the Main Rule.



- 13.** In the Sub-Rules pane of the Policy Wizard, select **Finish**.

- 14.** In the Console, select **Apply** to save the policy.

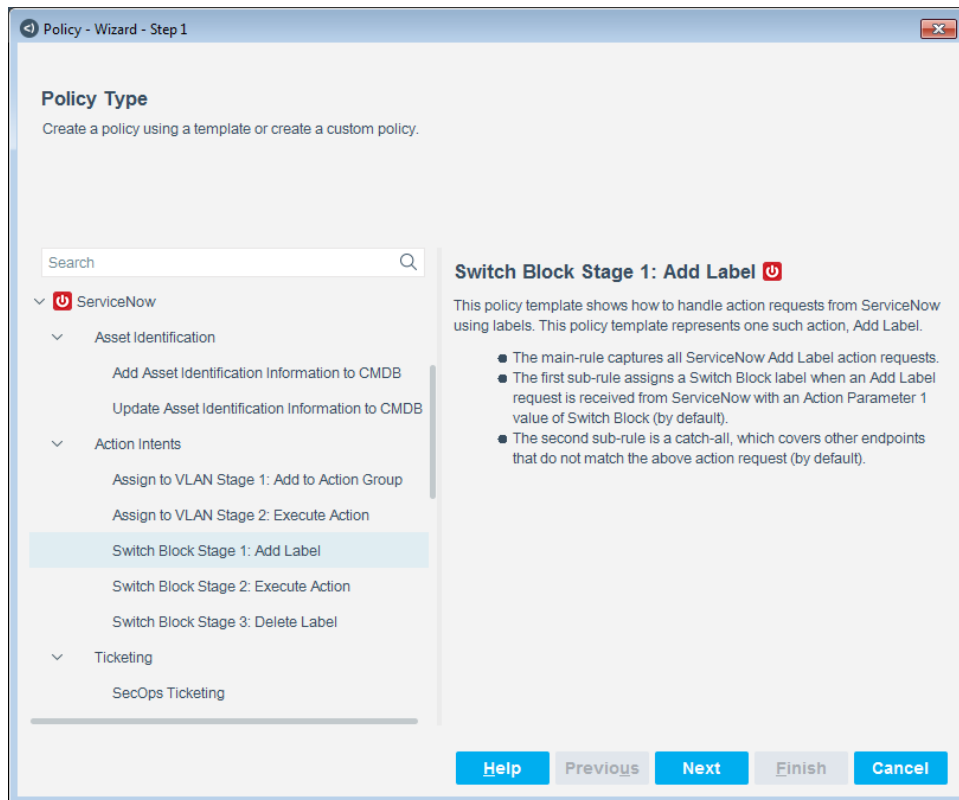
Create a Switch Block Stage 1 Policy

Use the Switch Block Stage 1: Add Label template to create policies that handle action requests from ServiceNow using labels. This policy template represents one such action, Add Label.

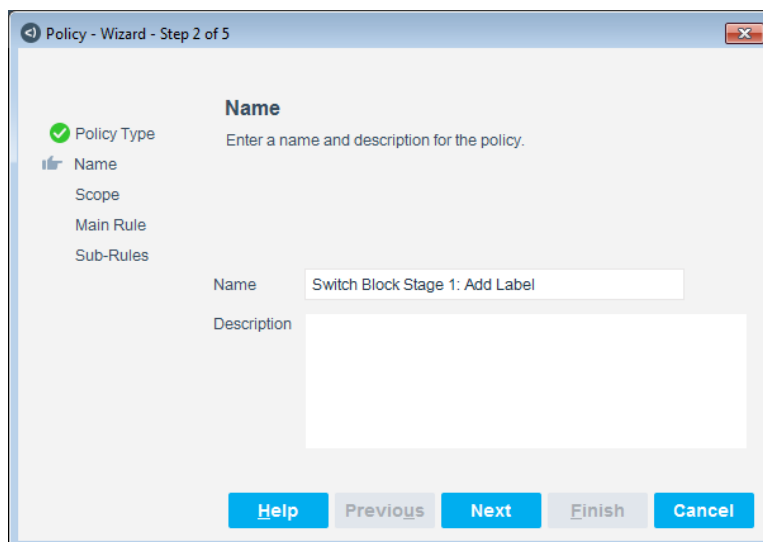
To create the policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.

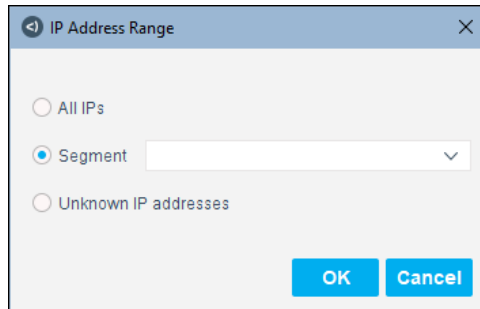
3. Expand the **ServiceNow** folder and select **Switch Block Stage 1: Add Label**.



4. Select **Next**.

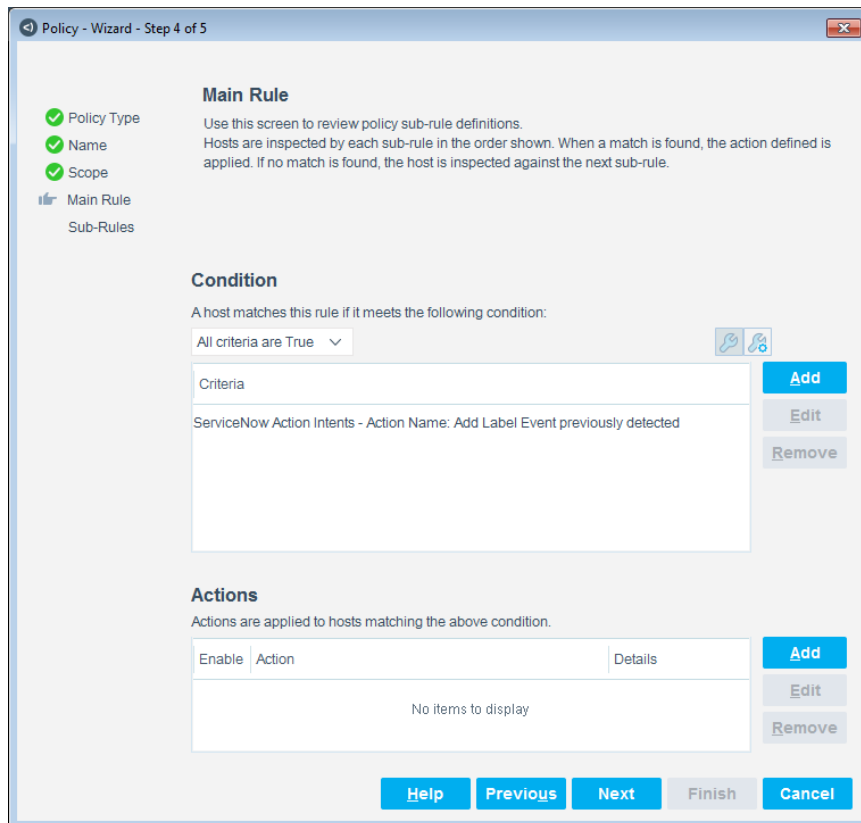


5. Define a unique name for the policy and enter a description.
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
 - **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
 - **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The range is displayed in the Scope pane.
 9. Select **Next**. The main rule filters out all endpoints for which an action intent is received with an Add Label action.



10. To add a condition, select **Add** in the Condition section. See [Policy Properties](#).

11. To add an action, select **Add** in the Actions section. See [Policy Actions](#).
12. Select **Next**. The sub-rules of the policy list the items the Forescout platform is to check when applying the Main Rule.

The screenshot shows the 'Policy - Wizard - Step 5 of 5' window. On the left, a progress bar indicates that 'Policy Type', 'Name', 'Scope', and 'Main Rule' are completed, while 'Sub-Rules' is the current step. The main area is titled 'Sub-Rules' and contains a table with two columns: 'Name' and 'Conditions'. The table lists two sub-rules: 1. 'Switch Block' with condition 'ServiceNow Action Intents: Action Name: ...' and 2. 'All other endpoints' with condition 'No Conditions'. To the right of the table are buttons for 'Add', 'Edit', 'Remove', 'Duplicate', 'Up', and 'Down'. At the bottom of the window are buttons for 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

	Name	Conditions	Exceptions	Actions
1	Switch Block	ServiceNow Action Intents: Action Name: ...		
2	All other endpoints	No Conditions		

13. Double-click the Switch Block sub-rule to open it.

The screenshot shows a dialog box titled "Policy: 'Switch Block Stage 1: Add Label1' --> Sub-Rule: 'Switch Block'". The dialog is divided into several sections:

- Name:** Shows "Name: Switch Block" and "Description: None." with an "Edit" button.
- Condition:** States "A host matches this rule if it meets the following condition:". It includes a dropdown set to "All criteria are True" and a list of criteria. One criterion is "ServiceNow Action Intents - Action Name: Add Label Action Parameter 1...". Buttons for "Add", "Edit", and "Remove" are on the right.
- Actions:** States "Actions are applied to hosts matching the above condition.". It contains a table with columns "Enable", "Action", and "Details". One action is "Add Label" with details "Add Label. Schedule: Start=immediately,...". Buttons for "Add", "Edit", and "Remove" are on the right.
- Advanced:** Shows "Recheck match: Every 8 hours, All admissions" and "Exceptions: None." with an "Edit" button.

At the bottom are "Help", "OK", and "Cancel" buttons.

The Switch Block sub-rule filters out all endpoints received with an Add Label action and Action Parameter 1 value of Switch Block. The Add Label action is not enabled by default but can be used to assign a Switch Block label for endpoints filtered by the sub-rule. The second sub-rule is a catch-all, which covers other endpoints that do not match the above action request (by default).

