ForeScout® Extended Module for ServiceNow®

Configuration Guide

Version 1.2

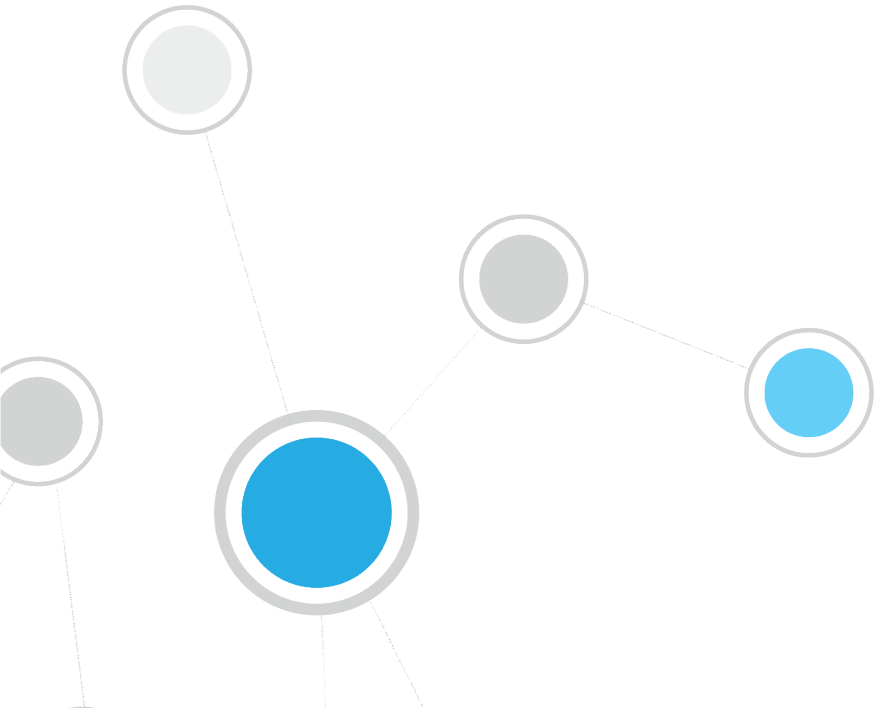


Table of Contents

About ServiceNow Integration

Configuration Management Database (CMDB) is enriched and supplemented by the bi-directional data exchange between ForeScout CounterACT® and ServiceNow®. Through adding or updating of device properties on ServiceNow's CMDB configuration item tables, CounterACT triggers and orchestrates the ServiceNow workflow by applying CounterACT policies. These policies are based on the CounterACT properties and the properties exchanged with the ServiceNow instance. The data exchange is as follows:

- CounterACT Appliance(s) identify devices on the network segments
- Update ServiceNow tables with device properties captured by CounterACT
- Import device properties from ServiceNow that CounterACT was not aware of

The ServiceNow Module comes with a package composed of one update set:

- Script that creates a scriptable API to utilize the identity and reconciliation services offered by ServiceNow.

This update set utilizes the identity and reconciliation services offered by ServiceNow to prioritize and merge the asset records into the ServiceNow configuration management database.

Use Cases

This section describes important use cases supported by this module. To understand how this module helps you achieve these goals, see About this Module.

- Asset Identification
- Asset Inventory True-up

Asset Identification

ServiceNow has IT Asset Management and CMDB as one of its widely-used components. The CounterACT asset identification and remediation functionality can provide and benefit from each other's rich information.

Workflow

1. Device on the network is identified through admission events and upon CounterACT scanning activity additional properties are captured. This device information is shared with ServiceNow.
2. ServiceNow adds this information in its repository and provides additional properties from its repository
3. CounterACT adds these ServiceNow properties to its repository and leverages them for policy decisions.
4. CounterACT and ServiceNow users view updated and correlated device information.

Asset Inventory True-up

The continuous monitoring function in CounterACT can play a role of “auditor” and help equalize and bring both CounterACT and ServiceNow systems up-to-date. CounterACT enriches asset attributes with additional context such as the switch port the device is connected to, VLAN information, network segment information, location, compliance status, etc. CounterACT monitors and update information to the asset inventory from the time a device enters the network to the time 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 increase overall network asset compliance.

Workflow

1. A device’s information is captured upon scan activity.
2. CounterACT gets information about this device from ServiceNow, points out discrepancies and then helps ServiceNow update its repository.
3. Additionally, CounterACT can also verify if the device has the latest patches; if not it can inform ServiceNow and take remediation actions.
4. Depending upon the configurations, additional optional remediation actions are taken.

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

Additional ServiceNow Documentation

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

https://docs.servicenow.com/bundle/istanbul-it-service-management/page/product/configuration-management/concept/c_ITILConfigurationManagement.html

About this Module

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

The ForeScout Extended Module for ServiceNow integrates CounterACT and ServiceNow so that you can:

- Use policies and actions provided by the ServiceNow Module to update current asset information (such as switch port, open ports, VLAN, etc.) to ServiceNow. See Add Asset Identification Information to CMDB Template and Update Asset Identification Information to CMDB Template.

The Extended Module for ServiceNow and the ForeScout App for ServiceNow CMDB work together to support full functionality between CounterACT and ServiceNow. You must install and configure both components to work with the features described in this document. For example, CounterACT policies and actions provided by the Extended Module for ServiceNow are used to populate the import set table in ForeScout App for ServiceNow CMBD with CounterACT data and the application transfers the data to ServiceNow CMDB. Read this document together with the *ForeScout App for ServiceNow CMDB Installation and Configuration Guide*.

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

To access the ForeScout App for ServiceNow CMDB:

1. Go to https://store.servicenow.com and conduct a search on “ForeScout App for ServiceNow CMDB” and select it.
2. Select the **Get** button to download the ForeScout App for ServiceNow CMDB (version 1.1-).
3. Be sure to download and read the *ForeScout App for ServiceNow CMDB Installation and Configuration Guide* located under Support Links & Docs.

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, ***IPv6 addresses are not yet supported by this component.*** 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 component.

Concepts, Components, Considerations

This section provides a basic overview of ServiceNow/ CounterACT architecture:

- 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 *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, the ServiceNow Module allows the operator to control the rate of insertion and update from CounterACT to the ServiceNow instance, thus avoiding the processing limit of ServiceNow.

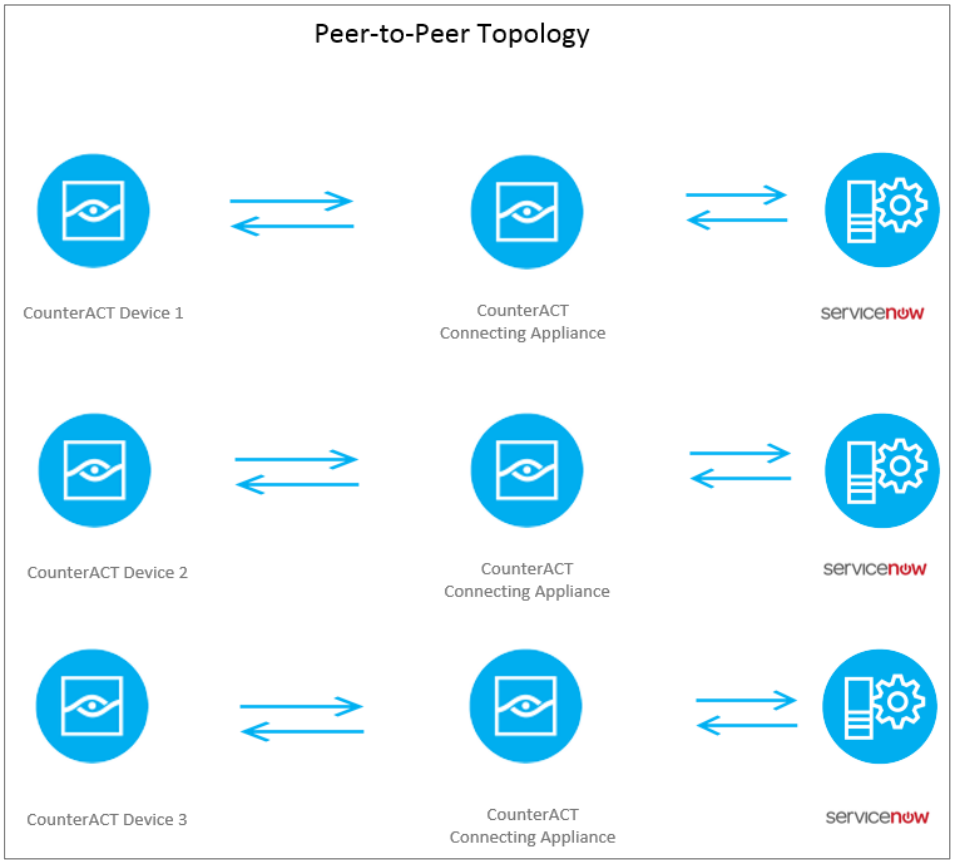
Typically, there is only one ServiceNow production instance per customer hosted in the cloud. CounterACT Appliances are connected to this ServiceNow instance using logical URL and user credentials.

Deployment Options

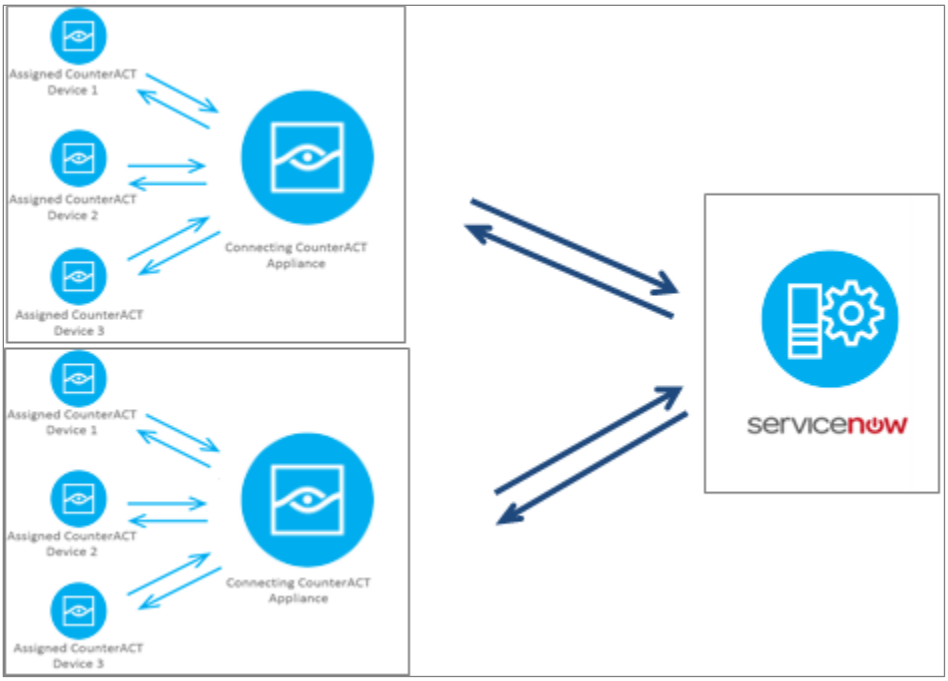
There are two topologies that can be used to set up multiple CounterACT Appliances to a ServiceNow instance. For both topologies, a single CounterACT Appliance can be assigned to only one ServiceNow instance.

