FORESCOUT

Forescout

Hybrid Cloud Module: VMware NSX Plugin

Configuration Guide

Version 1.2.1

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

2020-05-21 17:07

Table of Contents

About VMware NSX Integration

The VMware NSX® Plugin is a component of the Forescout Hybrid Cloud Module. See Hybrid Cloud Module Information for details about the module.

The VMware NSX Plugin provides integration with the VMware NSX Network Virtualization and Security Platform. VMware NSX is an integral part of VMware's Software Defined Data Center (SDDC) deployment that delivers micro-segmentation and granular security to the individual workload, thus enabling a more secure data center.

This integration provides users control functionality for virtual endpoints that are part of the data center managed by VMware vCenter® and VMware NSX. Using the capabilities offered by this integration, you can apply micro-segmentation on virtual machines (VM) based on user-defined security policies. For example,

- Forescout policies can be written based on OS patch status and, if needed, vulnerable VMs can be segmented by applying a security group that disallows all communication to and from that virtual endpoint.

About Certification Compliance Mode

Forescout Hybrid Cloud Module: VMware NSX Plugin supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation 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 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 module.

Use Cases

The primary use-case is to provide classification and compliance of virtual endpoints. Some examples include:

- Based on the security posture (this is user-defined based on some criteria), a user can write policies to apply the correct security tag or security group to one or more virtual machines. See Working with VMware NSX Policy Templates.
- A user can make sure that specific types of virtual endpoints, for example, production workloads, have the correct security tag or security group setting. See Applying NSX Actions.

Additional VMware Documentation

You should be familiar with virtualization concepts and the VMware environment in particular when working with this plugin. Installation, configuration, and general guides can be found at:

https://www.vmware.com/support/pubs/nsx_pubs.html

https://www.vmware.com/support/pubs/

About this Plugin

The Forescout VMware NSX Plugin interfaces with VMware® NSX™ Manager™ that provides the management plane of NSX. NSX Manager provides the single point of configuration and REST API entry-points. The NSX Manager is installed as a virtual appliance on an ESX™ host in a VMware vCenter Server® environment. NSX Manager and vCenter have a one-to-one relationship, for example, for every instance of NSX Manager, there is one vCenter Server.

The NSX Plugin leverages APIs to assign a virtual machine to a security group, security tag, or both. Security groups can have dynamic membership based on criteria such as security tags, VM name, or logical switch name. For example, all VMs that have the security tag "web" are automatically added to a specific security group destined for Web servers. After creating a security group, a security policy is applied to that group.

The security group is the primary means to achieve micro-segmentation, providing secure east-west communication and providing limitations on that communication. Within the Forescout platform, a user can apply or remove a security group (or tags) for a VM based on defined policies.

Dependency on Forescout VMware vSphere Plugin

VMware vCenter interfaces with the Forescout VMware vSphere Plugin. The vSphere Plugin provides visibility into an enterprise data center infrastructure by pulling in information about the ESXi hosts and VMs. Since VMWare NSX is a network virtualization technology that provides micro-segmentation capabilities for VMs, it is recommended to use the Forescout NSX Plugin in conjunction with the vSphere Plugin.

The Forescout platform uses the vSphere Plugin to pull information about ESXi hosts and VMs and populates various relevant properties such as guest OS, hardware details, VM name, etc. Based on VM classification, users can then use the NSX Plugin to micro-segment the VM based on policies.

The NSX Plugin can also automatically obtain the vCenter information that is configured as part of the vSphere Plugin. It is recommended that the NSX Plugin be used in conjunction with the vSphere Plugin.

What to Do

This section describes steps you should take to set up your system when integrating with VMware environments:

1. Verify that the system requirements are met. See Requirements.
2. Define Forescout Users in the VMware Environment.
3. Configure the Plugin.
4. Working with VMware NSX Policy Templates.
5. Using the VMware NSX Plugin to manage virtual devices.

Requirements

This section describes system requirements, including:

- Forescout Requirements
- Network Requirements
- Supported Vendor Requirements

Forescout Requirements

The plugin requires the following Forescout releases and other components:

- Forescout version 8.1.
- Hybrid Cloud Module version 2.0, with the VMware NSX component running.
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

Network Requirements

- The 443/TCP port must be open on the enterprise firewall to support communication between the Forescout platform and the NSX Manager
- NSX server certificate (self-signed acceptable)

  See Import SSL Server Certificate.

Supported Vendor Requirements

- VMware NSX®
- VMware vSphere®

- The following VMware licenses are required to work with the plugin.
  - VMware NSX® (standard)
  - VMware vSphere® Enterprise Plus Edition™
  - VMware vCenter Server® (standard)

Define Forescout Users in the VMware Environment

The plugin communicates with the VMware vCenter server to retrieve information on virtual machines, and to apply Forescout actions to them. Before you configure and test this connection in the Forescout platform, define a user or group of users with the required permissions in the VMware environment. The plugin uses these credentials to log in to VMware servers. Define these users as follows:

- Define a NSX user role that includes the Security Administrator permissions required for the Forescout platform.
- Define users and assign this role to them.

Details on configuring roles and users can be found in the VMware vSphere Security Hardening Guide. Specific steps required to create a user are provided below.

