FORESCOUT

Forescout

pxGrid Plugin

Configuration Guide

Version 1.0

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

2020-05-07 15:06

Table of Contents

About the pxGrid Plugin **4**

How It Works **4**

Requirements **4**

What to Do **5**

Configure Cisco ISE **5**

Enable Communication 5
Determine the pxGrid Hostname 5
Enable pxGrid 6
Determine the User Account Approval Method 6
Create Policies in ISE 6
Generate Certificates 7

Configure the Forescout Platform **8**

Install the Plugin 8
Install the Certificates 9
Install the ISE Trusted Root Certificate 9
Install the pxGrid System Certificate 10
Configure the pxGrid Plugin 11
Test the pxGrid Plugin 12

Policies, Actions, and Properties **13**

Properties Provided by the Plugin 14
Clear the Applied ISE ANC Policy 15
Action Provided by the Plugin 16
Apply ISE ANC Policy 16

Considerations and Troubleshooting **18**

System Certificate Error 18
If the System Certificate Error Recurs 19
pxGrid Subscriptions Are Off 19
One ISE per Deployment 19
Failover Cluster 19
Action Issues 20
Host Issues 20

Additional ForeScout Documentation **21**

Documentation Downloads 21
Documentation Portal 22
Forescout Help Tools 22

About the pxGrid Plugin

Forescout's pxGrid Plugin integrates with existing Cisco ISE (Identity Services Engine) deployments so that you can benefit from Forescout visibility and assessment for policy decisions, while continuing to use ISE as an enforcement point. The pxGrid Plugin enables Forescout platform policies to detect ISE-related properties on endpoints, and to apply Cisco ISE ANC policies, including policies that assign Security Groups to devices.

This plugin is also known as the Cisco pxGrid Plugin.

To use the plugin, you should have a solid understanding of Cisco ISE concepts, functionality, and terminology, and understand how Forescout platform policies and other basic features work.

How It Works

The plugin uses certificates to securely communicate with Cisco ISE.

1. A Forescout platform policy or manual action instructs ISE to apply an ANC (Adaptive Network Control) policy to devices that the operator selects or that meet Forescout platform policy conditions.
2. ISE applies a Security Group to the devices that match the ANC policy.
3. Cisco switches are configured to allow or deny access to resources for specific Security Group Tags (SGTs).

Requirements

The plugin requires the following:

- Forescout version 8.1.x or 8.2.x, configured and running
  - If you are using Flexx licensing, you must have a valid Forescout eyeControl license to use the plugin-provided policy action. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses. To access the guide, see Additional ForeScout Documentation.
- Cisco ISE 2.4 or above, configured and running

  Due to ANC policy issues in Cisco ISE 2.6, version 2.6 is only supported if it has been upgraded to patch 2 or above.

- A Cisco ISE Plus license

  If you use DNA Center with ISE, you have a Cisco ISE Plus license.

- The ISE FQDN must be accessible to the Forescout Appliance
  - The FQDN is resolvable by the DNS server.

  - Port 8910 is permitted.
- Cisco switches must be configured for Dynamic Authorization Commands

What to Do

1. Verify that your environment meets the Requirements.
2. Configure Cisco ISE.
3. Configure the Forescout Platform.
4. Configure your Cisco switches to allow or deny access to resources for specific Security Groups.
5. In the Forescout Console, create and run a policy that:
   a. Detects the conditions for which an ANC policy must be applied
   b. Applies the appropriate ANC policy to devices that match those conditions

   Ensure that only one ANC policy is applied to each device.

   For information about creating policies, refer to the *Forescout Administration Guide*. To access the guide, see Additional ForeScout Documentation.
6. ISE applies the pre-defined Security Group to the devices, and allows or denies access to resources based on the Security Group.
7. ISE shares each device's ANC policy and Security Group information with the Forescout plugin. You can use these properties as conditions in other Forescout platform policies.

Configure Cisco ISE

- Enable Communication
- Create Policies in ISE
- Generate Certificates

Enable Communication

Enable communication between ISE and the Forescout platform.

Determine the pxGrid Hostname

To determine the pxGrid hostname:

1. In the Cisco ISE Admin portal, go to Administration > Deployment.
2. In the Deployment Nodes table, identify the hostname of the pxGrid persona.

Enable pxGrid

To enable Cisco ISE pxGrid:

1. Determine the pxGrid Hostname.
2. In the Deployment Nodes table, select the pxGrid hostname before doing each of the following steps:
   a. At the bottom of the *General Settings* tab, select **pxGrid**, and select **Save**.
   b. At the bottom of the *Profiling Configuration* tab, select **pxGrid**, and select **Save**.