> *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 prompts 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 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.servcenow.com). The ServiceNow instance is already created and used by the company independent of CounterACT.
- A ***CounterACT Connecting Appliance cluster*** is a group of one or more CounterACT Appliances connecting to the ServiceNow instance through that logical URL associated with the ServiceNow. There may be more than one connecting appliance clusters in a company, typically set up by geographical region, business unit or functional separation.
- ***CounterACT Appliances*** are the ones that are managing or monitoring devices based on the network segments assigned to a particular CounterACT Appliance. When these appliances have to reach out to ServiceNow, they go through the CounterACT Connecting Appliance cluster(s).
- ***Devices on the network*** these are considered the hardware assets whose information has to be exchanged between CounterACT and ServiceNow. CounterACT continuously monitors the devices - not just when they enter and leave the network.

With this as the context, when the ServiceNow module is installed on CounterACT connecting appliance clusters (each CounterACT Appliance individually), the operator 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 advance settings.

Considerations

This section addresses any additional ForeScout Extended Module for ServiceNow considerations.

ServiceNow Instance Account

You will need to contact your ServiceNow administrator and get the username to connect to the ServiceNow instance. This is required to configure the ForeScout Extended Module for ServiceNow. The user account should contain **`x_ftpp_forescout.forescout_integration_role`**.

The instructions for creating a user credential are listed in the *ForeScout App for ServiceNow CMDB Installation and Configuration Guide*.

Upgrading from ServiceNow 1.0 to 1.1

You are able to upgrade ForeScout Extended Module for ServiceNow to 1.1- directly.

You will not be able to upgrade ForeScout App for ServiceNow CMDB from 1.0- to 1.1-, the new certified scoped application. Instead, the following needs to occur:

1. Delete the old ForeScout Application for ServiceNow on ServiceNow instance. This includes removing its related artifacts.
2. From the store (https://store.servicenow.com), search for ForeScout App for ServiceNow CMDB and get the application.
3. Install the application on ServiceNow instance.
4. Follow the *ForeScout App for ServiceNow CMDB Installation and Configuration Guide* to configure the application.

What to Do

Perform the following to carry out the integration:

1. Verify that requirements are met. See Requirements for details.
2. Download and install the ForeScout Extended Module for ServiceNow module from the ForeScout website: updates.forescout.com. See Install the Module for details.
3. Download and install the ForeScout App for ServiceNow CMDB on ServiceNow instance. See the *ForeScout App for ServiceNow CMDB Installation and Configuration Guide*.
4. Define target ServiceNow instance. Assign CounterACT Appliances to it. See Establish Connection to ServiceNow Instance for details.

5. Create policies for CounterACT to update ServiceNow assets. See Add Asset Identification Information to CMDB Template and Update Asset Identification Information to CMDB Template.
6. When the configurations have been tested and the policies created, you are ready to start Using the ServiceNow Extended Module.

Requirements

This section describes:

- CounterACT Software Requirements
- ForeScout Extended Module License Requirements
- ServiceNow Requirements

CounterACT Software Requirements

The ServiceNow Module requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0.-
- A module license for the ServiceNow Module
- An active Maintenance Contract for the licensed module is required.

ForeScout Extended Module License Requirements

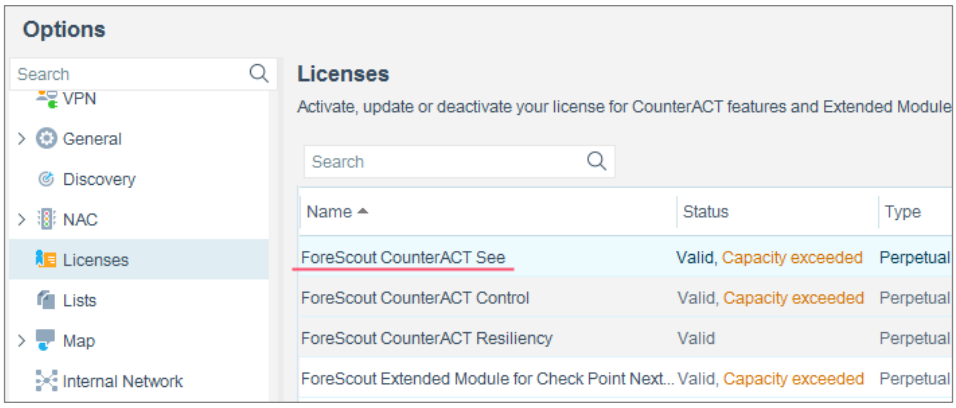
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Centralized Licensing Mode

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Per-Appliance Licensing Mode

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

When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the module, you must purchase the license*.

Demo license extension requests and permanent license requests are made from the CounterACT 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 CounterACT 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 CounterACT. 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 CounterACT, 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.

Centralized Licensing Mode

When you set up your CounterACT deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including Extended Modules. After the initial license file has been activated, you can update the file to add additional Extended Module licenses or change endpoint capacity for existing Extended Modules. For more information on obtaining Extended Module licenses, contact your ForeScout 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 Extended Module license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each Extended Module license varies by module, but does not exceed the capacity of the *See* license.

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

More License Information

Refer to the *CounterACT Administration Guide* for information on Extended Module licenses. You can also contact your ForeScout representative or license@forescout.com for more information.

ServiceNow Requirements

- ServiceNow Cloud Service version Helsinki, Istanbul or Jakarta Patch 4 or later.
- Verify connectivity between CounterACT and target ServiceNow servers on the configured HTTPS port.

> *HTTPS is always assumed for this connection.*

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 - ***Centralized Licensing Mode***

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.
2. Download the module **`.fpi`** file.
3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT 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 will not proceed if you do not agree to the license agreement.

> *The installation will begin 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.

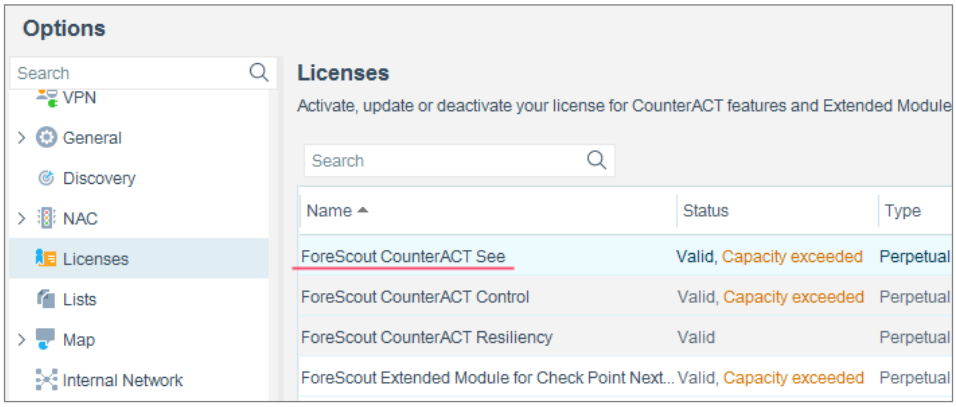
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

Some components are not automatically started following installation.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

This module interacts with the ForeScout App for ServiceNow CMDB. If you install only this module, you can send CounterACT information 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.

Configure the Module

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

Perform this procedure after the ForeScout Extended Module for ServiceNow is installed on your targeted CounterACT Appliance.

To complete 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

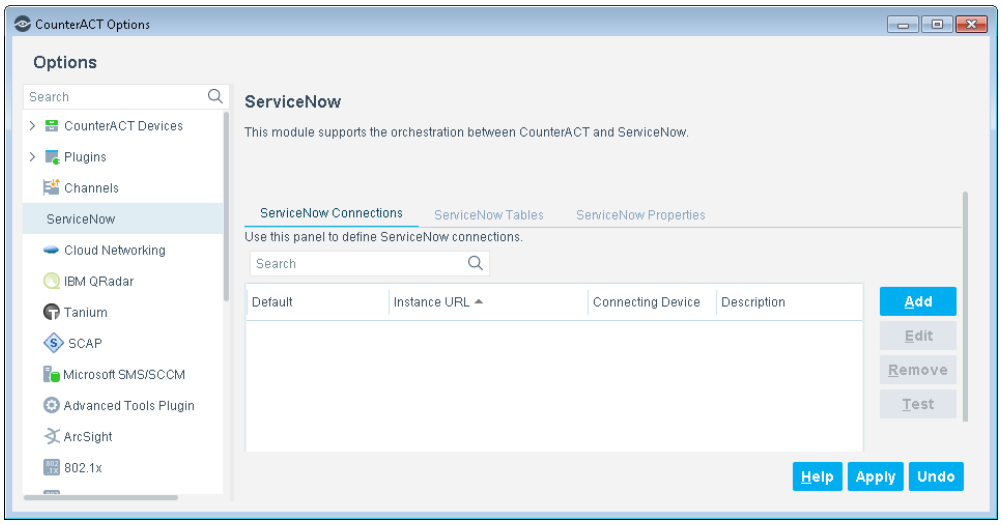
3. Define ServiceNow Tables
4. Define Host Properties
5. Test Your Configurations
6. Verify Configurations

Establish Connection to ServiceNow Instance

You will need to map your CounterACT Appliance to a ServiceNow instance.