Define a User Role for NSX

The NSX Plugin supports all of the types of user roles listed here:

- **Enterprise Administrator** – NSX operations and security.
- **NSX Administrator** – NSX operations only, for example, install virtual appliances, configure port groups.
- **Security Administrator** – NSX security only, for example, define data security policies, create port groups, or create reports for NSX modules. It is recommended that you have a Security Administrator user for the Forescout VMware NSX Plugin.
- **Auditor** – Read only. It is required that you have an Auditor user for the Forescout VMware NSX Plugin.

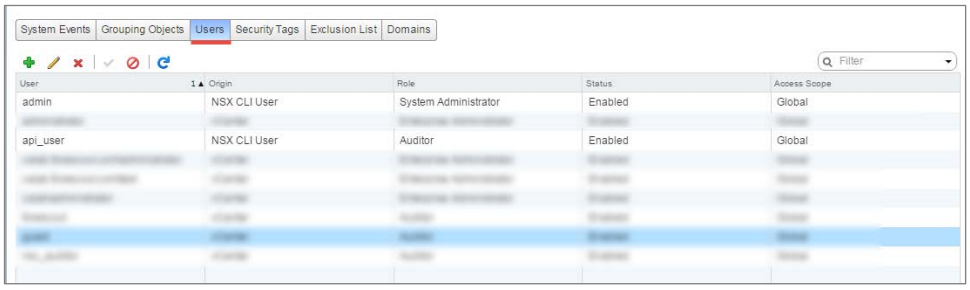
To define NSX Users and Permissions the NSX Manager:

The following steps use VMware NSX 6.2 as an example.

1. Log in to NSX as an administrator.
2. Go to the VMware NSX Documentation Center.

   The NSX Users and Permissions by Feature page of the VMware NSX 6.2 Documentation Center opens in a browser.

3. Follow the instructions listed for user management. Your end result should be similar to the following:



Configure the Plugin

This section describes the steps required to configure the VMware NSX Plugin.

- Import SSL Server Certificate
- Connect the NSX Plugin to a Server
- Test the VMware Server Connection

The following credentials are required for configuring the NSX Plugin:

1. *Connection to NSX Manager*. You need to provide a username and password for the NSX Manager.
2. *VMware vCenter Server credentials*. You need the vCenter Server username and password. You can configure the vCenter username and password or, if the Forescout VMware vSphere Plugin is installed and configured, the username and password from that configuration can be used.

Import SSL Server Certificate

You need to import a NSX SSL server certificate to the managing appliance.

1. Go to the VMware NSX 6 Documentation Center.
2. Follow the instructions on generating a SSL Certificate.

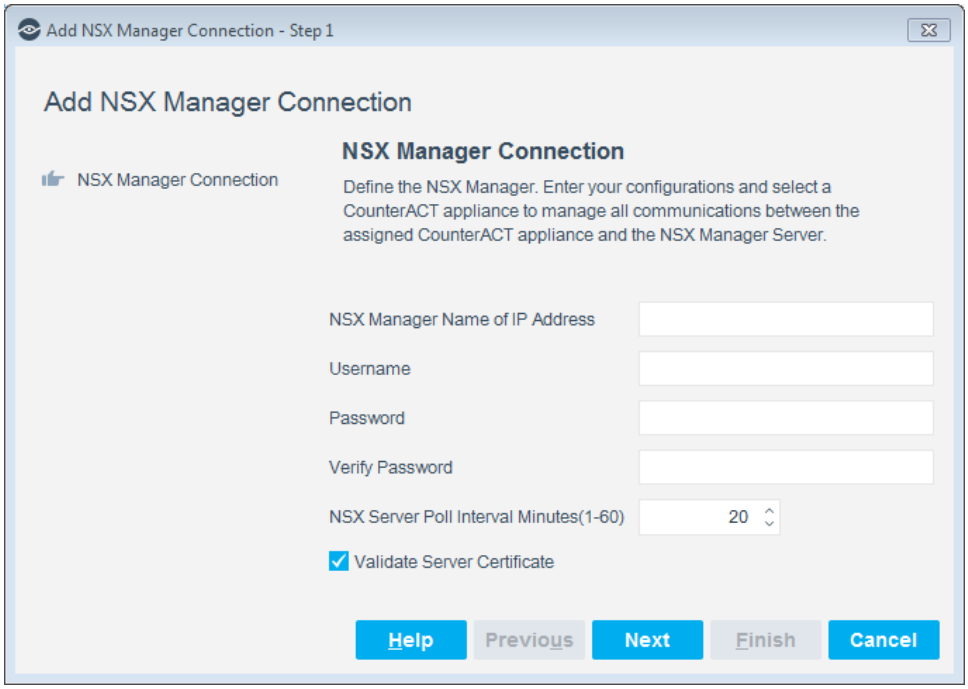
Connect the NSX Plugin to a Server

You need to map CounterACT® Appliances to a VMware NSX connection. Each CounterACT device communicates with a single VMware NSX connection. If you define more than one VMware NSX connection, you can assign individual CounterACT Appliances to each connection.

Removing a configured VMware vCenter server stops host discovery and property learning of virtual machines hosted by this server, but any actions remain enabled.

To connect the NSX Plugin to a server:

1. In the Console, select **Options** from the **Tools** menu.
2. In the left pane, select **VMware NSX**. The VMware NSX pane opens.
3. Select **Add**.