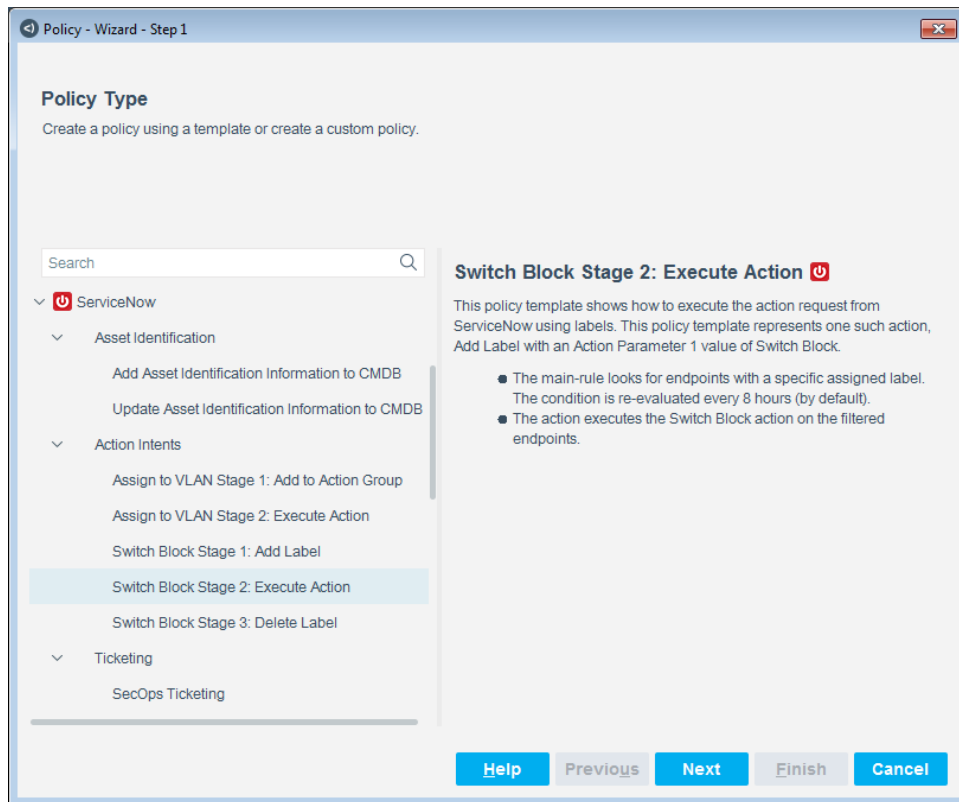
- 14.** To add a condition, select **Add** in the Condition section. See [Policy Properties](#).
- 15.** To add an action, select **Add** in the Actions section. See [Policy Actions](#).
- 16.** Select **OK** in each dialog box you open. In the Policy dialog box, select **OK**.
- 17.** In the Sub-Rules pane of the Policy Wizard, select **Finish**.
- 18.** In the Console, select **Apply** to save the policy.

Create a Switch Block Stage 2 Policy

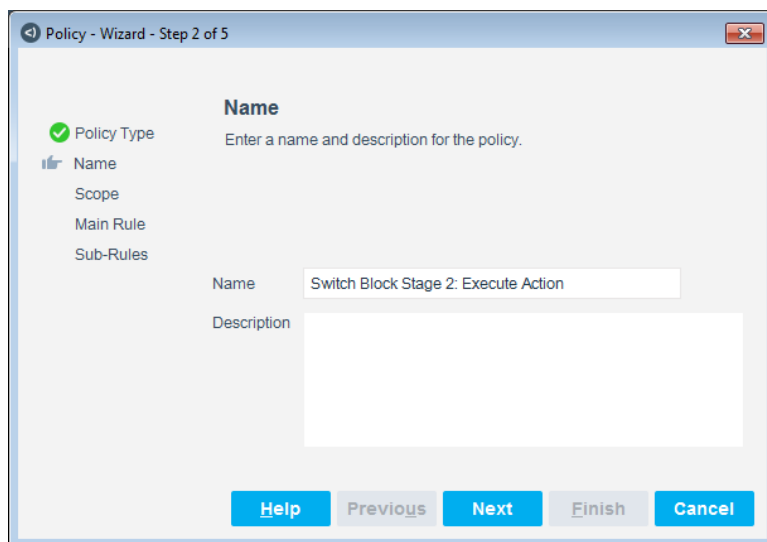
Use the Switch Block Stage 2: Execute Action template to create policies that execute the action request from ServiceNow using labels. This template represents one such action, Add Label with an Action Parameter 1 value of Switch Block.

To create the policy:

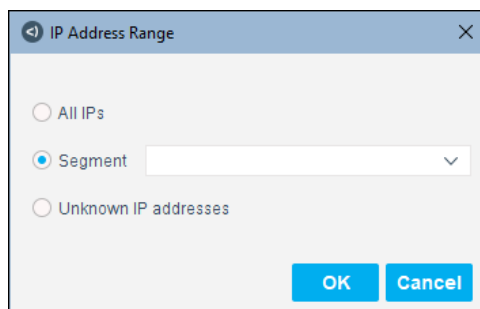
1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **ServiceNow** folder and select **Switch Block Stage 2: Execute Action**.



4. Select **Next**.



5. Define a unique name for the policy and enter a description.
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
 - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
 - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The range is displayed in the Scope pane.

9. Select **Next**. The main rule filters out all endpoints that contain an Assigned Label of Switch Block. The Switch Block in the Actions section is not enabled by default but can be used to turn off the switch port for endpoints filtered out by the main rule.

Policy - Wizard - Step 4 of 5

Main Rule

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Policy Type
Name
Scope
Main Rule
Sub-Rules

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria

Assigned Label - Contains Switch Block Event previously detected

Add
Edit
Remove

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
<input type="checkbox"/>	Switch Block	Switch Block. Schedule: Start=immediately...

Add
Edit
Remove

Help Previous Next Finish Cancel

10. To add a condition, select **Add** in the Condition section. See [Policy Properties](#).
11. To add an action, select **Add** in the Actions section. See [Policy Actions](#).
12. Select **OK** in each dialog box you open.

- 13.** In the Main Rule pane, select **Next**. The sub-rules of the policy list the items the Forescout platform is to check when applying the Main Rule.

Policy - Wizard - Step 5 of 5

Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Name	Conditions	Exceptions	Actions
No items to display			

Buttons: Add, Edit, Remove, Duplicate, Up, Down

Navigation: Help, Previous, Next, Finish, Cancel

- 14.** In the Sub-Rules pane of the Policy Wizard, select **Finish**.

- 15.** In the Console, select **Apply** to save the policy.

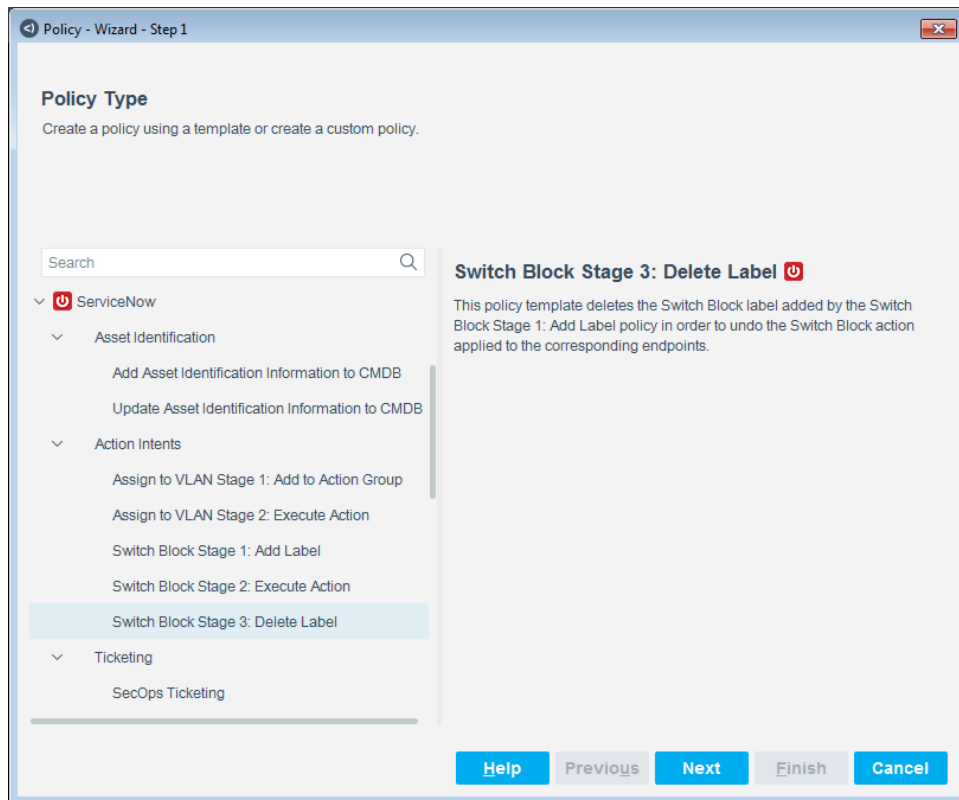
Create a Switch Block Stage 3 Policy

Use the Switch Block Stage 3: Delete Label template to create policies that delete the Switch Block label added by the Switch Block Stage 1: Add Label policy in order to undo the Switch Block action applied to the corresponding endpoints.