To add ServiceNow instance targets for CounterACT:

1. In the CounterACT Console toolbar, select **Options** from the Tools menu.
2. Select **ServiceNow** from the Options pane. The right pane opens to display three tabs: ServiceNow Connections, ServiceNow Tables, and ServiceNow Properties.

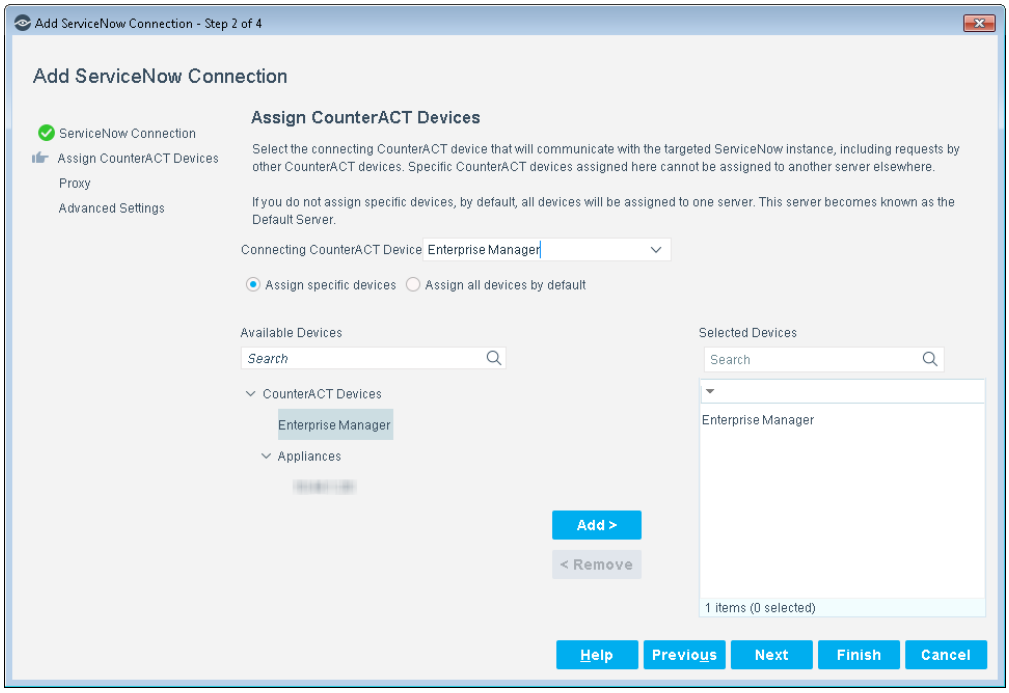


3. In the ServiceNow Connections tab, select **Add**. The Add ServiceNow Connection wizard opens.

4. In the ServiceNow Connection pane, enter your configurations.

Instance URL	Enter the URL for your online ServiceNow account followed by the port number. The port number is optional, but if no port number is provided, CounterACT will use 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.
Description	(Optional) Insert text, for example, a nick name of the ServiceNow connection. This is helpful if you have more than one ServiceNow connection.

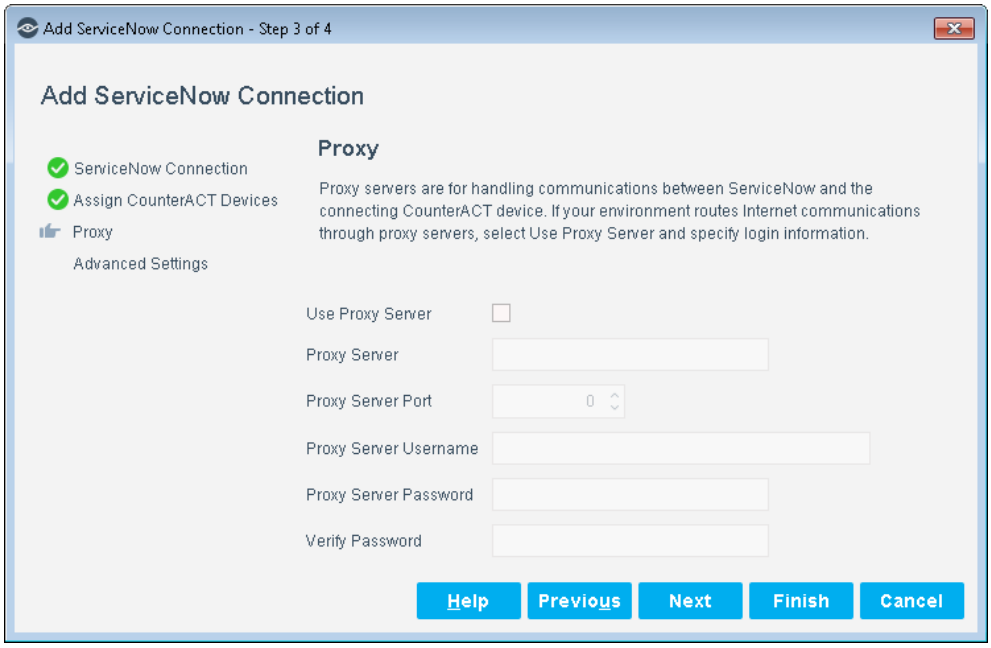
5. Select **Next**. The Assign CounterACT Devices tab displays.



Connecting CounterACT Device	In an environment where more than one CounterACT device is assigned to a single ServiceNow instance, the connecting CounterACT Appliance functions as a middle man between the ServiceNow instance and the CounterACT Appliance. The connecting CounterACT Appliance forwards all queries and requests to and from the ServiceNow instance. Select the **IP address** of the connecting CounterACT Device.
Assign specific devices	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. **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	This is the connecting appliance that CounterACT Appliances are assigned to by default - if they are not explicitly assigned to another connection appliance. Select **Assign all devices by default** to make this connecting appliance the middle man for all CounterACT Appliances not assigned to another connecting device

For more information, see Deployment Options.

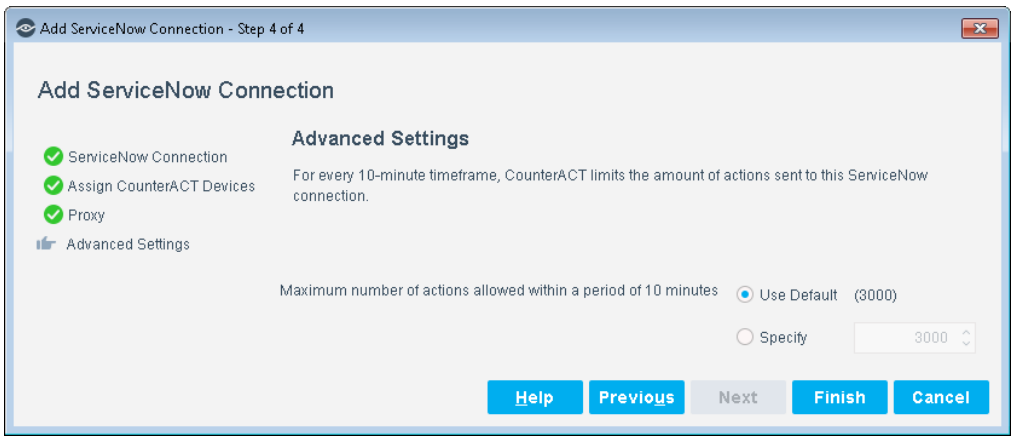
6. Select **Next**. The Proxy tab displays.



7. Using a proxy server is optional. If using a proxy server with Basic Authentication, you will need that proxy's credentials. See ServiceNow Requirements.

Use Proxy Server	If your environment routes internet communications through proxy servers, select this box.
Proxy Server	Enter the IP address of the proxy server.
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.

8. Select **Next**. The Advanced Settings tab displays.



Maximum number of actions allowed within a period of 10 minutes	Addresses the rate limiting. This means CounterACT has to limit the number of actions sent to this ServiceNow instance. This prevents the ServiceNow instance from becoming inundated, and therefore, causes problems. ▪ **Use Default** - select if you want to use the default setting of 3,000 action items per 10-minute timeframe. ▪ **Specify** - select a number from the list to specify the number of action items per 10-minute timeframe.

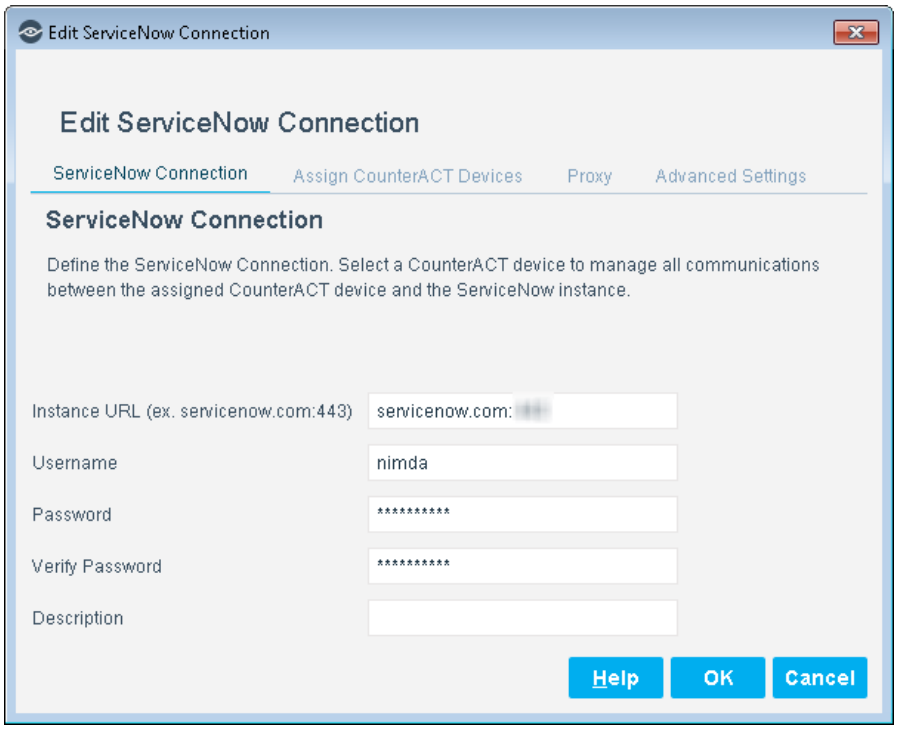
9. Select **Finish**. The server appears in the ServiceNow pane.
10. Continue to the Define ServiceNow Tables section.