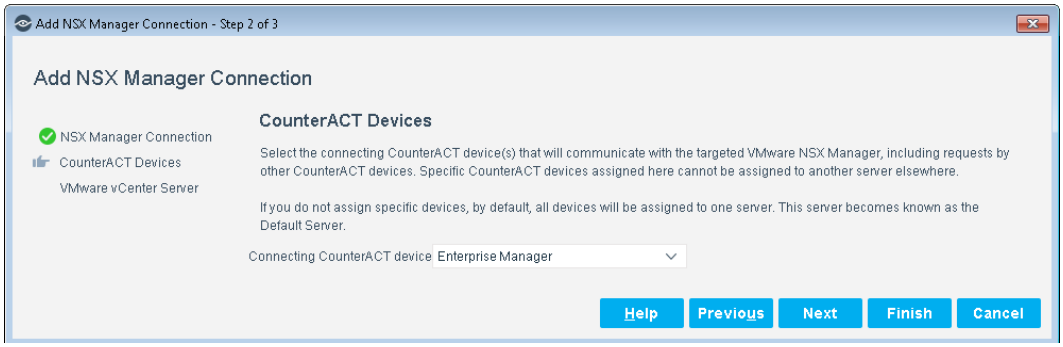


4. Define the NSX Manager Connection parameters.

NSX Manager Name or IP Address	Enter the hostname, a Fully Qualified Domain Name (FQDN) or the IPv4 address of the NSX Manager.
Username	Enter the username required to log in to the NSX Manager. For details, see Define Forescout Users in the VMware Environment.
Password	Enter the password required to log in to the NSX Manager.
Verify Password	Re-enter the password to verify it.
NSX Server Poll Interval Minutes (1-60)	Set the frequency (in minutes) at which the NSX Manager polls the server. The default setting is every 20 minutes.

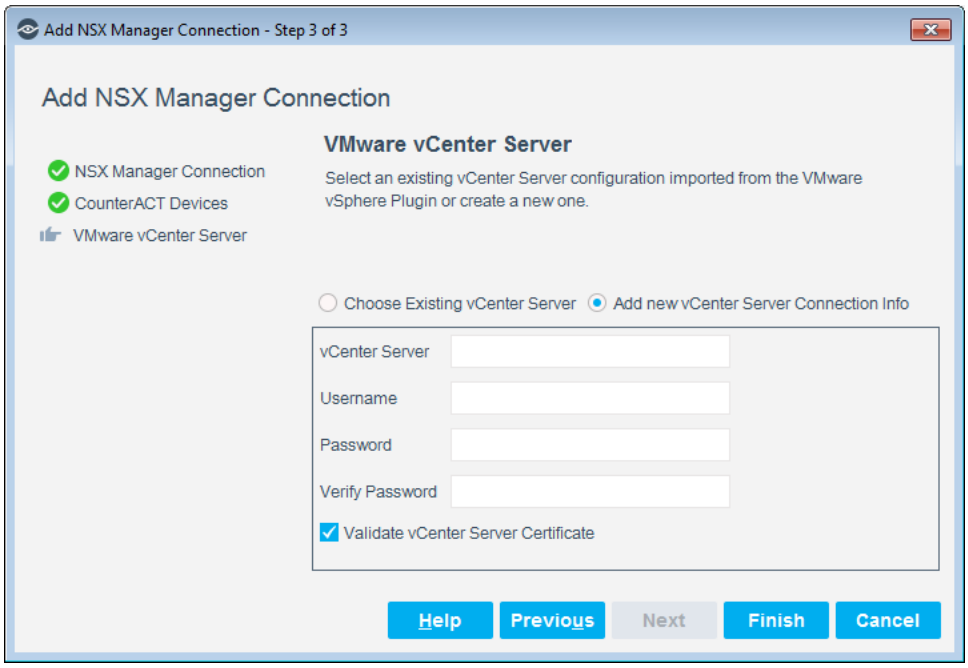
Validate Server Certificate	Select this option to validate the identity of the third-party server before establishing a connection, when the Plugin communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed: ▪ Self-signed server 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 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 *Forescout Administration Guide*.

5. Select **Next**.



6. Select the CounterACT device to connect to this server. The selected CounterACT device is the only device that communicates with the server.
   - When the Enterprise Manager is defined as the Connecting CounterACT device, endpoints without an IP address that the plugin detects are not displayed in the Console Detections pane.
   - To manage endpoints without an IP address, the Connecting CounterACT device must be an Appliance, and not the Enterprise Manager.

7. Select the Connecting CounterACT device and then select **Next**.



8. Configure the NSX Manager to connect to a vCenter server.

Choose Existing vCenter Server	If you already have a configured Forescout vSphere Plugin, select this option and then select the VMware vCenter server from the **VMware vCenter Selection** drop-down list.
Add new VMware vCenter Server Connection Info	By default, this option is selected. If the Forescout vSphere Plugin is not yet installed and configured, select this option.
vCenter Server	Enter the Fully Qualified Domain Name (FQDN) or the IPv4 address of the vCenter server.
Username	Enter the username required to log in to the vCenter server. For details, see Define Forescout Users in the VMware Environment.
Password	Enter the password required to log in to the vCenter server.
Verify Password	Re-enter the password to verify it.