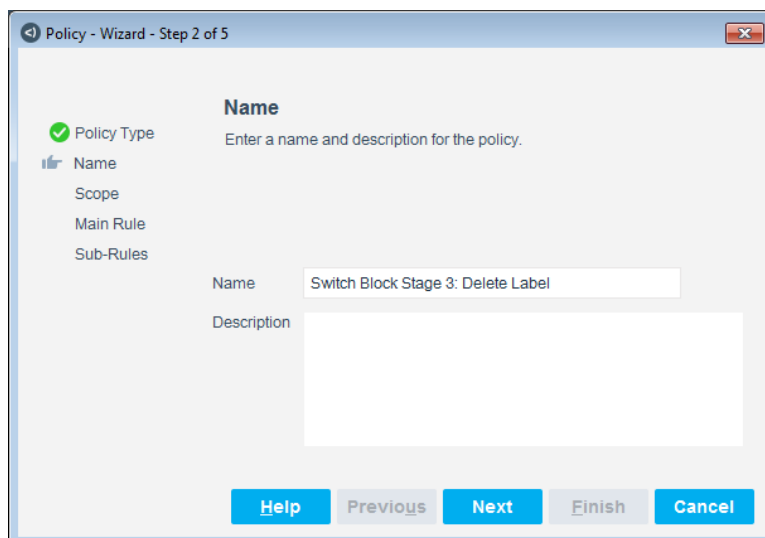
To create the policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.

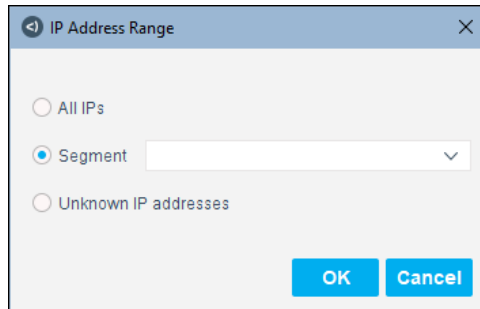
- Expand the **ServiceNow** folder and select **Switch Block Stage 3: Delete Label**.



- Select **Next**.



- Define a unique name for the policy and enter a description.
- Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
- Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The range is displayed in the Scope pane.

9. Select **Next**. The main rule filters out all endpoints for which an action intent has been received with a Delete Label action and Action Parameter 1 value of Switch Block. The Delete Label action is not enabled by default but can be used to delete the Switch Block label for endpoints filtered by the sub-rule.

Policy - Wizard - Step 4 of 5

Main Rule

Use this screen to review policy sub-rule definitions.

Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria	Add	Edit	Remove
ServiceNow Action Intents - Action Name: Delete Label Action Parameter...			

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details	Add	Edit	Remove
<input type="checkbox"/>	Delete Label	Delete Label. Schedule: Start=immediately...			

Buttons: Help, Previous, Next, Finish, Cancel

10. To add a condition, select **Add** in the Condition section. See [Policy Properties](#).
11. To add an action, select **Add** in the Actions section. See [Policy Actions](#).
12. Select **OK** in each dialog box you open.

- 13.** In the Main Rule pane, select **Next**. The sub-rules of the policy list the items the Forescout platform is to check when applying the Main Rule.

The screenshot shows the 'Policy - Wizard - Step 5 of 5' window. On the left, a sidebar lists steps: Policy Type, Name, Scope, Main Rule, and Sub-Rules (selected). The main area is titled 'Sub-Rules' and contains instructions: 'Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.' Below this is a table with columns: Name, Conditions, Exceptions, and Actions. The table is empty, displaying 'No items to display'. To the right of the table are buttons: Add, Edit, Remove, Duplicate, Up, and Down. At the bottom of the window are buttons: Help, Previous, Next, Finish, and Cancel.

- 14.** In the Sub-Rules pane of the Policy Wizard, select **Finish**.

- 15.** Select **Apply** to save the policy.

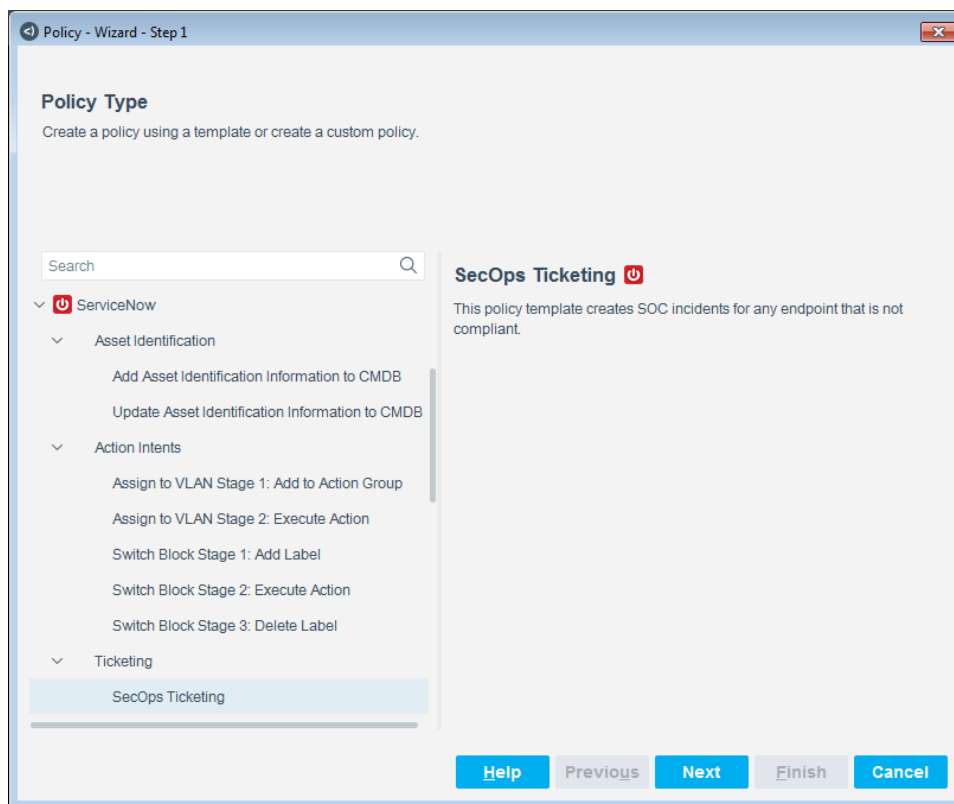
Create a SecOps Ticketing Policy

Use the SecOps Ticketing template to create policies that create SOC incidents for an endpoint that is not compliant.

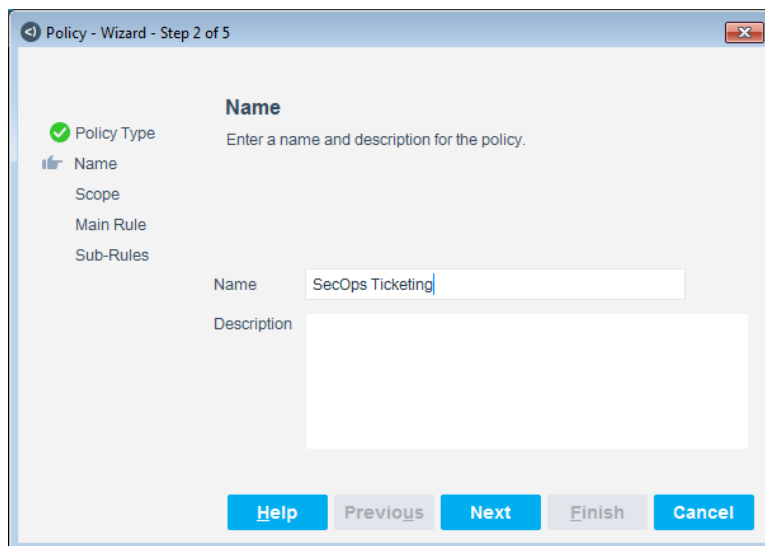
To create the policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.

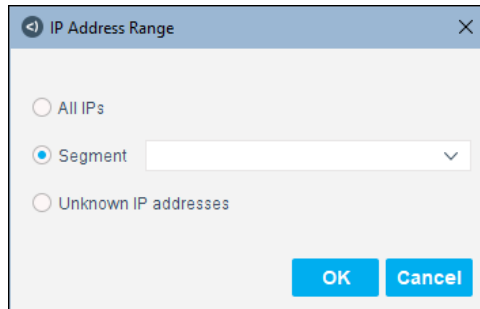
3. Expand the **ServiceNow** folder and select **SecOps Ticketing**.



4. Select **Next**.



5. Define a unique name for the policy and enter a description.
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The range is displayed in the Scope pane.

9. Select **Next**. The main rule filters out endpoints that are not compliant. The Create SOC Incident in the Actions section is not enabled by default but can be used to open SOC incidents on ServiceNow for endpoints filtered by the main rule.