Determine the User Account Approval Method

When the pxGrid Plugin is started, it receives the certificates that were generated in ISE and then installed in the Forescout platform. The plugin uses the certificates to create two user accounts in ISE for each Forescout Appliance.

- You can opt to automatically approve all certificate-based accounts:
  a. Go to Administration > pxGrid Services, and select the Settings tab.
  b. Select **Automatically approve new certificate-based accounts**.
- If automatic approval is not enabled, you will need to manually approve these user accounts in the Administration > pxGrid Services > All Clients tab the first time the plugin attempts to connect to ISE.

Create Policies in ISE

To work with Security Groups, define at least one ANC policy that assigns a Security Group name and numeric tag to devices.

If a rule assigns an Authorization Profile in addition to a Security Group, ensure that the Authorization Profile does not *assign a Security Group also.*

To add a new Security Group:

1. Go to Work Centers > TrustSec > Components.
2. In the Security Groups pane, select **Add**.
3. Enter a name for the new Security Group, and select **Submit**.

To add a new ANC policy:

1. Go to Operations > Adaptive Network Control > Policy List.
2. In the List pane, select **Add**.
3. Enter a name for the new list, select **QUARANTINE** as the action, and select **Submit**.

To add a new ISE Policy:

1. Go to Policy > Policy Sets.
2. At the right of the Default row, select the arrow: **>**.
3. To create a new rule, select the appropriate policy type to expand it, and select the plus sign: **+**.
4. You can change the new rule's Rule Name value to a meaningful name.
5. To open the Conditions Studio window, in the new rule's Conditions field, select the plus sign: **+**.
   a. In the top field of the Editor area, select **Click to add an attribute**.
   b. In the Attribute column, enter **anc**, and select **Session** (ANCPolicy Attribute).
   c. In the second field of the Editor area, select **Equals**.
   d. In the third field of the Editor area, select the appropriate ANC policy from the list.
   e. At the bottom of the window, select **Use**.
6. In the new rule's Security Groups field, select the appropriate Security Group name.
7. Select **Save**.

   *Be sure to select **Save** to save the configuration.*

Generate Certificates

Prepare two certificates for secure communication with the Forescout platform. If you have multiple ISE installations, be sure to do this on the installation that the pxGrid Plugin will integrate with.

Generate two certificates:

- a trusted root certificate
- a system certificate

To generate certificates:

1. In the Cisco ISE Admin portal, go to Administration > pxGrid Services, and select the Certificates tab.
2. In the *I want to* field, select **Generate a single certificate (without a certificate signing request)**.
3. Enter a Common Name and description.
4. Enter and confirm a password for the certificate.
5. To generate a trusted root certificate:
   a. In the *Certificate Download Format* field, select **Certificate in Privacy Enhanced Electronic Mail (PEM) format**.
   b. Select **Create**, and save the certificate locally.

c. From the zipped certificate file, extract the root certificate:
`CertificateServicesRootCA-`*{hostname}*`_.cer`**
where *{hostname}* is the pxGrid hostname.

See Determine the pxGrid Hostname.

6. To generate a system certificate:
   a. In the *Certificate Download Format* field, select **PKCS12 format**.
   b. Select **Create**, and save the certificate locally.
   c. From the zipped certificate file, extract the p12 certificate file:
   {CN}`_.p12`
   where *{CN}* is the Common Name you entered in step 3.

Configure the Forescout Platform

1. Install the Plugin
2. Install the Certificates
3. Configure the pxGrid Plugin
4. Test the pxGrid Plugin

Install the Plugin

To install the plugin:

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

   To identify your licensing mode, select **Help > About ForeScout** from the Console.
2. Download the plugin **`.fpi`** file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved plugin **`.fpi`** file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

The installation begins immediately after selecting Install and cannot be interrupted or canceled.

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

Some components are not automatically started following installation.

Install the Certificates

Install the certificates that were generated in ISE, and then restart the plugin.

- Install the ISE Trusted Root Certificate
- Install the pxGrid System Certificate

Install the ISE Trusted Root Certificate

To install the trusted root certificate:

1. In the Forescout Console, go to Options > Certificates > Trusted Certificates.
2. Select **Add**, and browse to the trusted root certificate saved in the Generate Certificates section, step 5c:

   `CertificateServicesRootCA-`*{hostname}*`_.cer`**

   where *{hostname}* is the pxGrid hostname.