Edit ServiceNow Connection

If you need to change the connecting device or assign a different CounterACT Appliance to the connecting device, use the **Edit** option:

To edit a ServiceNow connection:

1. In the Modules pane, select ServiceNow. The ServiceNow pane opens.
2. Select the instance then select **Edit**. The Edit ServiceNow Connection dialog box opens.



3. Make your edits and select **OK**.

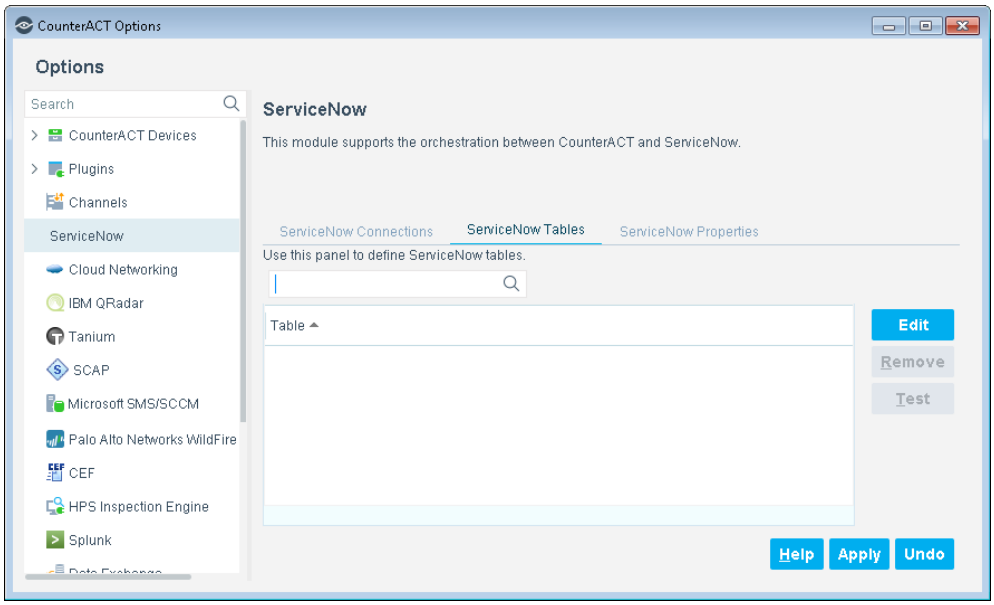
Define ServiceNow Tables

Configuration Management Database (CMDB) is enriched and supplemented by the bi-directional data exchange between CounterACT and ServiceNow. The ServiceNow table definitions are optional and it is used for bringing over properties from ServiceNow into CounterACT. You can create policies based upon CounterACT properties exchanged with the ServiceNow instance. The workflow is as follows:

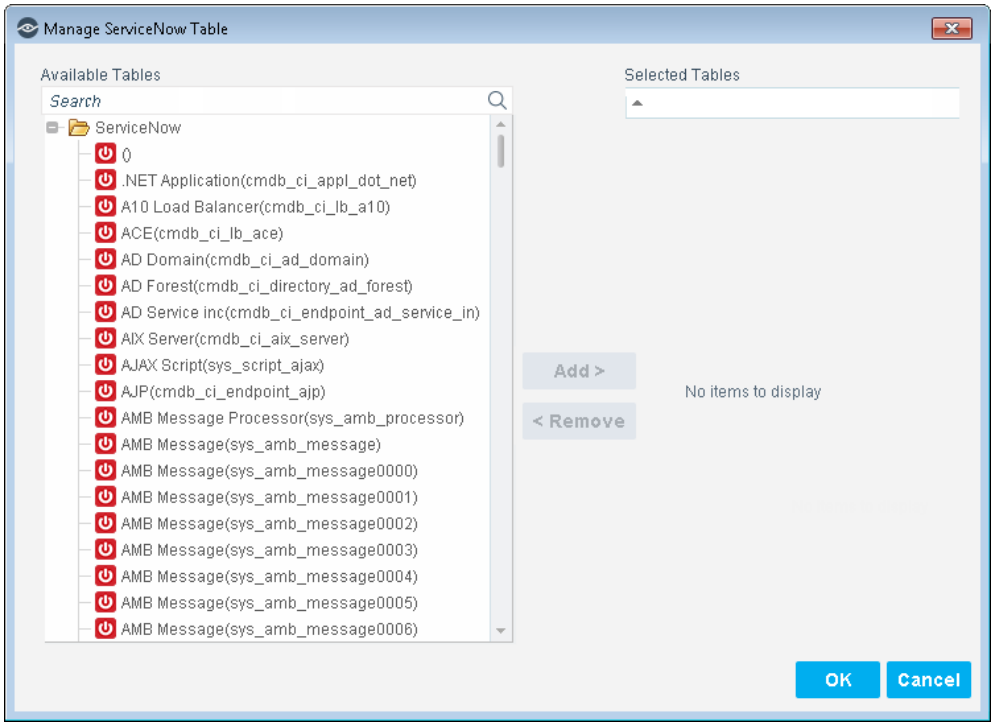
- Add host properties in CounterACT with values from ServiceNow table records.
- Use these as dynamic properties in policy decision through custom policies.

To add ServiceNow tables:

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



3. Select **Edit**. CounterACT connects with the ServiceNow server and pulls in the available tables. It displays these tables in the Manage ServiceNow Table dialog box.



4. In the Manage ServiceNow Table dialog box, you determine which tables in ServiceNow you want to be able to view in CounterACT.
   - Select a table in the Available Tables field and then select **Add**. The table displays in the Selected Tables field - these tables will be imported into CounterACT.
   - To remove a table, select a table in the Selected Tables field and then select **Remove**. The table returns to the Available Tables field.
5. When finished, select **OK**.
6. In the ServiceNow Tables tab, select **Test**. The ServiceNow Module will check if the table exists and try to access that table.
7. After reviewing the testing results, close the Test box.
8. Continue to the Define Host Properties section.

Removing ServiceNow Tables

There may be times where you need to remove the ServiceNow tables.

To remove ServiceNow Tables:

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

Define Host Properties

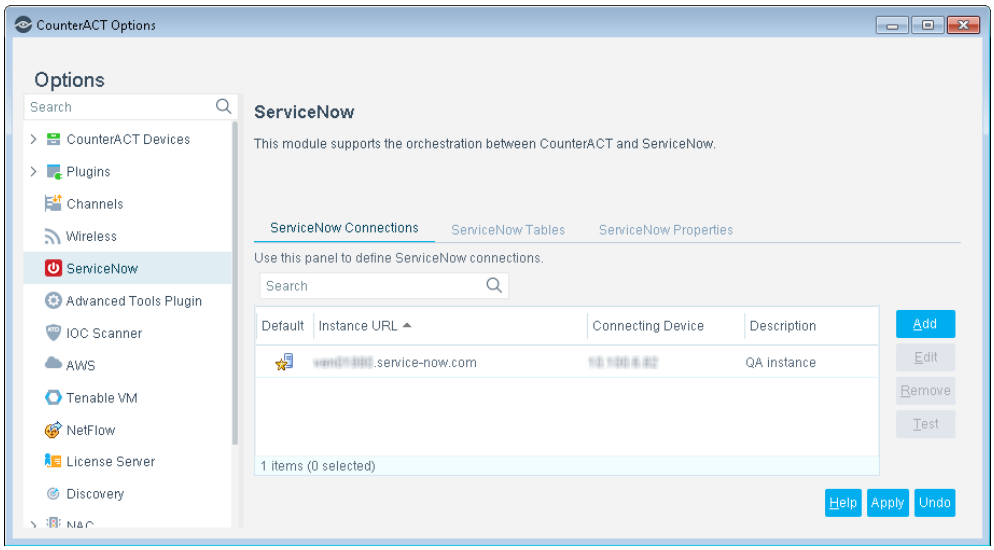
Host properties are information stored in CounterACT for each device identified on the network. When you work with this module, you create new CounterACT host properties to hold data extracted by querying the ServiceNow instance. This makes retrieved data available for use in CounterACT policies.

You can create single-value properties that contain one value, for example, a string property that contains the GUID of the device. In this version we only support String, Integer, Date and Boolean.

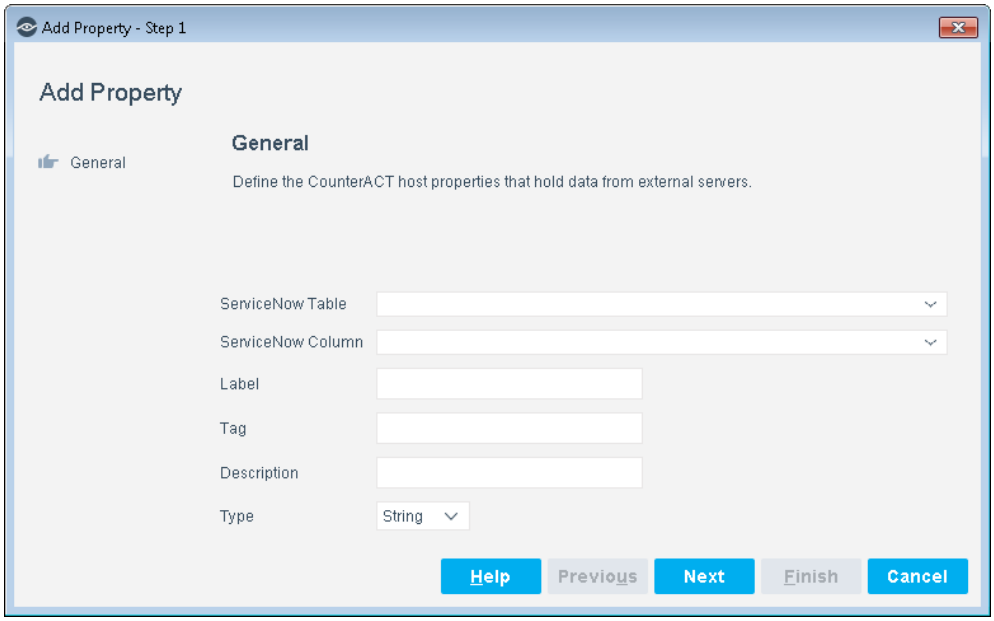
Track Changes properties let you define policy conditions that identify changes in the value of custom properties you define. You can define track changes properties for single-value, list, or Record Exists properties that you create.