Policy - Wizard - Step 4 of 5

☒ Policy Type
☒ Name
☒ Scope
☒ Main Rule
☐ Sub-Rules

Main Rule

Use this screen to review policy sub-rule definitions. Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria	
Compliance Status - Not Compliant	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>

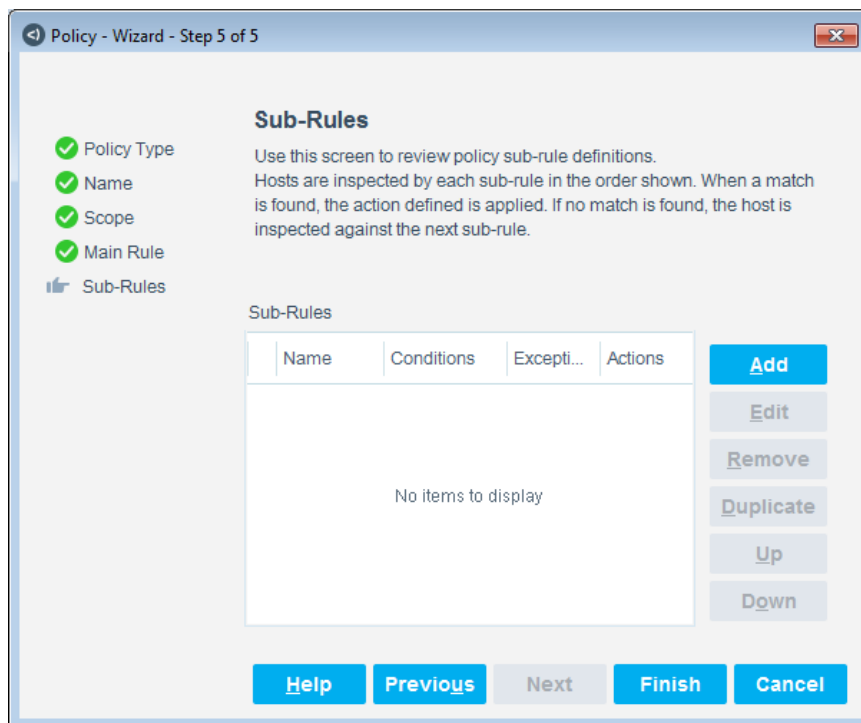
Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details	
<input type="checkbox"/>	Create SOC Incident	Create SOC Incident ...	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>

10. To add a condition, select **Add** in the Condition section. See [Policy Properties](#).
11. To add an action, select **Add** in the Actions section. See [Policy Actions](#).
12. Select **OK** in each dialog box.

- 13.** In the Main Rule pane, select **Next**. The sub-rules of the policy list the items the Forescout platform is to check when applying the Main Rule.



- 14.** In the Sub-Rules pane of the Policy Wizard, select **Finish**.

- 15.** In the Console, select **Apply** to save the policy.

Create Custom ServiceNow Policies

Forescout policies contain a series of rules. Each rule includes:

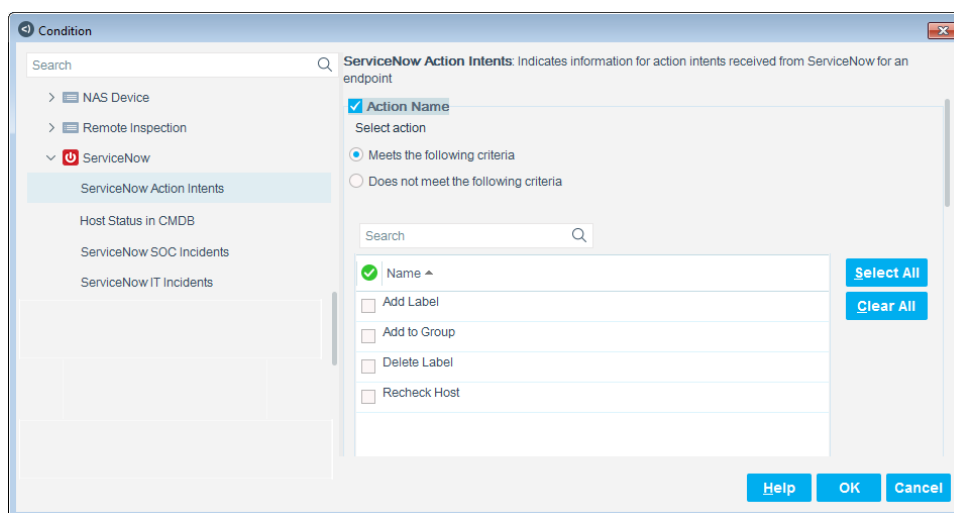
- Conditions based on host property values. The Forescout platform detects hosts with property values that match the conditions of the rule. Several conditions based on different properties can be combined using Boolean logic.
- Actions can be applied to hosts that match the conditions of the rule.

To create a custom policy:

1. In the Console, select **Policy**. The Policy Manager opens.
2. Select **Add** to create a policy, then select **Custom**, or select **Help** for more information about working with policies.

Policy Properties

In addition to the bundled Forescout properties and actions available for adding and updating ServiceNow tables, you can work with policy properties to create custom policies. These items are available when you install the module.



To access properties:

1. In the Policy Conditions dialog box, search for and expand the **ServiceNow** folder in the Properties tree.

The following properties are available:

ServiceNow Action Intents	<p>Indicates information for action intents received from ServiceNow for an endpoint.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Action Name: The action name. The possible values are: Add Label, Add to Group, Delete Label, and Recheck host. ▪ Action Parameter 1: The action parameter 1. ▪ Action Parameter 2: The action parameter 2.
Host Status in CMDB	<p>Indicates the host status in the ServiceNow CMDB. It checks whether the MAC address on a device exists in the ServiceNow CMDB. When the scheduled add/update occurs, the ServiceNow app also sends back existence to the Forescout platform.</p> <p>The possible values are: Does Not Exist in CMDB, Exists in CMDB, Last Add Action Failed, and Last Update Action Failed.</p>

ServiceNow SOC Incidents	<p>Indicates SOC incidents created by the Forescout platform.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> Number: The incident number. Category: The category. Subcategory: The sub-category. Business Impact: The business impact. Priority: The priority. Short Description: The short description. State: The state. Update Time: The time of the update received on the Forescout platform.
ServiceNow IT Incidents	<p>Indicates IT incidents created by the Forescout platform.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> Number: The incident number. Category: The category. Subcategory: The sub-category. Impact: The impact. Urgency: The urgency. Priority: The priority. Short Description: The short description. State: The state. Update Time: The time of the update received on the Forescout platform.

 To learn about ServiceNow properties, see [Define Host Properties](#).

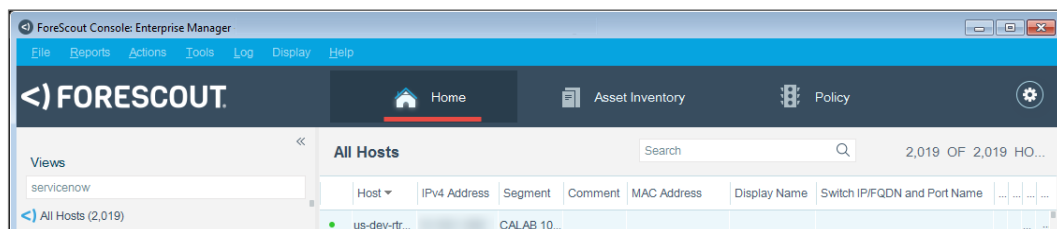
2. Select the property you want and select **OK**.

Policy Actions

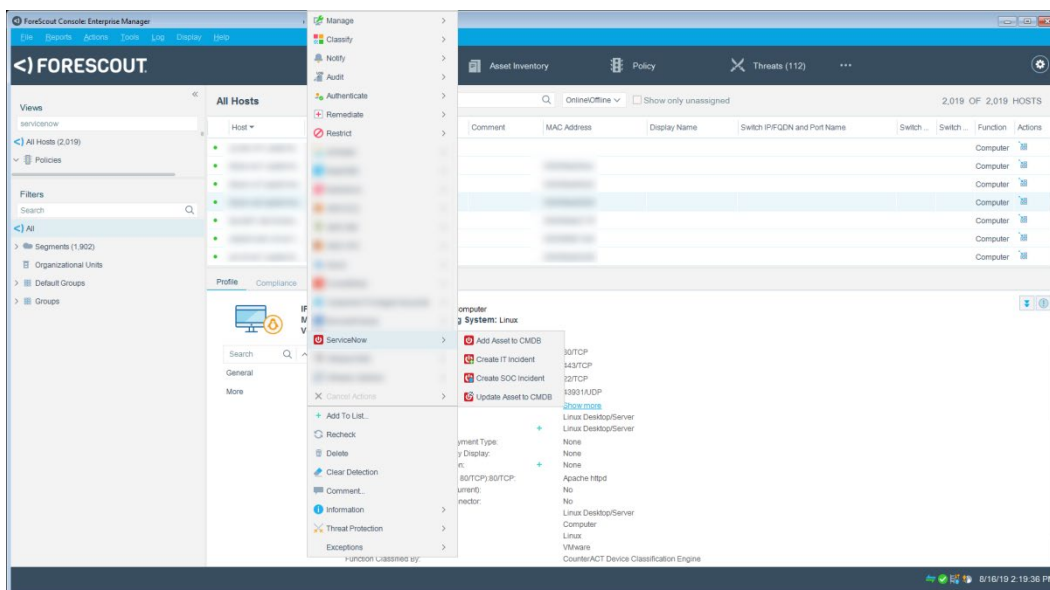
In addition to the bundled Forescout properties and actions available for adding and updating ServiceNow tables, you can work with policy actions to create customized policies. For example, a policy action could be used to apply mappings between existing properties on the Forescout platform and ServiceNow table columns.