   See Determine the pxGrid Hostname.

3. Select **Apply**.
4. Ensure that **Enable trusting this certificate** is selected.
5. Select **Next**, and then select **Next**.
6. In the Trusted for Subsystems window, select **Subsystems selected below**, and then **Clear All**.
7. From the list, select **pxGrid**, and then select **Next**.
8. In the Trusted for Devices pane, select **CounterACT devices selected below**, and select the CounterACT device that you will connect to Cisco ISE in the Configure the pxGrid Plugin section.

9. Complete the wizard, and select **Apply**.
10. Select **Yes** and **OK**.

Install the pxGrid System Certificate

To install the system certificate:

1. Go to Options > Certificates > System Certificates.
2. Select **Add from PKCS#12**, and browse to the system certificate saved in the Generate Certificates section, step 6c:

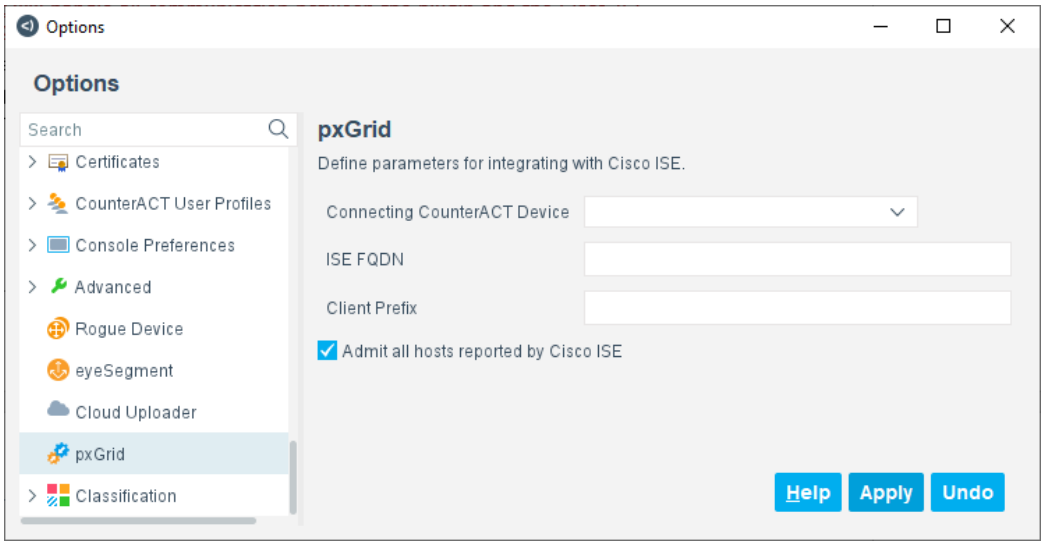
   {CN}`_.p12`

   where *{CN}* is the Common Name you entered in step 3 of that section.
3. Select **Next**.
4. Enter the certificate password, and select **OK**.
5. Ensure that the certificate details are correct, and select **Next**.
6. In the Issuer Chain table, select the certificate whose subject does ***not*** begin **`CN=Certificate Services`**, and select **Remove** to remove this self-signed root certificate.
7. Select **Next**.
8. In the *Used for Subsystem* field, select **pxGrid**, and select **Next**.
9. Enter a description, and select **Enable presenting this certificate**.
10. Complete the wizard, and select **Apply**.
11. Select **Yes** and **OK**.
12. After the certificates are installed, restart the pxGrid Plugin for the changes to apply.

Configure the pxGrid Plugin

To configure the plugin:

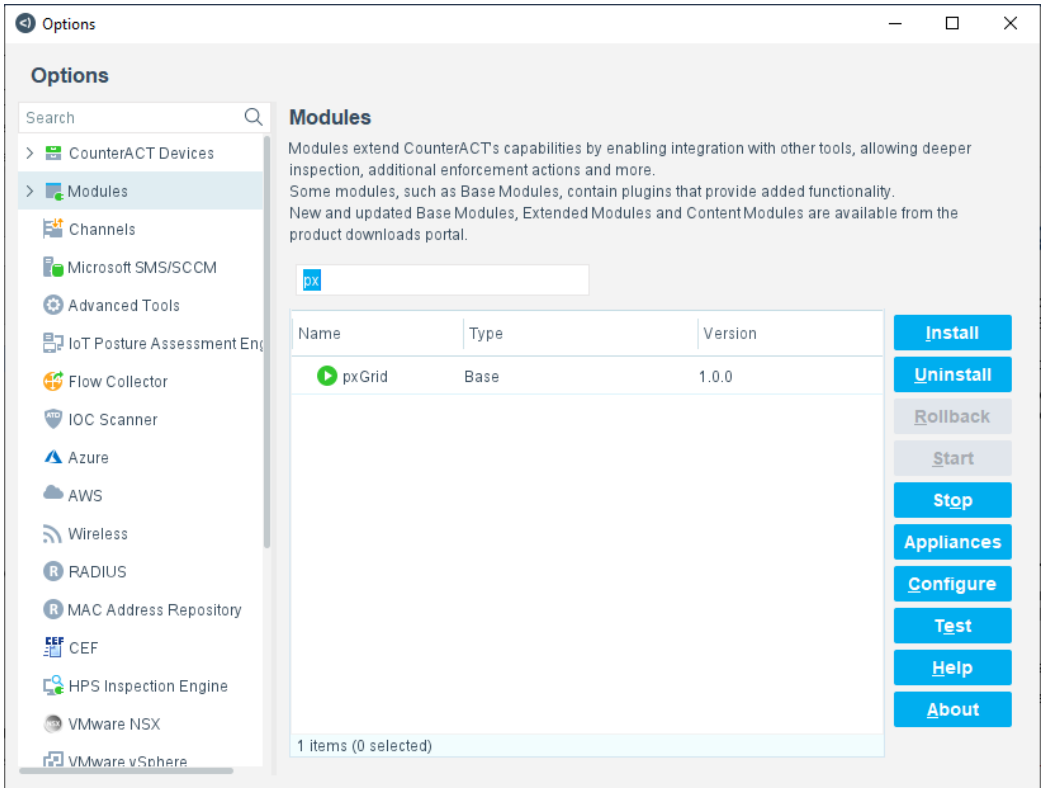
1. In the Console, select **Tools** > **Options** > **pxGrid**.



2. In the Connecting CounterACT Device field, select the CounterACT Appliance that will handle all communication between the plugin and the Cisco ISE FQDN defined in this window.

   Ensure that the selected CounterACT Connecting Device is not used in a failover cluster.

3. Enter the FQDN of the Cisco ISE on which you generated the certificates.
4. In the Client Prefix field, enter a value to be used as the deployment node name. The Forescout device ID is automatically appended to this value in ISE.
5. Deleting an endpoint from the Forescout platform on which the **Apply ISE ANC Policy** action is applied triggers an admission process in the Forescout platform. To prevent this automatic re-admission, clear the **Admit all hosts reported by Cisco ISE** checkbox.
6. Select **Apply** to save the configuration.
7. In the Options pane, select **Modules**.

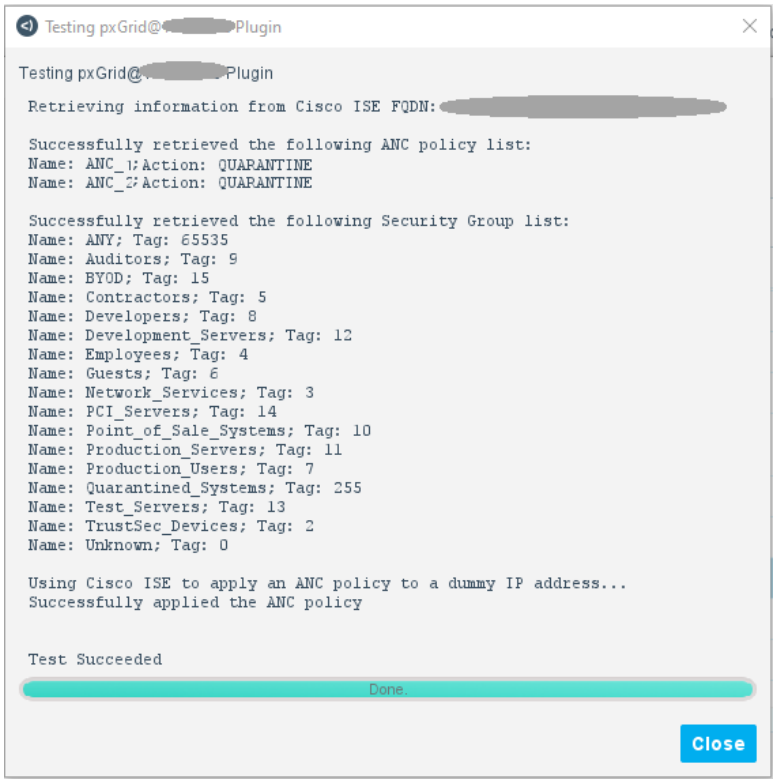


8. In the Modules pane, select **pxGrid**, and select **Start** to start the plugin.

Test the pxGrid Plugin

Ensure that the plugin can successfully communicate with the ISE FQDN.