To define CounterACT host properties:

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

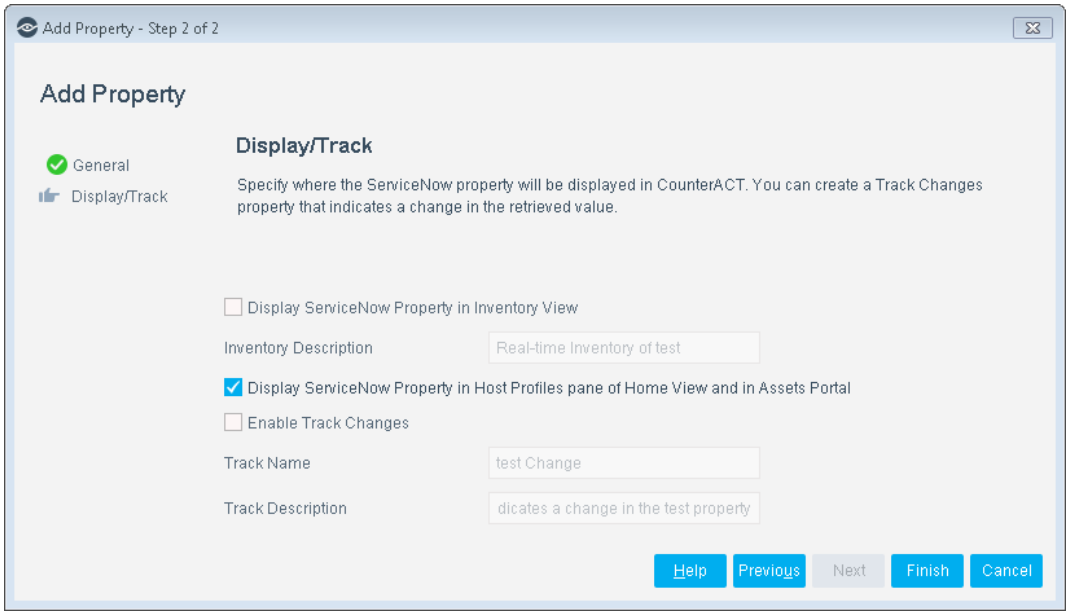


2. Select **Add**. The Add Property Wizard opens to the General pane.



ServiceNow Table	Lists the ServiceNow Table that you selected in the ServiceNow Table tab.
ServiceNow Column	The column name within the selected ServiceNow table.
Label	Create a name to refer to equate the name of the ServiceNow column
Tag	A unique text string using ASCII characters. CounterACT references the property using this unique identification string.
Description	(Optional) Insert text, for example, the nick name of this host property you are creating.
Type	In the Type drop-down list, select the type of data the property contains. Single-value properties contain one value, for example, string, Boolean, date, or integer

3. Select **Next**. The Display/Track pane displays.



Display Property in Inventory View	**Display Property in Inventory View** shows this property in the CounterACT Console Asset Inventory tab. De-select if you do not want it displayed there.
Inventory Description	Enter a description of the property you want to display in the CounterACT Console Asset Inventory. This description will only display if you have the Display Property in Inventory View box checked.
Display ServiceNow Property in Host Profiles Pane of Home View and in Assets Portal	Checked by default, **Display Property in Host Profiles Pane of Home View and in Assets Portal** lists this property in the Profiles tab of the Home view and in the Assets Portal. De-select if you do not want it displayed there.
Enable Track Changes	The Track Changes properties let you define policy conditions that identify changes in the value of custom properties you define. You can define track changes properties for single-value, list, or Record Exists properties that you create. 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 only applicable to single-value and list properties.
Track Name	The text you entered in the Label field in the previous screen populates this field. This field names the item you want to track.
Track Description	The text from the Tag field in the previous screen populates the Track Description field. This field provides a description to the Track Name.

4. Select **Finish**. The property is added to the table in the Property tab.
5. Repeat steps 2-4 for every host property you want to create and use.

6. When finished, in the ServiceNow pane, select **Apply**. The CounterACT infrastructure will save the configurations, update the internal database, and restart the ServiceNow Module. This may take 1-2 minutes for the changes to take effect.

Test Your Configurations

1. Select **Options** and then select **ServiceNow**. The ServiceNow pane opens to the ServiceNow Instance tab.
2. Select a connection and then select **Test**.
3. If the test failed, check your configurations and re-test. If the test passed, repeat step 2 for any additional connections.

Verify Configurations

1. In the CounterACT Consoles toolbar, select the Asset Inventory tab. The Views pane displays on the left.

   If you did not configure to show the property in the Asset Inventory tab, your ServiceNow properties will not display in the Views pane of the Asset Inventory tab.

2. In the left pane, select the **ServiceNow** icon to expand it and then select any of the items in the list to view its properties.
3. Check that the properties match the configuration requirements.

The configuration of the ServiceNow Module is now complete.

Delete ServiceNow Instance

The process for deleting a ServiceNow Instance is the reverse path of creating it:

- Remove ServiceNow Properties associated with the ServiceNow tables.
- Remove ServiceNow Tables.
- Remove ServiceNow Connection.

Remove ServiceNow Properties

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

To remove ServiceNow properties:

1. In the CounterACT 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.

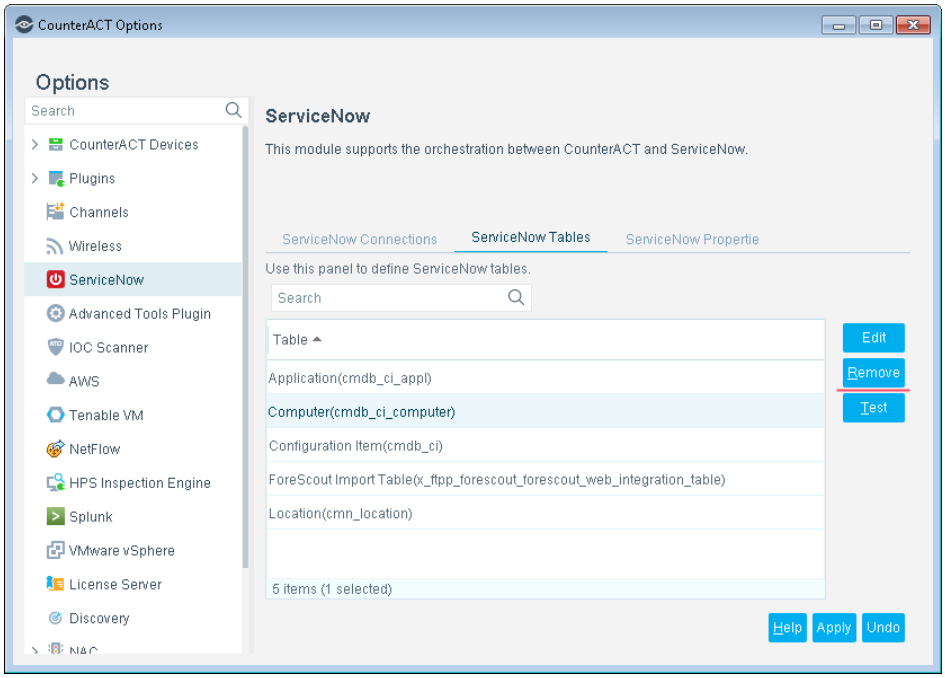
4. Select a property and then select **Remove**.
5. **Confirm** removal.
6. Repeat the steps for other properties, as necessary.
7. In the ServiceNow dialog box, select **Apply**.

Remove ServiceNow Tables

Once the ServiceNow properties have been deleted, you can now remove the tables from CounterACT.

To remove a ServiceNow table:

1. In the CounterACT 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 name and then select **Remove**.



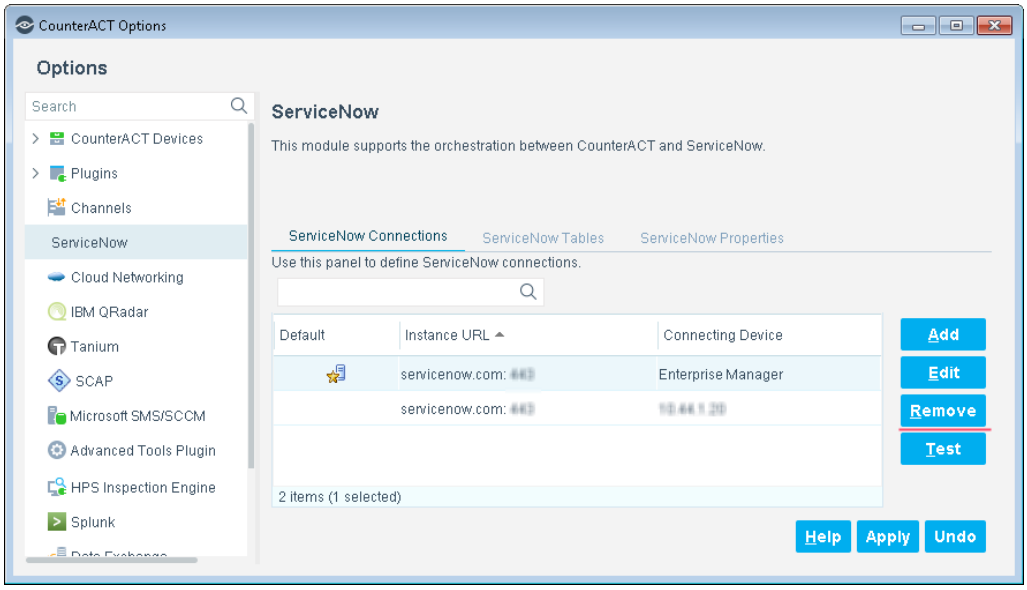
5. **Confirm** removal.
6. Repeat the steps for other tables, as necessary.
7. In the ServiceNow dialog box, select **Apply**.

Remove ServiceNow Connection

Once the ServiceNow tables have been deleted, you can now remove the ServiceNow instance from CounterACT.