To access the ServiceNow actions:

1. Log in to the Console, select **Home**, and select **All Hosts**.



2. In the All Hosts pane, select a host entry.
3. Right-click an endpoint and select **ServiceNow**.



4. Expand the ServiceNow folder in the Actions tree. The following actions are available:

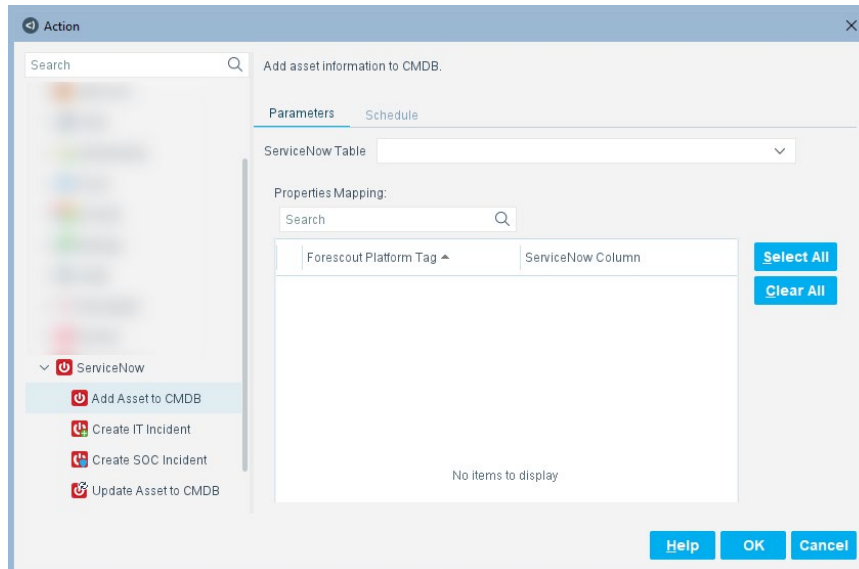
Add Asset to CMDB	Adds asset information to CMDB.
Create IT Incident	Creates an IT incident in ServiceNow with domain name, host name, IP address, MAC address, and description.
Create SOC Incident	Creates a SOC incident in ServiceNow with domain name, host name, IP address, MAC address, and description.
Update Asset to CMDB	Updates asset information in the CMDB.

Add or Update Asset to CMDB

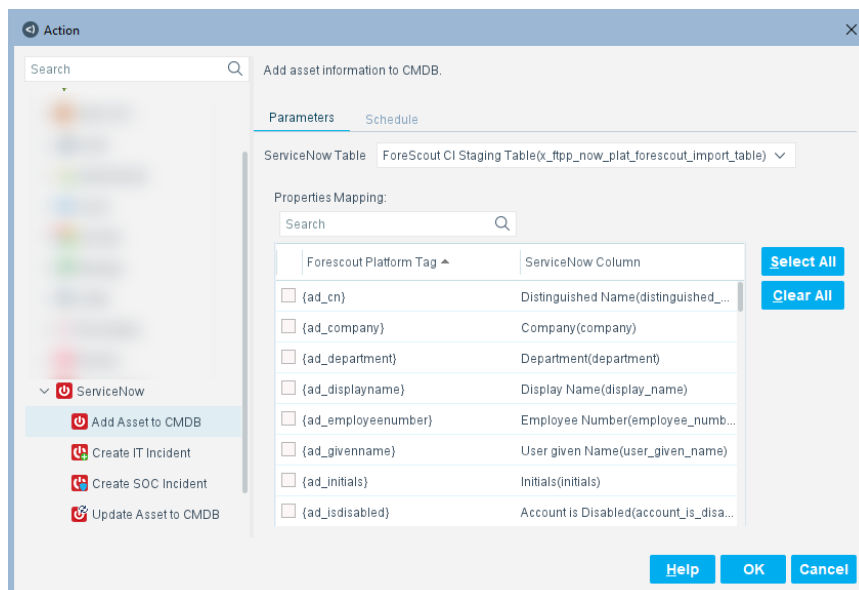
Use this action to add or update an asset to the CMDB.

To use the Add/Update Asset to CMDB action:

1. In the Actions tree, select **ServiceNow** and then select **Add Asset to CMDB** or **Update Asset to CMDB**.



2. Use the Parameters tab to map properties in the Forescout platform to ServiceNow table columns, for use within the scope of the selected policy. Select a table from the **ServiceNow Table** drop-down menu. The available tags for that table are listed.



3. Select the relevant Forescout Platform Tags and select **OK**.

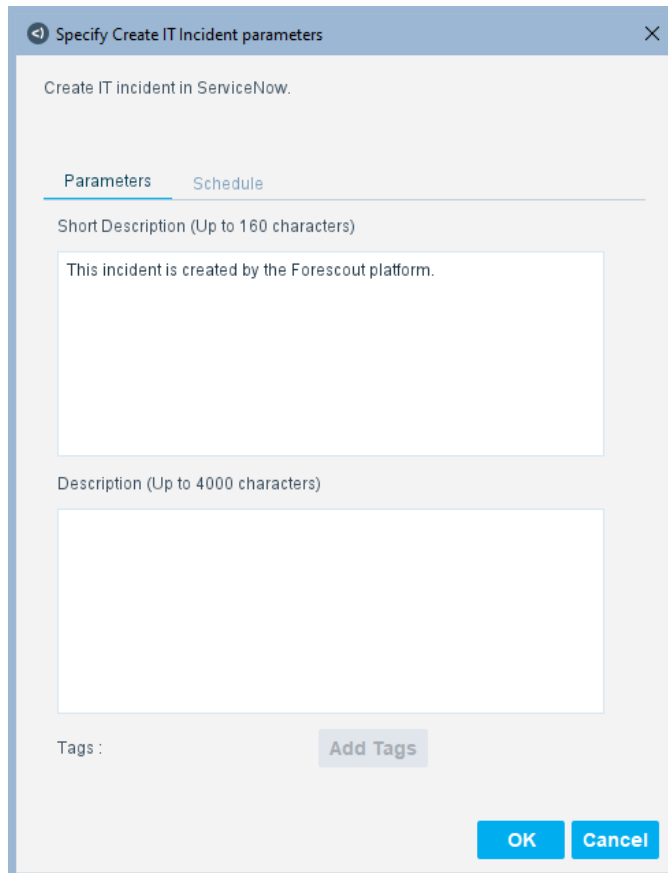
Create IT Incident

Use this action to create an IT incident in ServiceNow. You can specify the category, impact, urgency, and priority for the incident. You can also add tags.

Refer also to the *Forescout App for IT Incidents* installation and configuration guide in the section, Modify Transform Map.

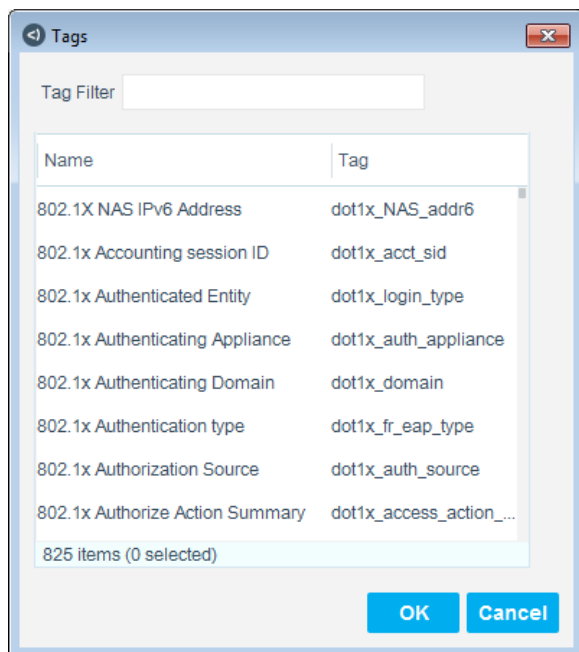
To use the Create IT Incident action:

1. In the Actions tree, select **ServiceNow** and then select **Create IT Incident**. The Specify Create IT Incident parameters dialog box opens to the Parameters tab.

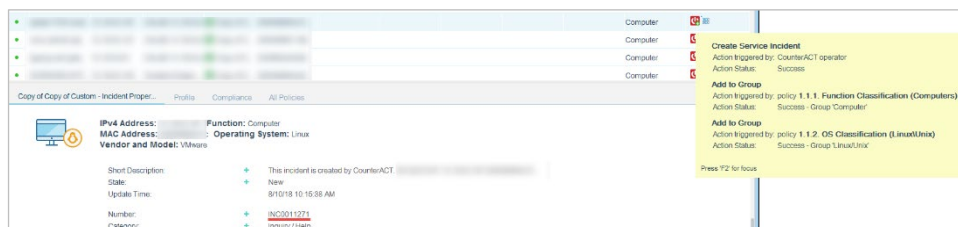


The dialog box titled "Specify Create IT Incident parameters" has a close button (X) in the top right corner. It contains the text "Create IT incident in ServiceNow." Below this, there are two tabs: "Parameters" (selected) and "Schedule". Under the "Parameters" tab, there are two text input fields. The first is labeled "Short Description (Up to 160 characters)" and contains the text "This incident is created by the Forescout platform." The second is labeled "Description (Up to 4000 characters)" and is empty. At the bottom left, there is a label "Tags :" and an "Add Tags" button. At the bottom right, there are "OK" and "Cancel" buttons.

2. Enter a short description and a description. You can add tags to the description or select **Add Tags**.



3. In the Specify Create IT Incident parameters dialog box, select the Schedule tab.
4. Schedule the action and select **OK**.
5. In the All Hosts pane, select a host with the ServiceNow action icon. Hold your cursor over the icon to view the action status. The incident number appears in the Details pane.



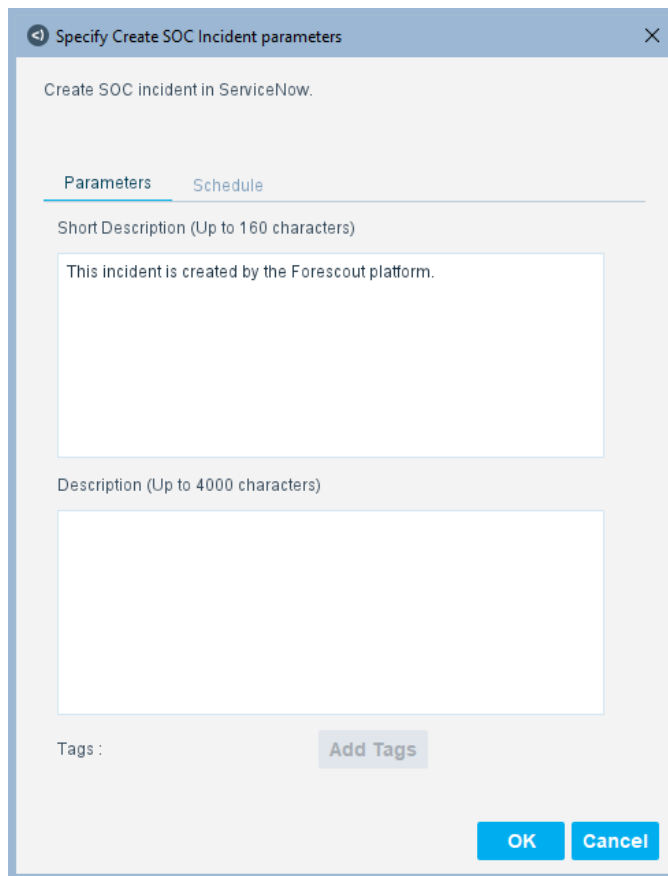
Create SOC Incident

Use this action to create a SOC incident in ServiceNow.