1. In the Modules pane, select **pxGrid**, and select **Test**.



If the test is run from an Appliance that is not the Connecting CounterACT Device, a message identifies the Connecting CounterACT Device.

2. If the test is not successful, use the information shown in the window to identify and correct the error, and then save and test the configuration again.

   *If the plugin test results repeatedly indicate a system certificate error (*Unauthorized Error 401*), see System Certificate Error.*

3. If your ISE installation is not configured to automatically approve all certificate-based accounts, see Determine the User Account Approval Method.

Policies, Actions, and Properties

Forescout platform policies are powerful tools used for automated endpoint access control and management.

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

- Conditions based on host property values. The Forescout platform detects endpoints 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 endpoints that match the conditions of the rule.

For information about using properties and actions in policies, refer to the Forescout Administration Guide. *See Additional ForeScout Documentation for information about how to access the guide.*

In addition to the bundled Forescout properties and actions available for detecting and handling endpoints, you can use the Properties Provided by the Plugin to create custom policies that:

- Detect if an ISE session is active on an endpoint.
- Detect if an ANC policy has been applied to an endpoint.
- Detect which Security Group name and tag is applied to an endpoint.

In addition, you can create one custom policy having one or more sub-rules that initiate the Action Provided by the Plugin on endpoints.

To create a custom policy:

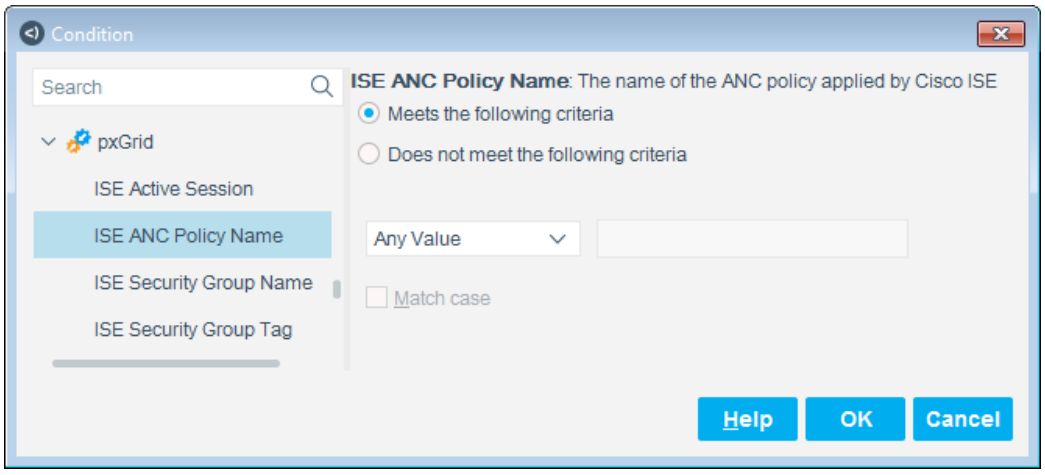
1. In the Console, select **Policy**. The Policy Manager opens.
2. Select **Add** to create a policy or select **Help** for more information about working with policies.
3. In the Policy Type window, select **Custom**, and then select **Next**.
4. Follow the wizard to create a new policy using properties and actions.

Properties Provided by the Plugin

Several properties are installed with the plugin. The Forescout platform populates and evaluates these properties based on information provided by Cisco ISE. Endpoints are not directly queried. Refer to Cisco ISE documentation for details about these data fields.

To access pxGrid Plugin properties:

1. From the Policy Wizard Main Rule or Sub-Rules panes, select **Add** in the Condition section.
2. Expand the pxGrid folder in the Properties tree.



3. Select a condition. The following pxGrid Plugin properties are available:

ISE Active Session	Indicates if the endpoint currently has an active session in ISE.
ISE ANC Policy Name	The name of the ANC policy applied to this endpoint by Cisco ISE.
ISE Security Group Name	The name of the security group applied to this endpoint by Cisco ISE.
ISE Security Group Tag	The numeric security tag applied to this endpoint by Cisco ISE.

You can use your policy to clear the applied ANC policy whenever the endpoint goes offline. For more information, see Clear the Applied ISE ANC Policy.