Validate vCenter Server Certificate	Select this option to validate the identity of the third-party server before establishing a connection, when the Plugin communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed: ▪ 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 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 *Forescout Administration Guide*.

9. Select **Finish**. You are now ready to add these properties to your customized policy.

The best practice is to perform a **Test** after setting up a connection. See Test the VMware Server Connection.

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

1. Select **Tools** > **Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Test the VMware Server Connection

You can test NSX Plugin communication with a VMware server.

To test the communication:

1. In the VMware NSX pane, select a VMware server defined in the Forescout platform.
2. Select **Test**. Using the configured settings, the Forescout platform attempts to connect to the server.

   The Test results are displayed.

Working with VMware NSX Policy Templates

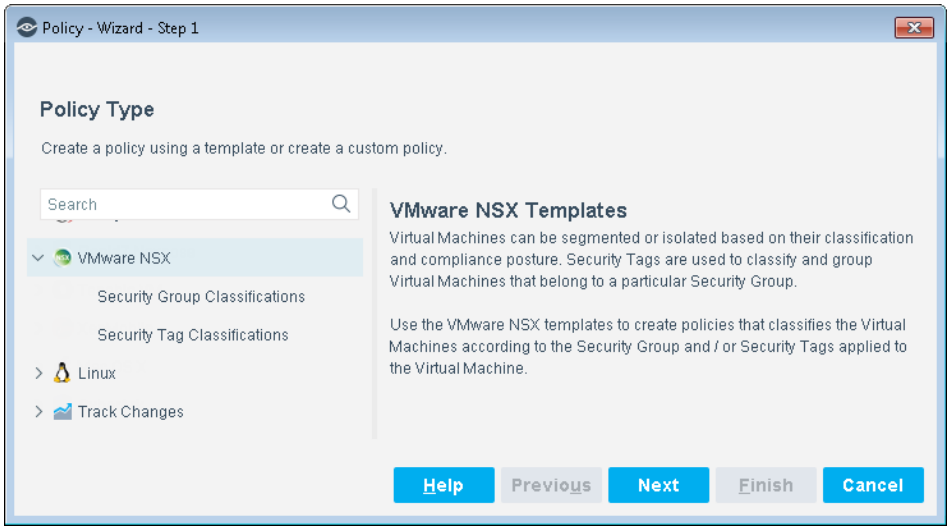
Forescout templates help you quickly create important, widely used policies that easily control endpoints and can guide users to compliance. These policies can be viewed in the Console's Policy Manager.

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.

Predefined actions – instructions regarding how to handle endpoints – are generally disabled by default when working with templates. You should only enable actions after testing and fine-tuning the policy.

This plugin provides the following policy templates used to detect, manage, and remediate VMware virtual machine endpoints.

- Security Group Classifications Template – generates a Forescout policy for classifying virtual machines based on security tags.
- Security Tag Classifications Template – generates a Forescout policy for classifying virtual machines based on security tags.



It is recommended that you have a basic understanding of Forescout policies before working with the templates. Refer to the Forescout Templates and Policy Management chapters of the Forescout Administration Guide.

Security Group Classifications Template

A Security Group can contain multiple object types and have dynamic membership criteria based on Security Tags.

A security group classification can be role-based (for example, testing or development) or function-based (for example, web, application, or database tier).

Use this template to create a Security Group Classification policy that classifies the virtual machines with security group information. Then assign to the Security Group

the Security Tags that define what properties you want checked on the virtual machines.

Prerequisites

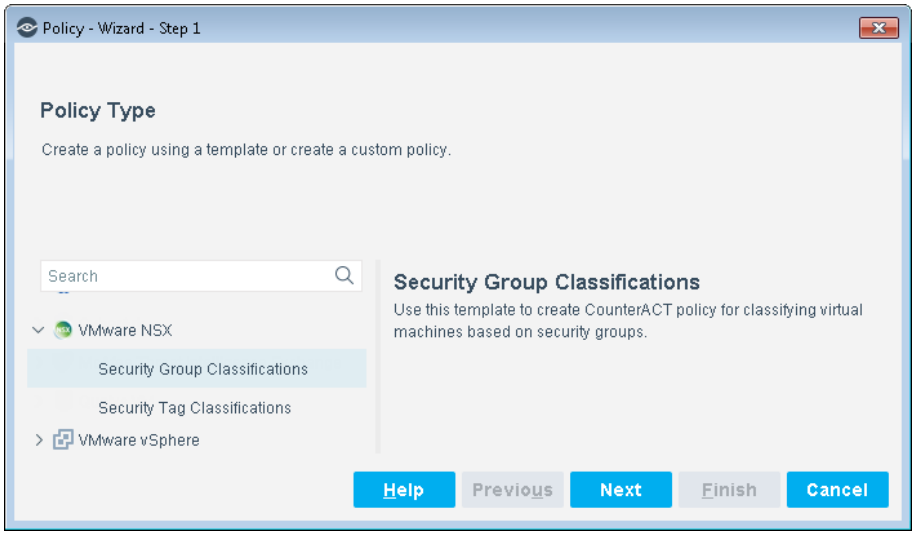
Before you run a policy based on this template, verify that you have configured the NSX Plugin so that the Forescout platform can communicate with its associated VMware vCenter server.