Refer also to the *Forescout App for SOC Incidents* installation and configuration guide in the section, Modify Transform Map.

To use the Create SOC incident action:

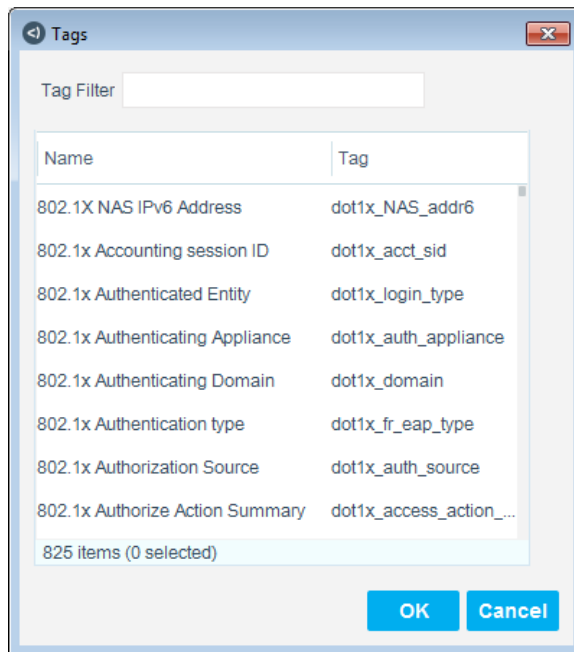
1. In the Actions tree, select **ServiceNow** and then select **Create SOC Incident**. The Specify Create SOC Incident parameters dialog box opens to the Parameters tab.



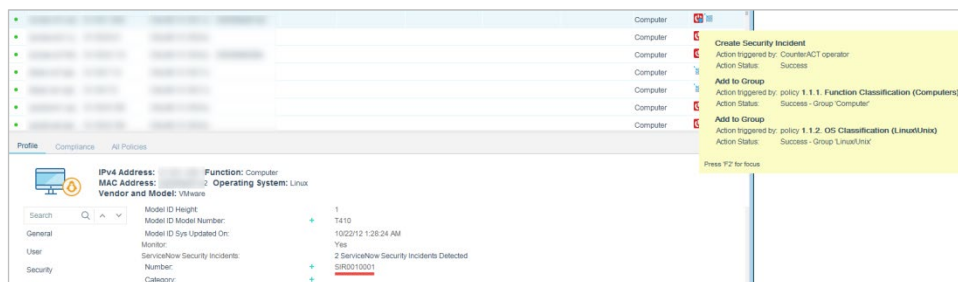
The dialog box is titled "Specify Create SOC Incident parameters" and contains the following elements:

- A header bar with a back arrow, the title, and a close button (X).
- A subtitle: "Create SOC incident in ServiceNow."
- Two tabs: "Parameters" (active) and "Schedule".
- A "Short Description (Up to 160 characters)" section with a text area containing the text: "This incident is created by the Forescout platform."
- A "Description (Up to 4000 characters)" section with a larger text area.
- A "Tags :" label and an "Add Tags" button.
- At the bottom right, "OK" and "Cancel" buttons.

2. Enter a short description and a description. You can add tags to the description or select **Add Tags**.



3. In the Specify Create SOC Incident parameters dialog box, select the Schedule tab.
4. Schedule the action and select **OK**.
5. In the All Hosts pane, select a host with the ServiceNow action icon. Hold your cursor over the icon to view the action status. The incident number appears in the Details pane.



Set Action Thresholds

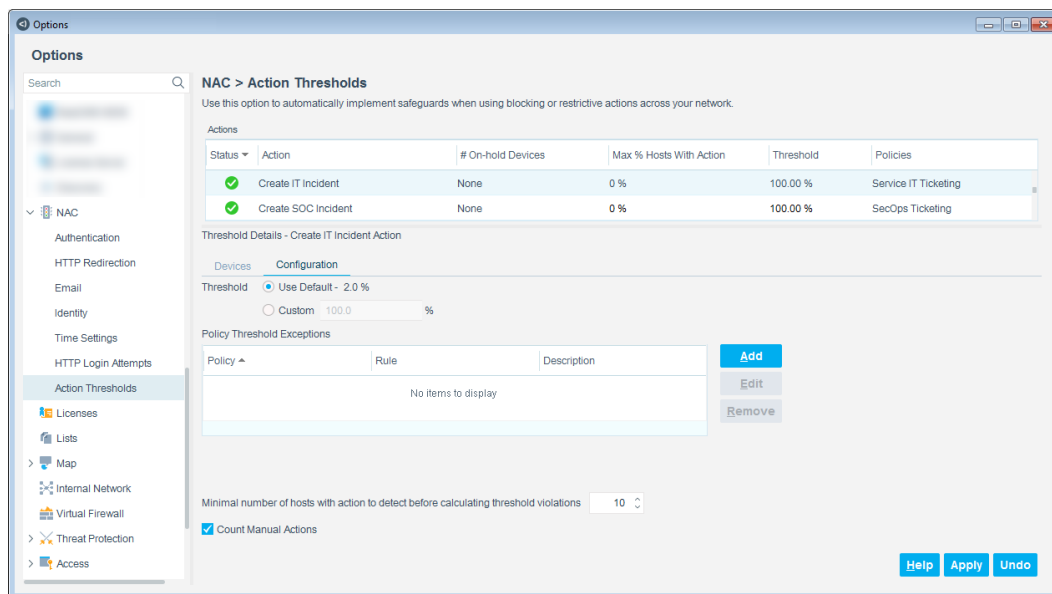
Use **Action Thresholds** to restrict the number of actions. Action thresholds are designed to automatically implement safeguards. An action threshold is the maximum percentage of endpoints that can be controlled by a specific action type defined at a single device.

The **Create IT Incident** and the **Create SOC Incident** actions have a default 2% action threshold, which can be scaled up to 100%.

For information about action thresholds, refer to the *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

To change an action threshold:

1. In the Options pane, select **NAC > Action Thresholds**.



2. In the Actions table, select **Create IT Incident** or **Create SOC Incident**.
3. In the Threshold Details section, select the Configuration tab, select **Custom**, and type a value in the field.
4. Select **Apply**.

Send Additional Properties


Additional properties are those not included in the pre-loaded Outbound Mapping configuration described in [Define Outbound Mapping](#). Additional properties can be sent to ServiceNow.

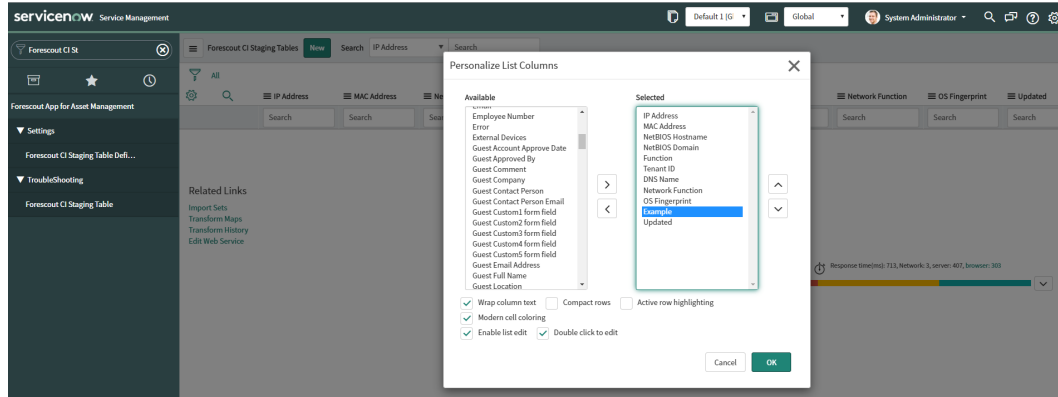
To send additional properties:

1. Log in to the ServiceNow instance and go to **Forescout App for Asset Management > Settings > Forescout CI Staging Table Definition**.

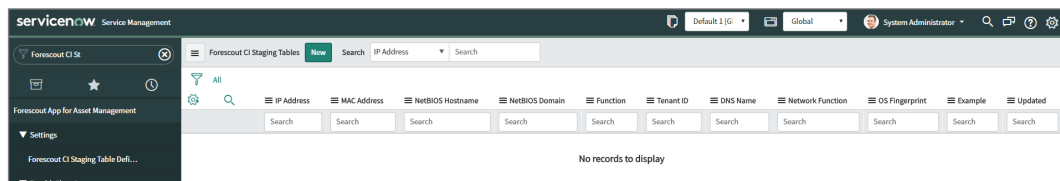
2. To create a new table column, select **New**.