4. Enter the values for the condition, and select **OK**.

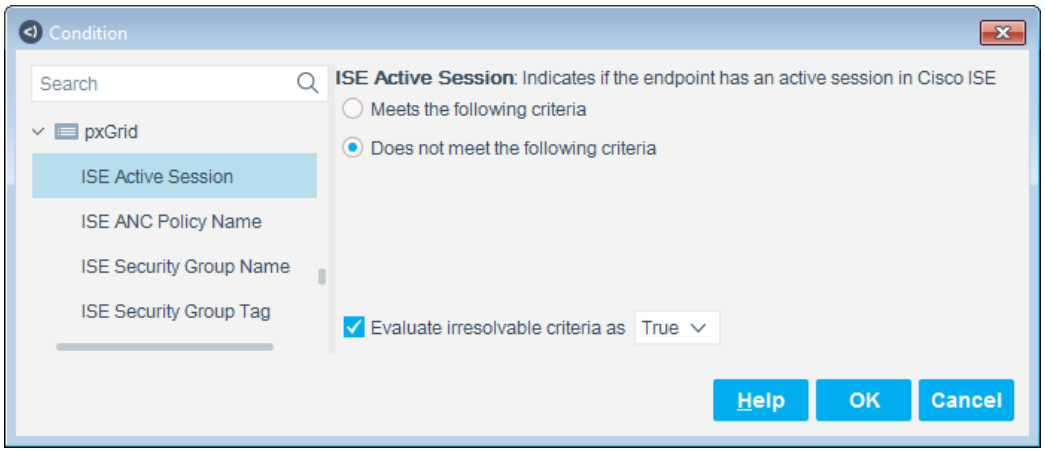
Clear the Applied ISE ANC Policy

The plugin can communicate to Cisco ISE that the selected ANC policy must be cleared from the endpoint whenever the endpoint goes offline.

It might take a few minutes for an endpoint to be reported as disconnected and for an ISE session to reported as ended.

To clear the applied ISE ANC Policy from offline endpoints:

1. In the Forescout Console Policy view, do one of the following:
   - Select **Add** to create a new policy, and follow the policy wizard to add a sub-rule.
   - Select the existing policy that applies a pxGrid action, and select **Edit**.
2. From the Condition section of a new policy sub-rule, select **Add**.
3. Expand the pxGrid folder in the Condition tree and select **ISE Active Session**.



4. Select **Does not meet the following criteria**.
5. Select **Evaluate irresolvable criteria as**, and select **True**.
6. Select **OK**.
7. Do not add a *pxGrid* action for this sub-rule.

   Ensure that this is the first sub-rule if the policy contains other sub-rules that run the Action Provided by the Plugin.

Action Provided by the Plugin

The plugin provides the following action:

- Apply ISE ANC Policy

Apply ISE ANC Policy

The Apply ISE ANC Policy action communicates to Cisco ISE that the selected ANC policy must be applied to the endpoint.

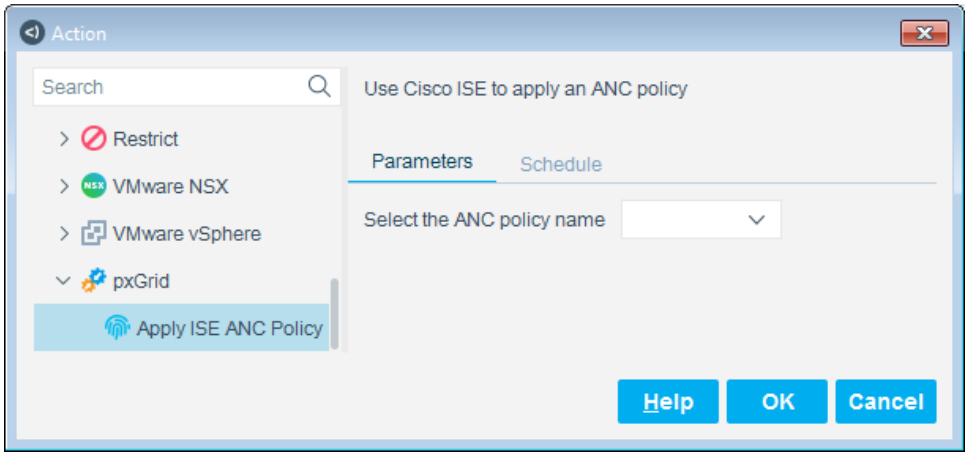
Use the Apply ISE ANC Policy action in only one policy. Each sub-rule of the policy can apply a different ANC policy.

Select a single ANC policy from the list in the dropdown box.