Create a Security Group Classification Policy

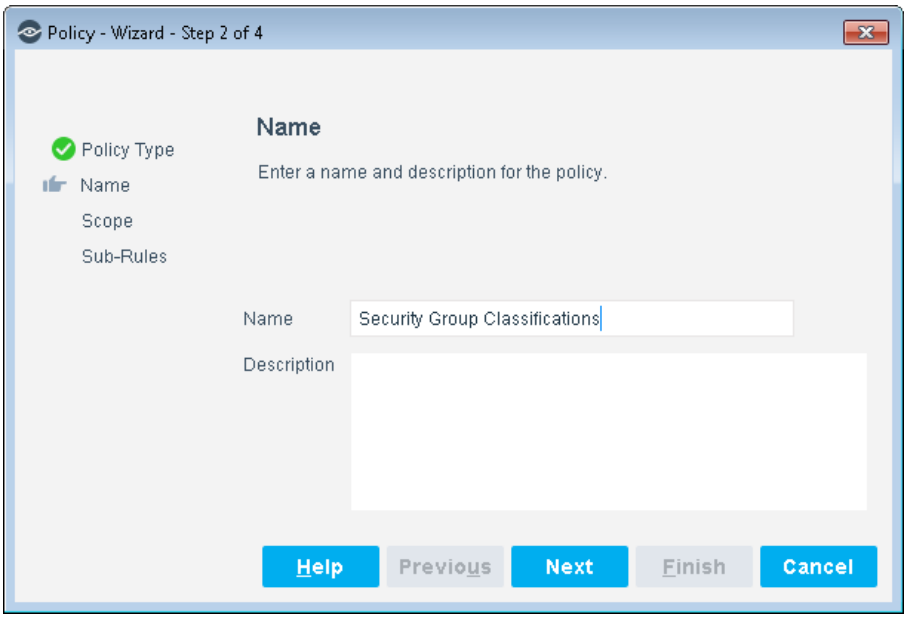
This section describes how to create a policy based on the Security Group Classifications Policy template.

To create the policy:

1. In the Console, select **Policy**.
2. Select **Add**. The Policy Wizard opens.
3. Select **VMware NSX** and then select **Security Group Classifications Template**.



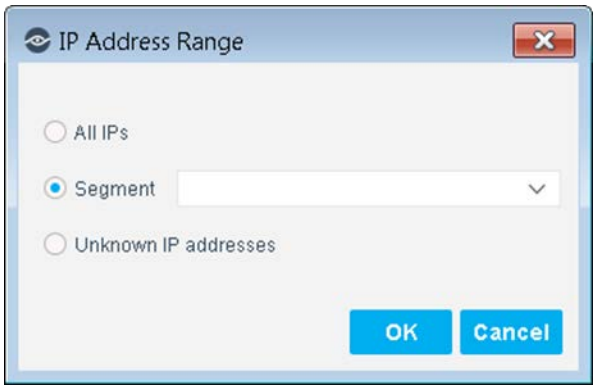
4. Select **Next**.



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 are taken.
   - Ensure that the name indicates whether the policy criteria needs to be met or not.
   - Avoid having another policy with a similar name.

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

6. Select **Next**. Both the Scope pane and the IP Address Range dialog box 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 added range is displayed in the Scope pane.
9. Select **Next**. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See How Endpoints are Detected and Handled for details of default policy logic.
10. Review the sub-rule conditions and actions, and then select **Finish**.
11. In the Policy Manager, select **Apply** to save the policy.
12. Select **Start** to execute the policy.

How Endpoints are Detected and Handled

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

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

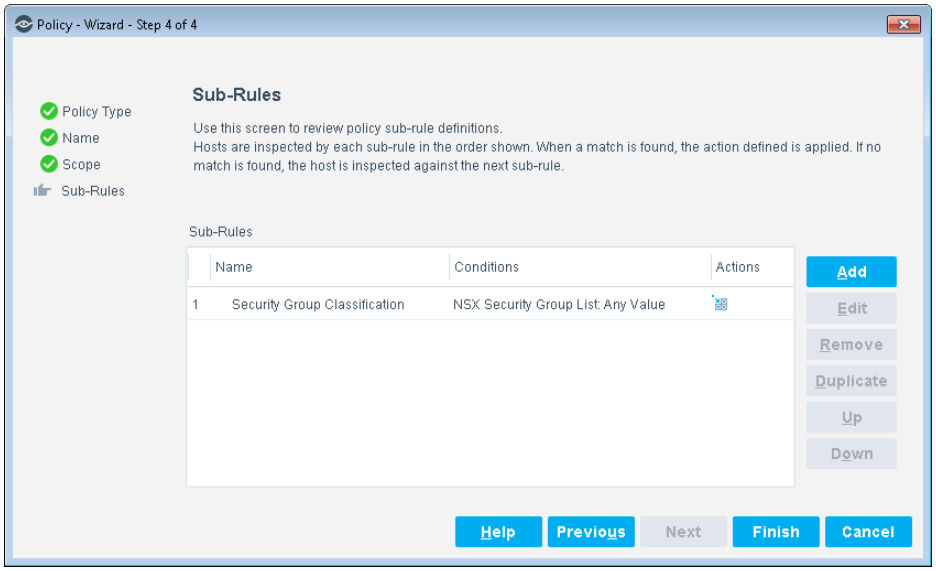
Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

By default, this template only inspects endpoints that are members of the VMware virtual machines group.