To remove a ServiceNow instance:

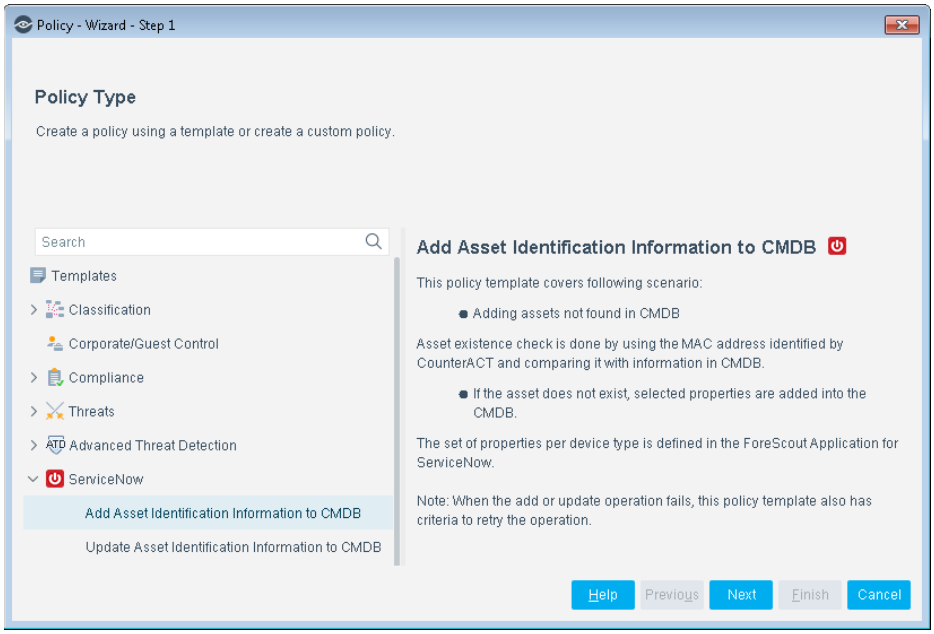
1. In the CounterACT Console, select **Options** from the **Tools** menu.
2. Select **ServiceNow**. The ServiceNow pane opens to the ServiceNow Connections tab.
3. Select the instance name and then select **Remove**.



4. **Confirm** removal.
5. In the ServiceNow dialog box, select **Apply**.

Run ServiceNow Policy Templates

CounterACT 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 the ForeScout Extended Module for ServiceNow, CounterACT policies can include adding and updating ServiceNow tables as an action.



Add Asset Identification Information to CMDB Template

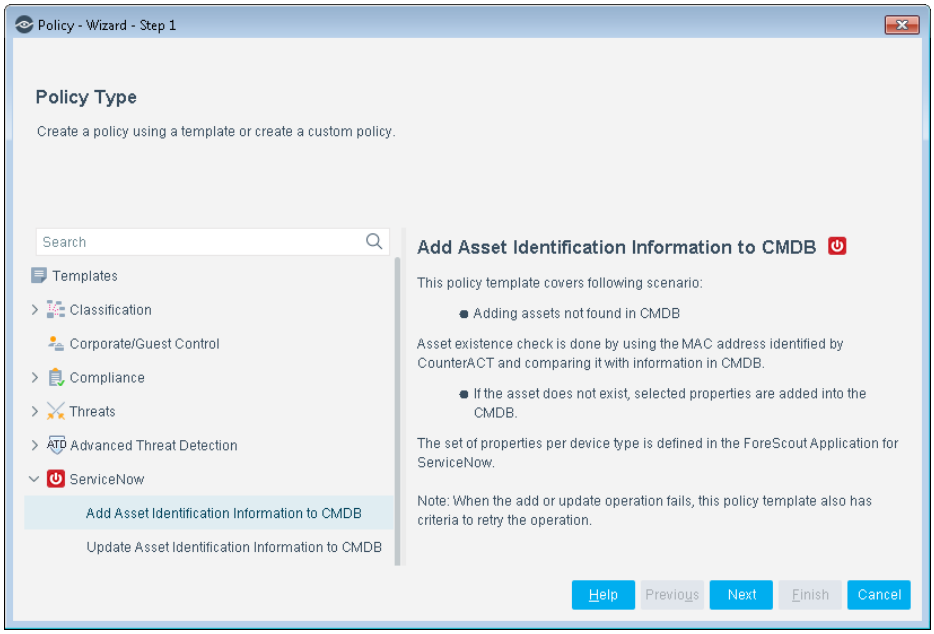
Use the Add Asset Identification Information to CMDB template to create policies that add assets not found in the CMDB. Asset existence check is done by using the MAC address identified by CounterACT and comparing it with information in CMDB.

- If the asset does not exist, selected properties are added into the CMDB.

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

To use the Add Asset Identification Information to CMDB policy template:

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



4. Select **Next**. The Name pane opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. 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.

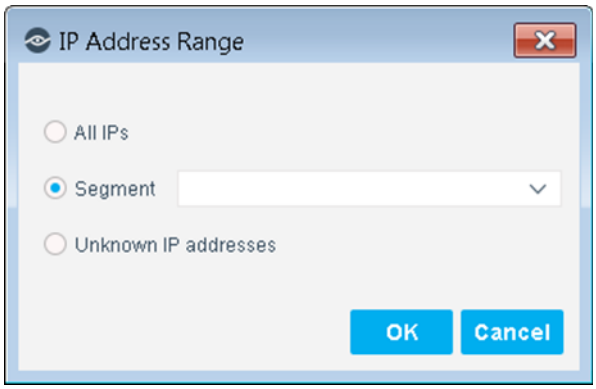
5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will 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.

6. Select **Next.** The Scope pane and IP Address Range dialog box opens.

Define which Devices will be Inspected - Policy Scope

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 page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

  Not applicable for this policy template.

Filter the range by including only certain CounterACT groups and/or by excluding certain devices or users or groups when using this policy.

8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**. The Main Rule pane opens. Continue to the next section.

How Devices are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle devices defined in the policy scope.

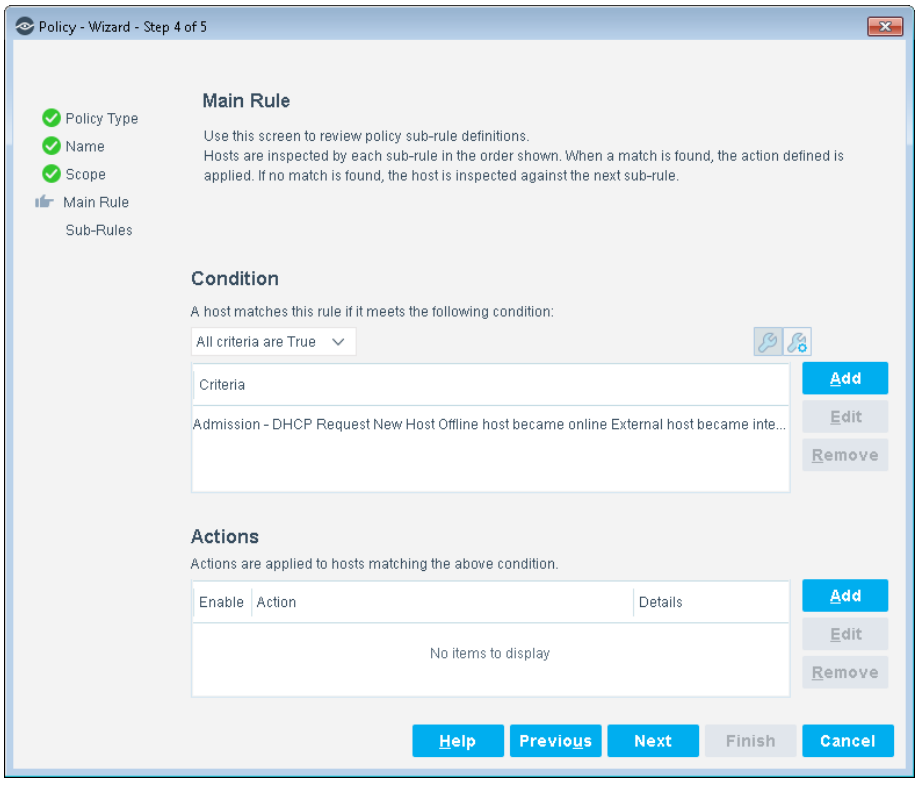
Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with hosts after initial detection and handling, streamlining separate detection and actions into one automated sequence.

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.

Main Rule

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

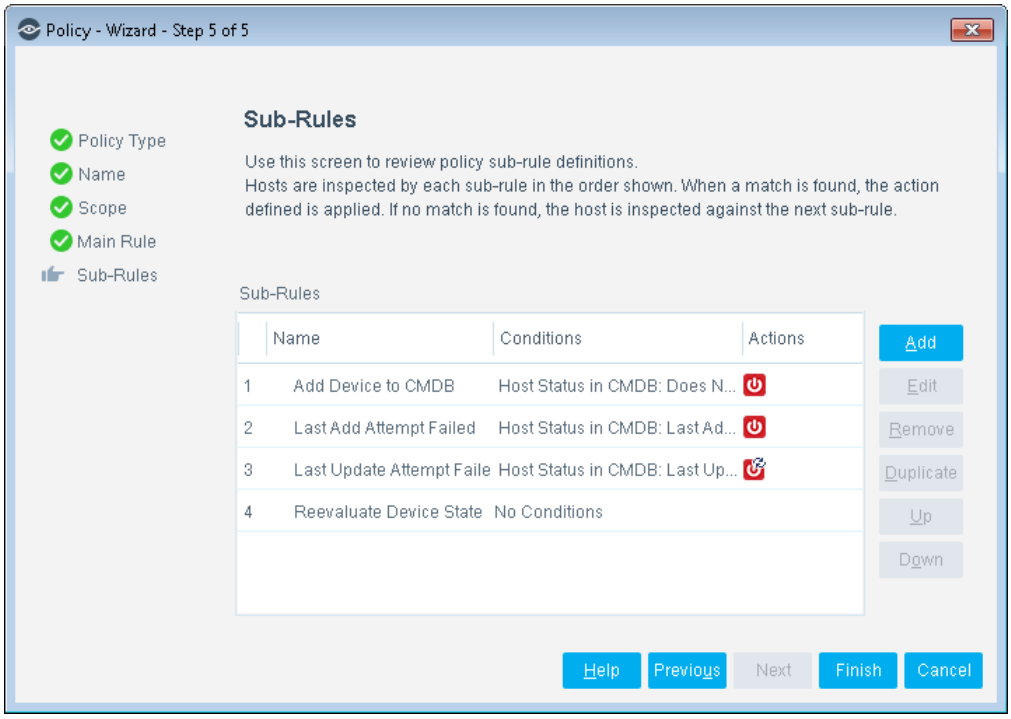
- Authentication via CounterACT HTTP Login action
- DHCP Request
- External host became internal
- External SecureConnector Connected
- Host Connected to a Switch Port
- IP Address Change
- Linux SecureConnector Connected
- Login to an authentication server
- Macintosh SecureConnector Connected
- New Host
- Offline host became online
- Property administrative deletion event
- SecureConnector Connected



10. The Condition Criteria section is populated by default.
11. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties and Policy Actions sections.
12. Select **Next**. The Sub-Rules pane opens.