3. Configure the Type, Column label, Column name, and other parameters, and then select **Submit**.

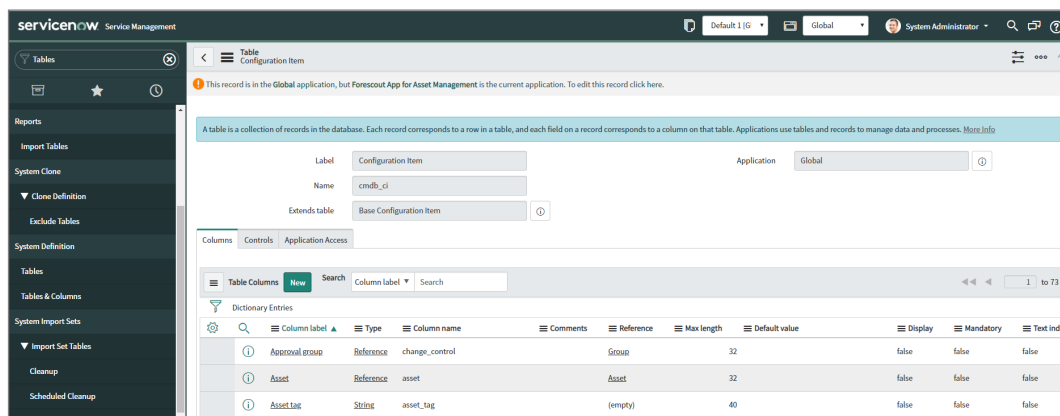
4. (Optional) To display the column in the Forescout CI Staging Table list view, go to **Forescout App for Asset Management > Troubleshooting > Forescout CI Staging Table** and select . In the Personalize List Columns, move Example to Selected, and then select **OK**.



The Example column is displayed in the list view.



5. (Optional) To create a new column in the target table, go to **System Definition > Tables**, and then select the target table, for example, Configuration Item.



6. (Optional) Repeat steps [2](#) to [3](#) to create a new column in the target table.

ServiceNow Service Management

Dictionary Entry
New record [Advanced view]

A dictionary entry manages how ServiceNow stores data in tables and fields (columns). For new dictionary entries, select a Table and the field Type of the new column. Also enter a column label, which becomes the field label, and the column name. If necessary, set a Max length for text String type fields, make the field Mandatory to save a record, and make the field a [Display Value](#) for reference fields so it appears on records that reference this table. [More info](#)

* Table: Configuration Item [cmdb_ci] Application: Global

* Type: String Active: ☒

* Column label: Example Function field: ☐

* Column name: u_example Read only: ☐

* Max length: 40 Mandatory: ☐

Display: ☐

Attributes

7. Go to **Forescout App for Asset Management > Settings > Transform Maps** and select **Forescout CI Transform Map**.

ServiceNow Service Management

Transform Maps

Name	Source table	Target table
Forescout CI Transform Map	Forescout CI Staging Table [x_ftpp_now_plat_forescout_import_table]	Configuration Item [cmdb_ci]
Forescout Dynamic Properties	Forescout Dynamic Properties Import Set	Forescout Dynamic Properties

8. Select the active **onBefore** in the Transform Scripts tab.

ServiceNow Service Management

Table Transform Map
Forescout CI Transform Map

* Name: Forescout CI Transform Map Created: 2018-10-23 15:02:39

* Source table: Forescout CI Staging Table [x_ftpp_now_plat_forescout_import_table]

* Target table: Configuration Item [cmdb_ci]

Active: ☒

Run business rules: ☐

Enforce mandatory fields: No

Copy empty fields: ☐

Create new record on empty codebase fields: ☐

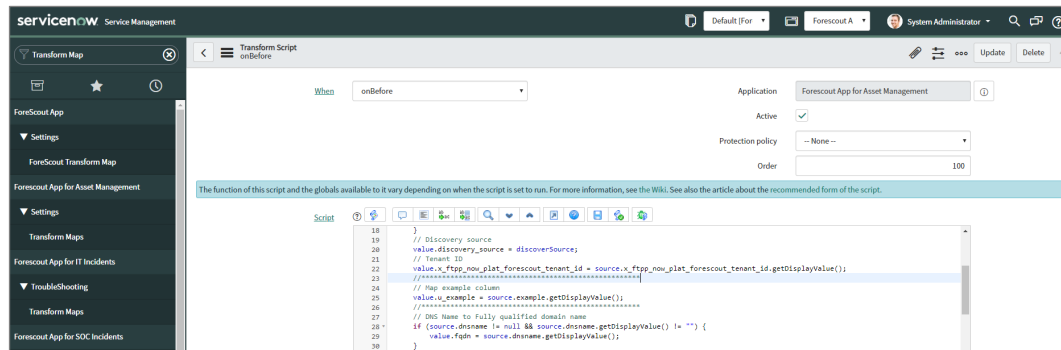
Update Copy Delete

Related Links
Add to Update Set
Auto Map Matching Fields
Mapping Assist

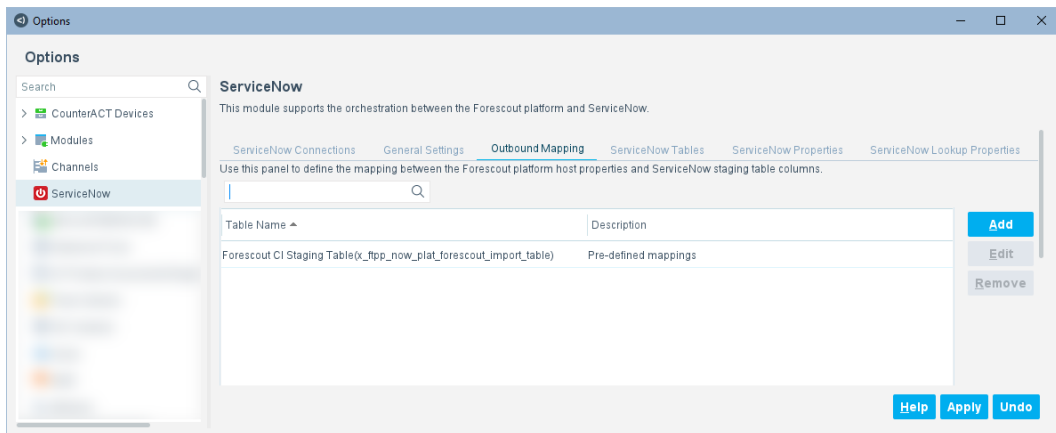
Field Maps Transform Scripts (3)

When	Script	Order	Active	Created	Replace on upgrade (No Longer Used)
onBefore	(function runTransformScript(source, map...	100	true	2019-08-05 10:23:21	false
onAfter	(function runTransformScript(source, map...	100	false	2018-10-23 15:08:59	false

9. Modify the script to map the newly created column to the target column, then select **Update**.



10. Log in to the Console, open the Options pane, and go to **ServiceNow > Outbound Mapping**. To edit the ForeScout CI Staging Table, select **Edit**.



11. Select the Map Data tab.

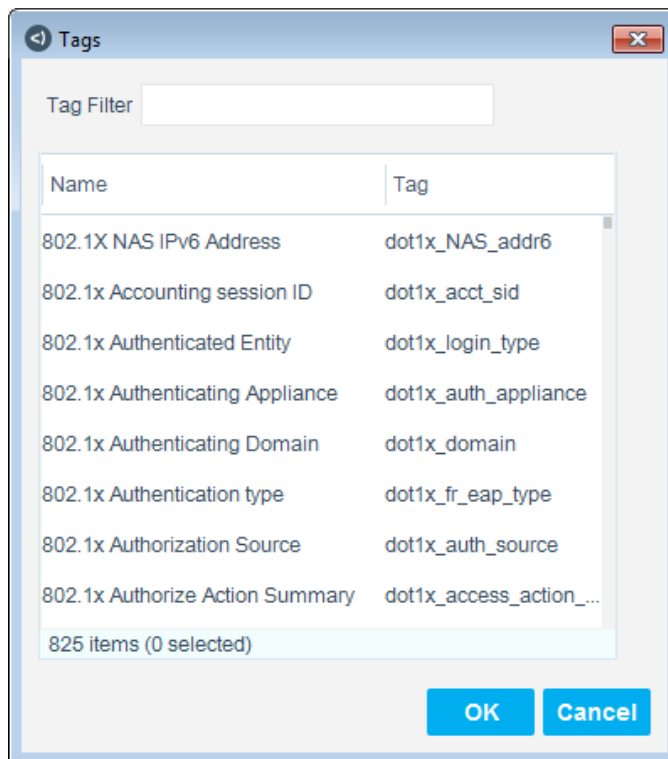
The screenshot shows the 'Edit Outbound Mapping' dialog box with the 'Map Data' tab selected. The dialog has a title bar with a back arrow and a close button. Below the title bar, there are two tabs: 'General' and 'Map Data'. The 'Map Data' tab is active, showing a section titled 'Map Data' with the instruction 'Map the Forescout platform tag value to the ServiceNow column.' Below this is a search bar with the placeholder text 'Search'. A table lists various Forescout Platform Tags and their corresponding ServiceNow Columns. The table has two columns: 'Forescout Platform Tag' and 'ServiceNow Column'. The rows include: {windows_updates_waiting_for_reboot} to Windows Updates Installed - Reboot R..., {hostname} to DNS Name(dnsname), {vendor} to NIC Vendor(nicvendor), {linux_operating_system} to Linux Version(linux_version), {gst_comment} to Guest Comment(guest_comment), {linux_file_exists} to Linux File Exists(linux_file_exists), {user_agent} to WLAN Client User Agent(wlan_client_u..., {va_os_comp} to Windows Version Fine-tuned(windows..., {file_attr_wua_dll_version} to Windows Update Agent Installed(windo..., {device_interfaces} to Device Interfaces(device_interfaces), {banner} to Service Banner(service_banner), {process_no_ext} to Windows Process Running(windows_p..., and {ad_sn} to Last Name(last_name). At the bottom of the table, it says '177 items (0 selected)'. To the right of the table are three buttons: 'Add', 'Edit', and 'Remove'. At the bottom of the dialog are three buttons: 'Help', 'OK', and 'Cancel'.