Sub-Rules

Sub-rules of the policy evaluate the endpoint to classify the virtual machines according to the existing security group that the virtual machines are assigned to. Sub-rule actions are enabled by default.

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.



Condition	Definition
NSX Security Group List: Any Value	Lists the existing security groups that the VM belongs to.

Security Tag Classifications Template

Use this template to create a Security Tag Classifications policy to define what properties (including existing security tags) you want to check for assessing virtual machine vulnerability.

Define the tags and then assign them to a virtual machine. Once the Security Tags are associated to a virtual machine, the tags are then associated to a specific Security Group.

Prerequisites

Before you run a policy based on this template, verify that you have configured the NSX Plugin so that the Forescout platform can communicate with one or more vCenter servers.

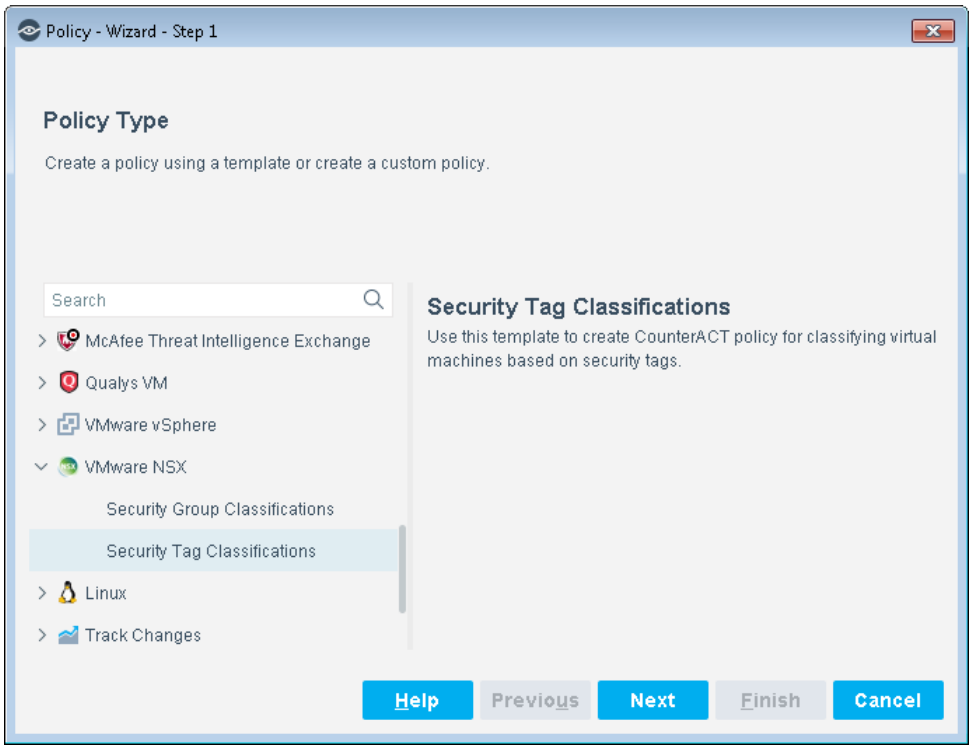
Create a Security Tag Classification Policy

This section describes how to create a policy based on the Security Tag Classification Policy template.

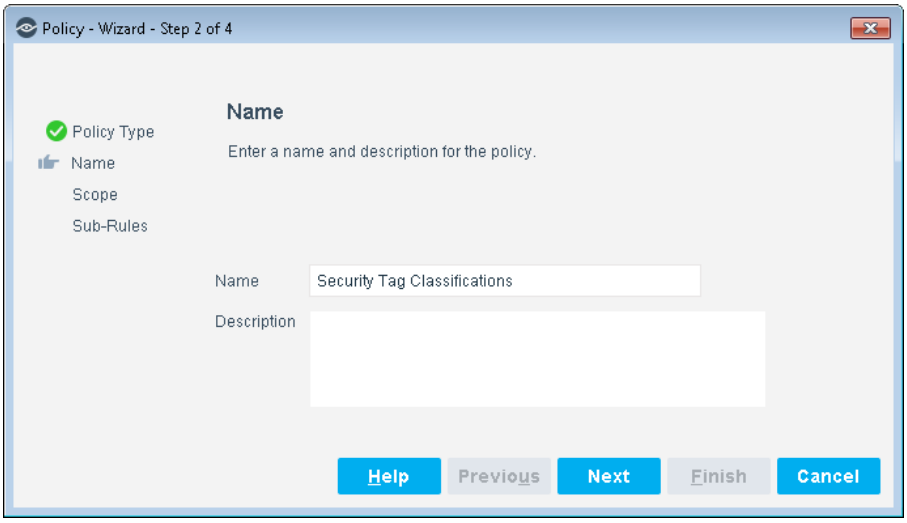
To create the policy:

1. In the Console, select **Policy**.
2. Select **Add**. The Policy Wizard opens.

3. Select **VMware NSX** and then select **Security Tag Classification**.



4. Select **Next**.

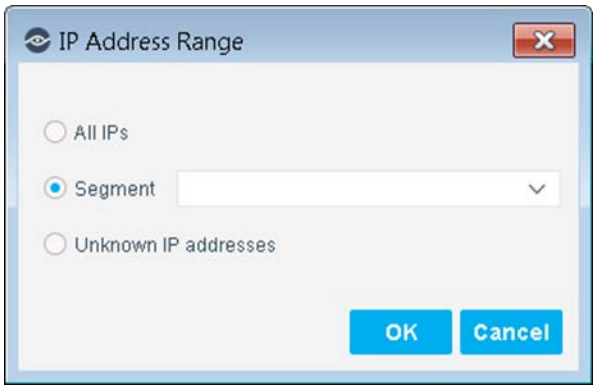


5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your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

- Ensure that the name indicates whether the policy criteria need to be met or not.
- Avoid having another policy with a similar name.