If the ANC policy list is empty, create an ANC policy in ISE. See Create Policies in ISE.

To run the action in a policy:

1. From the Actions section of a policy rule, select **Add**.
2. Expand the pxGrid folder in the Action tree and select **Apply ISE ANC Policy**.

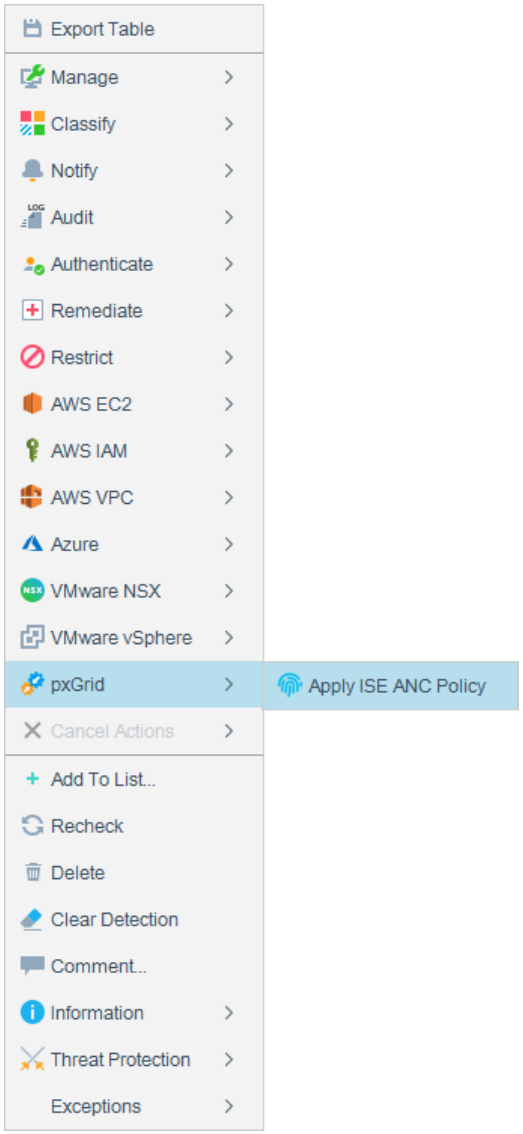


3. From the dropdown menu, select the ANC policy to apply to this endpoint.
4. Select **OK**.

The action is cancelled when the endpoint no longer matches the policy rule.

To run the action manually:

1. From the All Hosts pane, right-click one or more endpoints and select **pxGrid** > **Apply ISE ANC Policy**.



2. From the dropdown menu, select the ANC policy to apply to this endpoint.
3. Select **OK**.

To manually cancel the action, right-click one or more endpoints, and select **Cancel Actions** > **Remove ISE ANC Policy**, and select **Yes**.

Considerations and Troubleshooting

Use the information in this section to resolve common issues.

- System Certificate Error
- pxGrid Subscriptions Are Off
- One ISE per Deployment
- Failover Cluster
- Action Issues
- Host Issues

System Certificate Error

If the test results of the plugin installation repeatedly indicate a system certificate error (*Unauthorized Error 401*), replace the certificate.

To replace the system certificate:

1. Follow the instructions in the Generate Certificates section, step 6, to create another system certificate.

   Be sure to use the Cisco ISE whose FQDN you entered in step 2 of Configure the pxGrid Plugin.

2. In the Cisco ISE Admin portal, go to Administration > pxGrid Services, and select the All Clients tab.
3. In the Client Name column, select both pxGrid Accounts for the current Appliance.

   You can see the user account names in the Administration > pxGrid Services > All Clients tab.

4. Select **Deleted Selected**, and select **Yes**.

   Be sure to delete the certificate for the two Forescout Appliance user accounts before continuing.

5. In the Console, select **Tools** > **Options** > **pxGrid**, and stop the plugin.
6. Go to Options > Certificates > System Certificates.
7. Select the Cisco ISE certificate you added in the Install the pxGrid System Certificate section, and select **Remove**.
8. Install the pxGrid System Certificate.
9. Restart the pxGrid Plugin for the changes to apply.
10. In the Console, select **Tools** > **Options** > **pxGrid**, and start the plugin.
11. Select **Test** to ensure that the plugin can successfully communicate with the ISE FQDN.

If the System Certificate Error Recurs

The pxGrid Plugin uses the ISE certificates to create two user accounts in ISE for each Forescout Appliance. Even after the system certificate is replaced and the new accounts are created in ISE, ISE might continue to use the accounts of the certificate that was in error. The problem should resolve itself when the inactive pxGrid accounts are automatically purged from ISE after 15 minutes. You can manually delete the accounts sooner.