Sub-Rules

The sub-rules of the Add Asset Identification Information to CMDB policy lists the items CounterACT is to check when applying the Main Rule.



13. Double-click the Add Asset to CMDB sub-rule to open it. The Policy: [Name of Add Asset Identification Information to CMDB policy] Sub-Rule: Add Asset dialog box opens.
14. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties and Policy Actions sections.
15. Select **OK**. In the Policy: [Name of Add Asset Identification Information to CMDB policy] Sub-Rule: Add Asset dialog box, select **OK**.
16. Repeat steps 12 - 14 to make changes in other sub-rules.
17. In the Sub-Rules pane of the Policy Wizard, select **Finish**.
18. On the CounterACT Console, select **Apply** to save the policy.

Update Asset Identification Information to CMDB Template

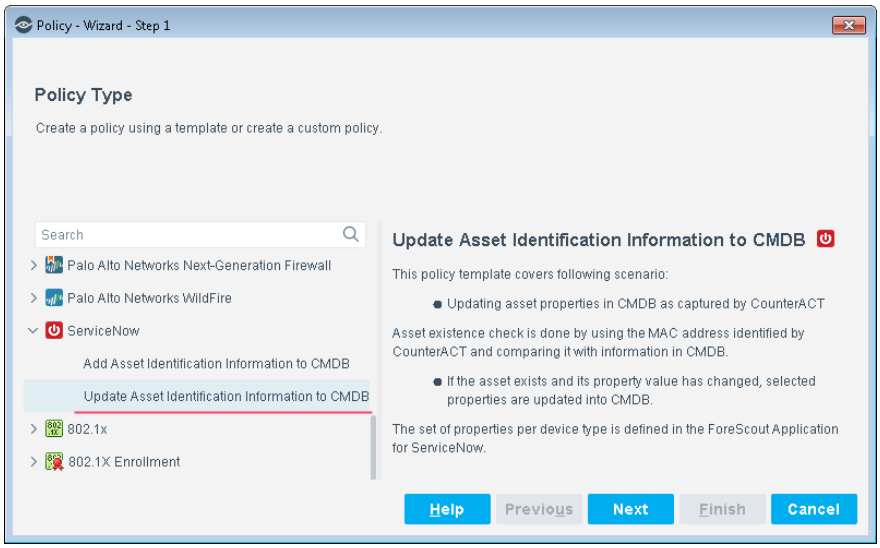
Use the Update Asset Identification Information to CMDB template to create policies that updates existing asset properties in CMDB, as captured by CounterACT. Asset existence check is done by using the MAC address identified by CounterACT and comparing it with information in CMDB.

- If the asset exists and its property value has changed, selected properties are updated in CMDB.

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

To use the Update Asset Identification Information to CMDB policy template:

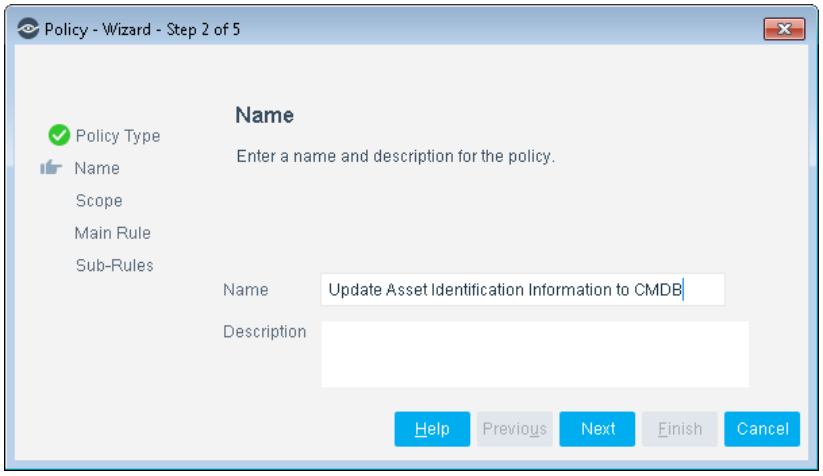
1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **ServiceNow** folder and select **Update Asset Identification Information to CMDB**. The Update Asset Identification Information to CMDB pane opens.



4. Select **Next**. The Name pane opens.

Name the Policy

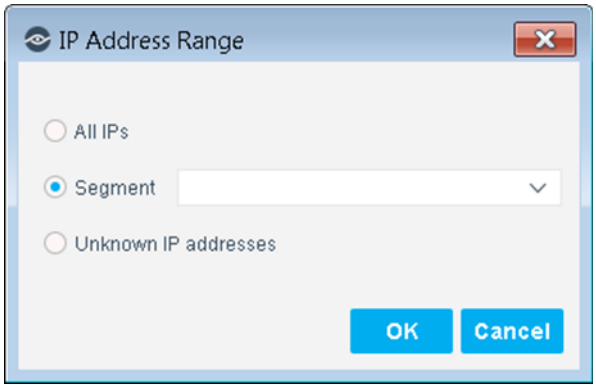
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - 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 is verifying and which actions will 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.
6. Select **Next.** The Scope pane and IP Address Range dialog box opens.

Define which Devices will be Inspected - Policy Scope

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 page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

  Not applicable for this policy template.

Filter the range by including only certain CounterACT groups and/or by excluding certain devices or users or groups when using this policy.

8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**. The Main Rule pane opens. Continue to the next section.

How Devices are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle devices defined in the policy scope.

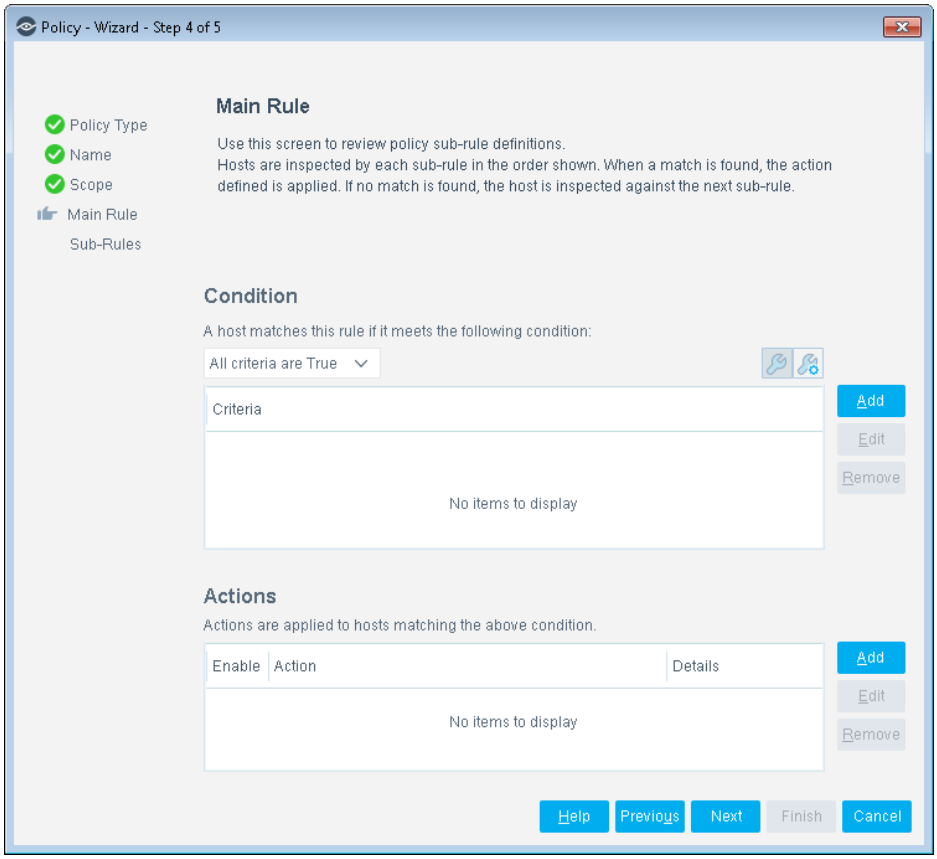
Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with hosts after initial detection and handling, streamlining separate detection and actions into one automated sequence.

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.

Main Rule

The main rule of this policy detects admission events, by default there are no rules in this pane. However, you can add to suit your needs:

- Host Status in CMDB



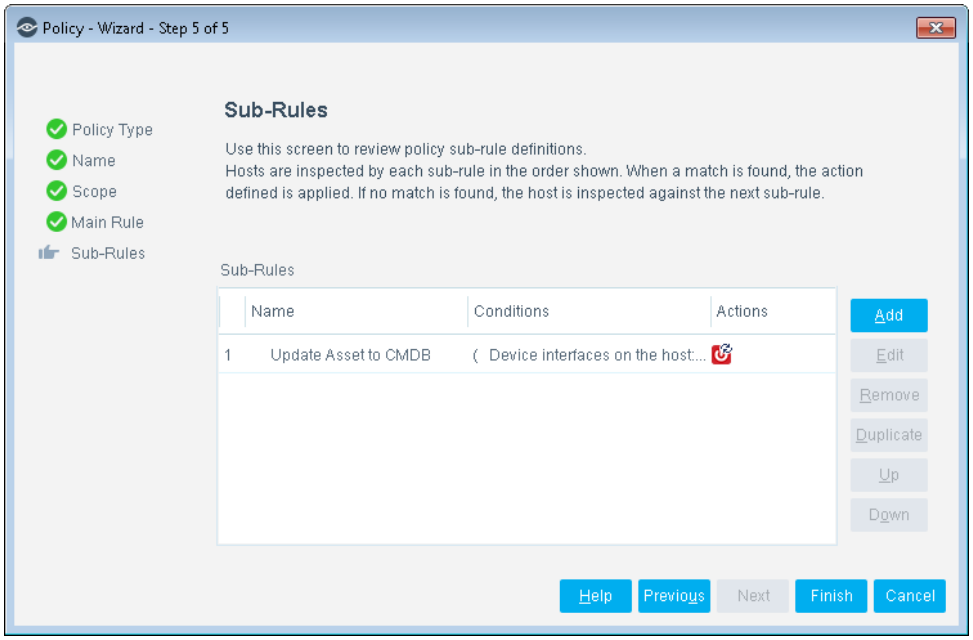
10. The Condition Criteria section is populated by default.

11. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties and Policy Actions sections.

12. Select **Next**. The Sub-Rules pane opens.

Sub-Rules

The sub-rules of the Add Asset Identification Information to CMDB policy lists the items CounterACT is to check when applying the Main Rule.



13. Double-click the Update Asset to CMDB sub-rule to open it. The Policy: [Name of Update Asset Identification Information to CMDB policy] Sub-Rule: Update Asset to CMDB dialog box opens.
14. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties and Policy Actions sections.
15. Select **OK**. In the Policy: [Name of Update Asset Identification Information to CMDB policy] Sub-Rule: Update Asset to CMDB dialog box, select **OK**.
16. Repeat steps 12 - 14 to make changes in other sub-rules.
17. In the Sub-Rules pane of the Policy Wizard, select **Finish**.
18. On the CounterACT Console, select **Apply** to save the policy.

Create Custom ServiceNow Policies

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

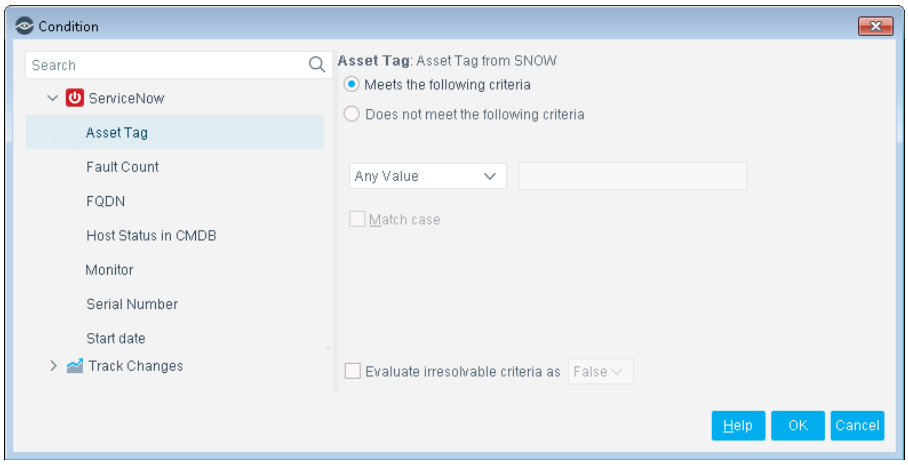
- Conditions based on host property values. CounterACT detects hosts with property values that match the conditions of the rule. Several conditions based on different properties can be combined using Boolean logic.
- Actions can be applied to hosts that match the conditions of the rule.

To create a custom policy:

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

Policy Properties

In addition to the bundled CounterACT 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 CounterACT properties:

1. In CounterACT, navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the **ServiceNow** folder in the Properties tree.

The following default property comes with the ServiceNow Module:

Host Status in CMDB	Checks whether or not the MAC address on a device exists in the ServiceNow CMDB.

To learn more about the ServiceNow properties, see the ServiceNow Helsinki User Guide*.*

3. When finished, select **OK**.

Policy Actions

In addition to the bundled CounterACT 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 would allow your mappings between CounterACT existing properties and ServiceNow table columns to occur.

To access the ForeScout Extended Module for ServiceNow actions:

1. In the CounterACT Console, navigate to the Actions tree from the Policy Conditions dialog box.
2. Expand the **ServiceNow** folder in the Actions tree. The following actions are available.

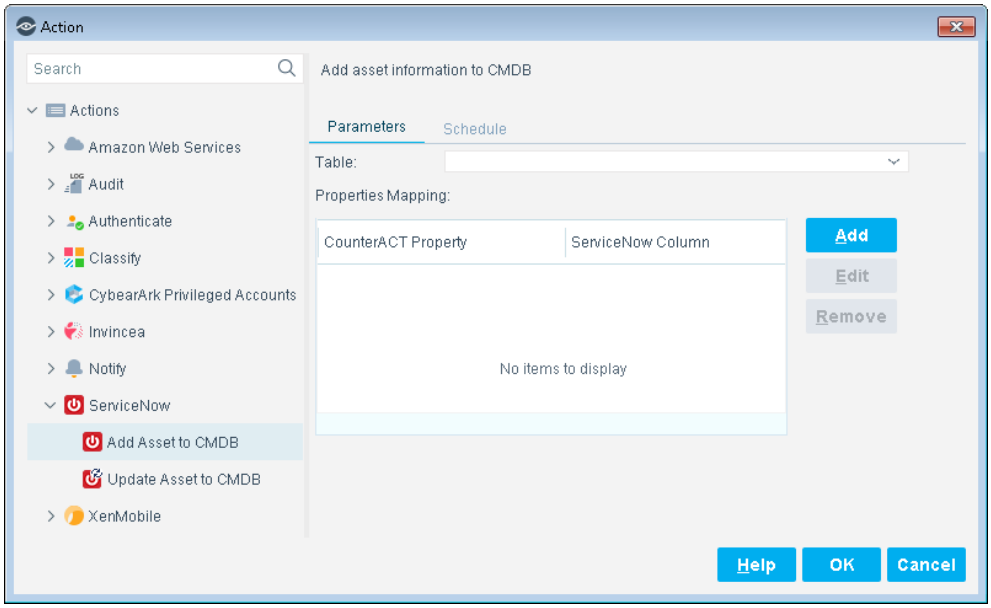
ServiceNow - Add Asset to CMDB	Add device properties to ServiceNow CMDB table.
ServiceNow - Update Asset to CMDB	Updates the table in CounterACT with ServiceNow properties. In order for this action to work, the device must exist in ServiceNow Configuration Item table.

Add or Update Asset to CMDB

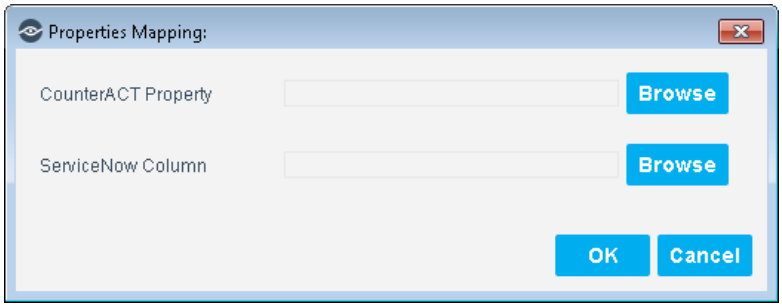
This section covers both how to add or update an asset to CMDB.

To create an Add to Table action in a CounterACT policy:

1. Create or edit a policy, and then **Edit** policy Actions.
2. In the Actions tree, select **ServiceNow** and then select **Add Asset to CMDB** or **Update Asset to CMDB**. The Parameters tab opens. Use this tab to map CounterACT properties to ServiceNow table columns. These will be used within the scope of the selected policy.



3. Select a **Table** from the drop-down.
4. Select **Add** to configure the CounterACT property to the ServiceNow Column. The Properties Mappings dialog box opens.



5. Map the CounterACT Property to the same or equivalent in the ServiceNow table. Select **Browse**, and select a CounterACT Property. Select **OK**.
6. Mapping the ServiceNow Column is the second part of properties mapping. This is to associate the CounterACT Property to a ServiceNow column located in a ServiceNow table. Select **Browse**. The column list from ServiceNow opens. Select a **ServiceNow** table column and then select **OK**.
7. The results of your mapping displays in the Parameters tab of the Actions dialog box. Repeat steps 3-5 to map other properties.
8. (Optional) Select the **Schedule** tab. You can use these standard action scheduling options to further customize message delivery. For example, you can choose the **Customize action start time** option to delay message delivery, or to limit the duration of repeated or regularly scheduled messages.
9. In the Actions dialog box, select **OK**.

Using the ServiceNow Extended Module

Once the ServiceNow Module has been configured, you can view and manage the virtual devices from Asset Inventory view in the CounterACT 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

Access the Asset Inventory

To access the inventory:

1. Log in to the CounterACT Console and select the **Asset Inventory** tab.
2. In the Views pane, expand the **ServiceNow** folder.
3. Select an item and the details display in the Hosts tab.

Access the Home Tab

To access the Home tab:

1. In the CounterACT Console, select the Home tab.
2. In the Views tree, expand **ServiceNow**.
3. Select an item in the Detections pane. The Profile, Compliance and All policies tabs display the information related to the host selected.

Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

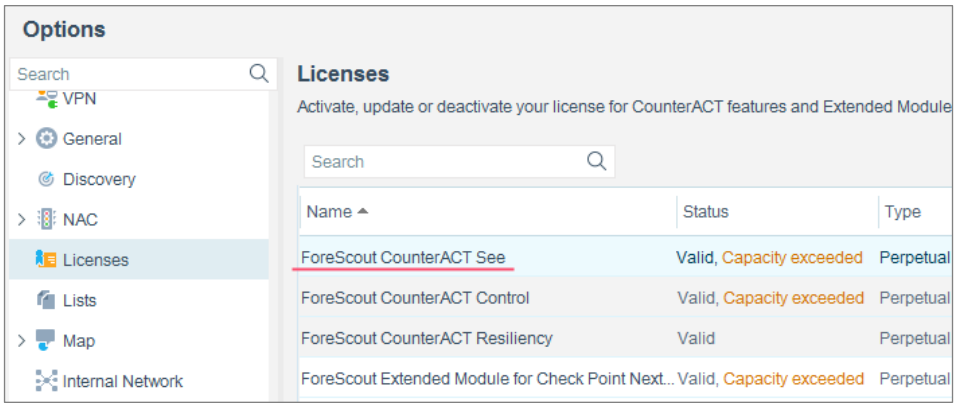
Documentation Portal

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

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21