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

6. Select **Next**. Both the Scope pane and the IP Address Range dialog box 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 added range is displayed in the Scope pane.
9. Select **Next**. The Sub-Rules pane opens and lists the default rules of the policy generated by the template. Rules can be modified at this point if required. See How Endpoints are Detected and Handled for details of default policy logic.
10. Review the sub-rule conditions and actions, and then select **Finish**.
11. In the Policy Manager, select **Apply** to save the policy.
12. Select **Start** to execute the policy.

How Endpoints are Detected and Handled

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

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

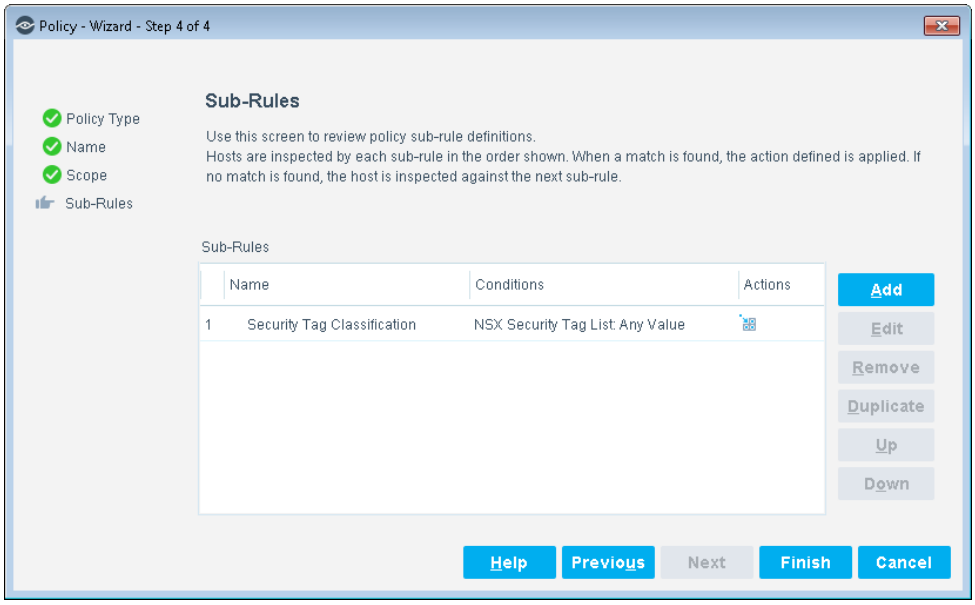
Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

By default, this template only inspects endpoints that are members of the VMware virtual machines group.

Sub-Rules

Sub-rules of the policy evaluate the endpoint to classify the virtual machines according to the security tag assigned to the virtual machines. Sub-rule actions are enabled by default.

By default, the policy is evaluated every eight hours, and is applied to newly discovered endpoints.



Condition	Definition
NSX Security Tag List: Any Value	Lists the existing security tag string assigned to the VM.

Create Custom Policies

Custom Forescout policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy to instruct the Forescout platform to apply a policy action to hosts that match (or do not match) conditions based on host property values. You may need to create a custom policy to deal with issues not covered in the policy templates provided by this plugin.

Properties

Policy properties let you instruct the Forescout platform to detect hosts with specific attributes. For example, create a policy that instructs the Forescout platform to detect hosts running a certain operating system or with a certain application installed.

Actions

Policy actions let you instruct the Forescout platform to control detected devices. For example, assign a detected device to a quarantined VLAN or send the device user or IT team an email.

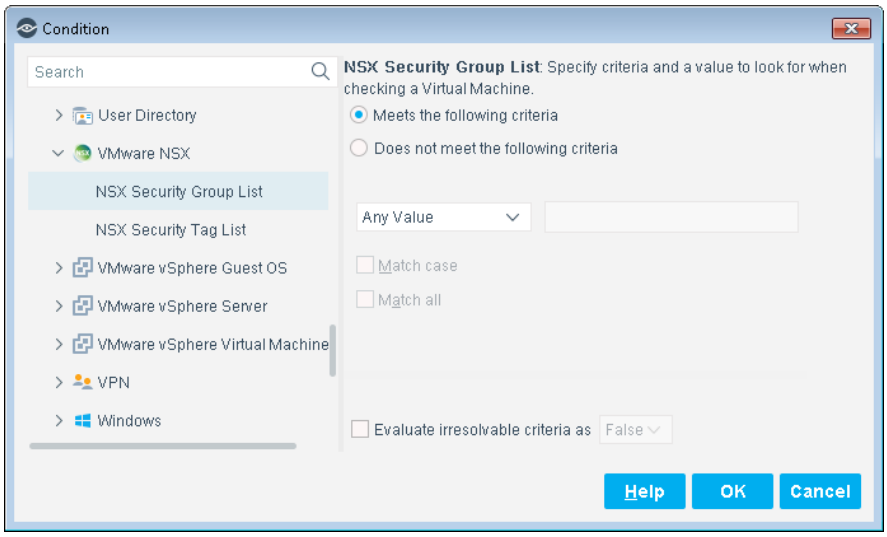
VMware NSX Plugin Properties and Actions

This plugin provides additional properties and actions that are useful for virtual device management. Use these properties and actions to construct customized policies for virtual device management.