To delete the old accounts:

1. In the Cisco ISE Admin portal, go to Administration > pxGrid Services, and select the All Clients tab.
2. In the Client Name column, delete both pxGrid Accounts for the current Appliance.
3. Restart the pxGrid Plugin so that new pxGrid accounts are created.

pxGrid Subscriptions Are Off

If Forescout actions remain in Pending state and eventually time out, ensure that the Connecting CounterACT Device's relevant subscriptions are on.

To ensure that the subscriptions are on:

1. In the Cisco ISE Admin portal, go to Administration > pxGrid Services, and select the Web Clients tab.
2. Use the Client Name or IP Address search fields to search for the Connecting CounterACT Device.
3. Ensure that the subscription status is ON for the following three topics:
   - /topic/com.cisco.ise.session
   - /topic/com.cisco.ise.config.anc.status
   - /topic/com.cisco.ise.config.trustsec.security.group
4. If they are not on, manually restart the pxGrid Plugin.

One ISE per Deployment

The plugin can communicate with only one ISE installation.

Each ISE installation can communicate with only one Forescout deployment.

Failover Cluster

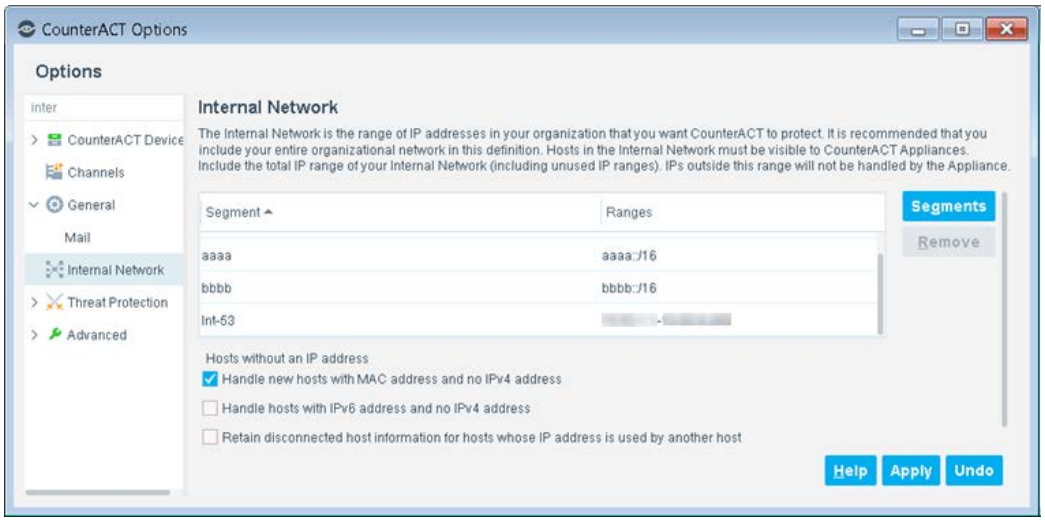
Ensure that the selected CounterACT Connecting Device is not used in a failover cluster.

Action Issues

- Create no more than one policy that applies the **Apply ISE ANC Policy** action. Each sub-rule of the policy can apply a different ANC policy.
- If the **Apply ISE ANC Policy** actions immediately fails on all hosts, ensure that the pxGrid account is activated in ISE. See Determine the User Account Approval Method.
- The **Apply ISE ANC Policy** action fails with *Session lookup failure* on endpoints that did not authenticate to ISE and do not have an active ISE session.
- If the **Apply ISE ANC Policy** action was successful but the Security Group was not applied, ensure that the Security Group is defined correctly in the ISE policy set. See Create Policies in ISE.

Host Issues

- An endpoint is only supported if it meets at least one of the following conditions:
  - It has an IPv4 address.
  - It has a MAC address without an IPv4 address, and the **Handle new hosts with MAC address and no IPv4 address** option is enabled in the Internal Network configuration.



- Overlapping IP addresses, which occur when IP addresses repeat across your network, are not supported.
- Use the Cisco ISE live sessions page to ensure that the following are applied correctly to the host:
  - ANC Policy
  - Security Group

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 Technical Documentation Page, and one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:

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

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 Support Portal

The Downloads page on the Forescout Customer Support Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, 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.

To access documentation on the Customer Support Portal:

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

Documentation Portal

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

To access the Documentation Portal:

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

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

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

Plugin Help Files

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

Documentation Portal

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