Forescout Platform Tag	ServiceNow Column
{windows_updates_waiting_for_reboot}	Windows Updates Installed - Reboot R...
{hostname}	DNS Name(dnsname)
{vendor}	NIC Vendor(nicvendor)
{linux_operating_system}	Linux Version(linux_version)
{gst_comment}	Guest Comment(guest_comment)
{linux_file_exists}	Linux File Exists(linux_file_exists)
{user_agent}	WLAN Client User Agent(wlan_client_u...
{va_os_comp}	Windows Version Fine-tuned(windows...
{file_attr_wua_dll_version}	Windows Update Agent Installed(windo...
{device_interfaces}	Device Interfaces(device_interfaces)
{banner}	Service Banner(service_banner)
{process_no_ext}	Windows Process Running(windows_p...
{ad_sn}	Last Name(last_name)

12. Select Add.

The screenshot shows the 'Add Mapping' dialog box. It has a title bar with a back arrow and a close button. Below the title bar, there are two input fields: 'Forescout Platform Tag' and 'ServiceNow Column'. Each input field has a 'Browse' button next to it. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

- 13.** To browse Forescout Platform Tags, select the adjacent **Browse** button.

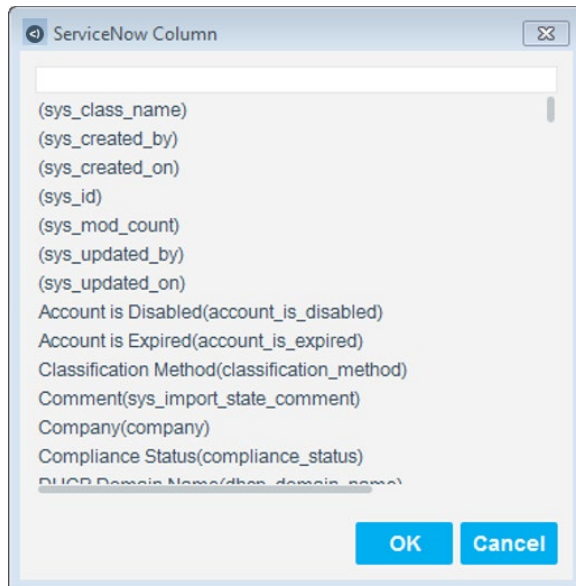


- 14.** Select the tag to send, then select **OK**.

- 15.** To browse ServiceNow Column, select the adjacent **Browse** button.



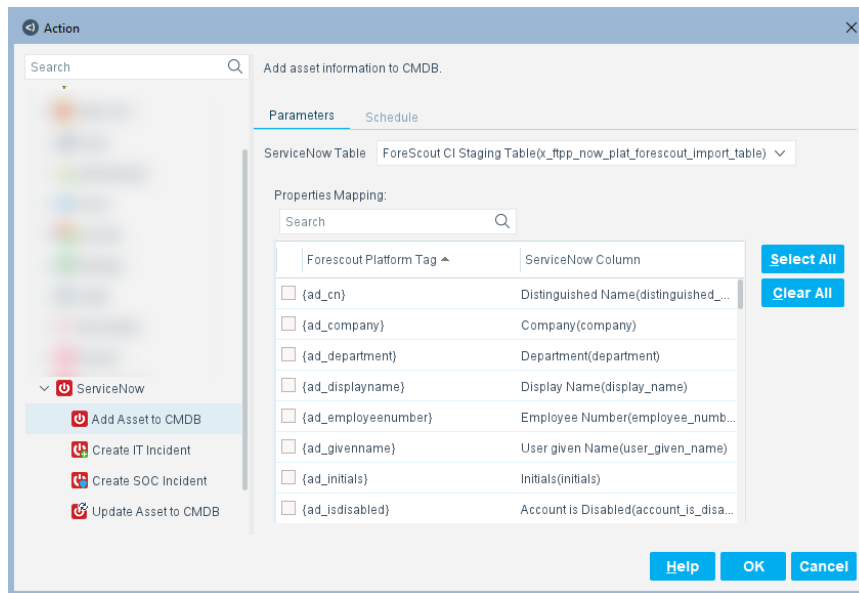
16. Select the column created in step [3](#), then select **OK**.



17. To add the mapping, select **OK**.



- 18.** Edit the Add Asset to CMDB and Update Asset to CMDB actions in policies to include the new property.



Work with ForeScout eyeExtend for ServiceNow

Once ForeScout eyeExtend for ServiceNow has been configured, you can view and manage the virtual devices from the Asset Inventory view in the Console. This provides activity information, accurate at the time of the poll, on cloud endpoints based on certain instances' properties.

The Asset Inventory lets you:

- Complement a device-specific view of the organizational network with an activity-specific view
- View virtual machine endpoints that were detected with specific attributes
- Incorporate inventory detections into policies

Best Practices

Communication Thresholds

The default setting for connections from the ForeScout platform to ServiceNow is the maximum permissible: 3,000 actions per 10 minutes per CounterACT Appliance configured to connect to ServiceNow.

While ServiceNow can support a higher number of connections in that timeframe from all sources, a single ForeScout platform connection cannot go higher than 3,000

actions per 10 minutes. Therefore, this value should be modified only if a lower value is required for performance or some other consideration.

The maximum data rate is 20,000 actions per 10 minutes for ServiceNow as a whole. If multiple ServiceNow connections are defined, this limit must be respected for the total number of connections the Forescout platform consumes as well as what other systems utilize in their connection with ServiceNow.

Appliance Sizing

We recommend one CT10000/VCT 10000 Appliance per 40,000 endpoints, as determined by peak traffic loads. If, for example, peak load is approximately 70,000 users logged on at the same time, two ServiceNow focal Appliances would be appropriate. For customers with lower peak loads, a single Appliance would be appropriate for handling the ServiceNow connection.

Appliance Clustering

Clustering Appliances for ServiceNow connections is purely an administrative function. Clustering is done to organize communications between ServiceNow and the Forescout platform and does not provide any failover benefits.

The endpoints in the IP address ranges handled by the CounterACT Appliances in a cluster must also be handled by the instance of ServiceNow the cluster is associated with.

ServiceNow Tables

The CMDB tables that will be used to host properties received from the Forescout platform must be defined in ServiceNow **prior** to their configuration in Forescout eyeExtend for ServiceNow. The same guidance applies for columns in existing tables which will have the Forescout platform properties mapped to them. By default, there are 177 properties the Forescout platform sends to the Forescout CI Staging Table in ServiceNow. However, the Forescout Classification Mapping table needs to be modified to take the data and move it to the appropriate table within the CMDB (for example, *cmdb_ci_computer*). You can also find this information on the ServiceNow instance Forescout App for Asset Management under **Forescout Classification Mappings**.

It is recommended that you import device information according to function, as determined by the Forescout platform. Those functions include Information Technology and Operational Technology, with each of those categories further subdivided.

Information Technology is broken down into the categories: Accessory, Appliance, Computer, Mobile, Multimedia, Networking, Storage, and Wearable. Operational Technology categories include Energy & Power, Gaming, Healthcare, Metal & Allied, Mining, Non-Industry Specific, Retail & Financial, and Traffic & Parking Management. Each of these categories is further divided into sub-categories. Organizations may consider building tables for sub-categories or may find that certain categories may not apply to their network. It is recommended that you use the Function classification as a starting point for organizing the data on the Forescout platform that will be brought into ServiceNow.

When selecting properties to import into the Forescout platform, if a ServiceNow property is not a String, Integer, Date, or Boolean value, it cannot share that property with the Forescout platform. Reference type 2.0 is also supported.

Additional Properties

You can send additional properties outside the default 177. This requires some effort on the Forescout CI Staging Table, Transform Maps, and the **Add Asset Identification Information to CMDB** policy.

Best Practice would be to define those columns in ServiceNow **before** adding the properties to the Forescout platform in the policy.

General Guidance

ServiceNow tables should be set up in advance to receive fields from the Forescout platform.

Key Value in ServiceNow

Forescout strongly recommends using the device MAC address as a key value for endpoints in ServiceNow, as the MAC address is the default means that the Forescout platform identifies a device. Using a different value in ServiceNow as a key is not a best practice.

Visibility of MAC Addresses

Because the Forescout platform reconciles ServiceNow data using an endpoint MAC address as a key, it is vital that all of your network devices be configured to send accurate and timely MAC address information to the Forescout platform. Endpoints in the Forescout platform without an associated MAC address will not automatically be associated with data from ServiceNow.

Refer to the *Forescout Network Module: Wireless Plugin Configuration Guide* and/or the *Forescout Network Module: Switch Plugin Configuration Guide* regarding proper configuration of devices. See [Additional Forescout Documentation](#) for information on how to access these guides.

Forescout Account in ServiceNow

The default permissions (rights) associated with the Forescout account in ServiceNow are sufficient for most deployments. It is not recommended to add the *Delete* permission to the Forescout account in ServiceNow.

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from the [Technical Documentation Page](#), and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

 Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to <https://www.Forescout.com/company/technical-documentation/>

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend products. The portal also provides additional documentation.

To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend products. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Console.

Console Help Buttons

- Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with in the Console.

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools > Options > Modules**, select the plugin, and then select **Help**.

Content Module, eyeSegment Module, and eyeExtend Product Help Files

- After the component is installed, select **Tools > Options > Modules**, select the component, and then select **Help**.

Documentation Portal

- Select **Documentation Portal** from the **Help** menu.