For more information about creating custom policies, refer to the *Forescout Administration Guide*.

Detecting Virtual Devices – Host Properties

This section describes the host properties that are made available when the VMware NSX Plugin is installed.



NSX Security Group List	Specify criteria and a value to look for when checking a virtual machine.
NSX Security Tag List	Specify criteria and a value to look for when checking the Security Tags on a virtual machine.

Managing Virtual Devices – Policy Actions

This section describes the actions that are available when the VMware NSX Plugin is installed.

Action thresholds have been defined for some of these actions. These thresholds limit the percentage of endpoints managed by each Appliance to which the action can be applied simultaneously. For more information, refer to *Working with Action Thresholds* in the *Forescout Administration Guide*.

VMware NSX Actions

Add to Security Group	Add the virtual machine to the pre-defined security group. The Security group name is case sensitive.
Apply Security Tag	Add the pre-defined security tag to the virtual machine. The Security tag name is case insensitive.
Remove from Security Group	Remove the virtual machine from the pre-defined security group. The Security group name is case sensitive.
Remove Security Tag	Remove the pre-defined security tag from the virtual machine. The Security tag name is case insensitive.

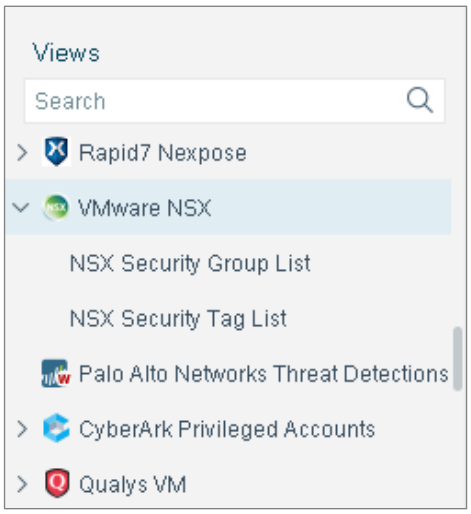
Using the VMware NSX Plugin

Once the VMware NSX Plugin has been configured, you can view and manage the virtual endpoints based on their association with a security group or security tag from the Inventory view in the Console. The Inventory lets you:

- View virtual machine endpoints that were detected with specific attributes
- Incorporate inventory detections into policies

To access the inventory:

1. In the Console, select **Inventory**.
2. Go to the Inventory entries related to this plugin.



Refer to *Working at the Console>Working with Inventory Detections* in the *Forescout Administration Guide* for information about how to work with the Forescout Inventory. See Additional Forescout Documentation for information on how to access the guide.

Applying NSX Actions

This section addresses how to use the NSX Actions.

If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl license to use these actions. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

To apply VMware NSX actions:

1. In the Console, select **Home**.
2. In the Detections pane, right-click an item, select **VMware NSX**, and then select one of the available actions.

Add to Security Group	Adds the selected VM to a security group that is pre-defined in the NSX Manager. This action can be applied via policy as well. For example, you can add web servers running on Windows to a windows_web_server security group.

Apply Security Tag	Based on the security settings defined in a policy, you can apply a security tag to classify the selected virtual machine. In the NSX Manager, the security tag would normally be associated with a security group. For example, you can define a security group for web servers and add VMs to that security group that have a “web” security tag. The “web” security tag can be applied from the Forescout platform based on some user defined policy.
Remove from Security Group	Removes the selected VM from the security group it is currently assigned to. Note that when the virtual machine is assigned to a security group using VMware criteria, for example, VM Name, the virtual machine can only be removed from the security group by removing the corresponding VMware criteria. This means the virtual machine cannot be removed from the security group using the Remove from Security Group action in the Forescout NSX Plugin.
Remove Security Tag	Removes the security tag from the selected virtual machine.

Hybrid Cloud Module Information

The VMware NSX Plugin is installed with the Forescout Hybrid Cloud Module.

The Forescout Hybrid Cloud Module provides visibility and control functions across physical and virtual devices that are on-premises and off-premises through the following plugin integrations:

- AWS Plugin
- Azure Plugin
- VMware NSX Plugin
- VMware vSphere Plugin

The Hybrid Cloud Module is a Forescout Base Module. Base Modules are delivered with each Forescout release.

The plugins listed above are installed and rolled back with the Hybrid Cloud Module.

Refer to the *Forescout Hybrid Cloud Module Overview Guide* for more module information, such as module requirements, upgrade, and rollback instructions.

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 Forescout Resources 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 Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Resources Page

The Forescout Resources page provides links to the full range of technical documentation.

To access the Forescout Resources page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation,** and search for documents.

Product Updates Portal

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

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer 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

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

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

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).