



Fore Scout

Windows Applications

Configuration Guide

Version 20.0.9



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

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

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

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

Legal Notice

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

2020-09-13 19:16

Table of Contents

| | |
|--|-----------|
| About Windows Applications | 4 |
| Requirements | 4 |
| Endpoint Applications Detected by the Module | 5 |
| Installation | 5 |
| Ensure That the Windows Applications Plugin Is Running | 6 |
| Configuration | 6 |
| Working with Endpoint Information | 6 |
| Detect Windows Versions | 7 |
| Detect Third-Party Applications | 8 |
| Manage Third-Party Applications | 10 |
| Kill Cloud Storage on Windows | 10 |
| Kill Instant Messaging on Windows | 11 |
| Kill Peer-to-Peer on Windows | 11 |
| Start Antivirus on Windows..... | 12 |
| Update Antivirus on Windows..... | 13 |
| Additional Forescout Documentation | 13 |
| Documentation Downloads | 13 |
| Documentation Portal | 14 |
| Forescout Help Tools..... | 14 |

About Windows Applications

Windows Applications is a Content Module that works with the HPS Inspection Engine to support in-depth discovery and management of the following software and applications on Windows endpoints:

- Windows operating system information, including:
 - Release
 - Package/flavor
 - Service Pack
- The following third-party applications, which present unique security challenges:
 - Antivirus
 - Peer-to-peer
 - Anti-spyware
 - Personal Firewall
 - Instant Messaging
 - Hard Drive Encryption
 - Cloud Storage
 - Microsoft products and other applications on Windows endpoints

The Windows Applications Module provides host properties and actions that let you detect and manage endpoints based on this information. Use the Forescout policies to discover endpoints running specific applications, and to apply remediation actions.

For example:

- Identify endpoints running specific Windows operating systems, and apply patches or vulnerability updates.
- Identify endpoints running specific peer-to-peer applications, and kill the application.
- Update a specific antivirus package, and start it on an endpoint.

Requirements

The module requires the following:

- CounterACT® 8.0, Forescout 8.1, 8.2.0, 8.2.1.
- Endpoint Module version 1.0 or above, with the HPS Inspection Engine running.
- It is recommended to install the latest version of the Device Profile Library Content Module together with Windows Applications.
- 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.

Endpoint Applications Detected by the Module

For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

Refer to the *Windows Applications Release Notes* for information regarding changes, updates, and recommendations for working with this release.


Installation


To install the module:

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

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

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

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

 *In modules that contain more than one component, the installation proceeds automatically one component at a time.*

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

 *Some components are not automatically started following installation.*




Ensure That the Windows Applications Plugin Is Running

After installing the Windows Applications Plugin (and configuring it, if necessary), ensure that it is running.

To verify:

1. Select **Tools** > **Options** > **Modules**.
2. In the *Modules* pane, hover over the Windows Applications Plugin name to view a tooltip indicating if it is running on Forescout devices in your deployment.

The name is preceded by one of the following icons:

-  - The Windows Applications Plugin is stopped on all Forescout devices.
 -  - The Windows Applications Plugin is stopped on some Forescout devices.
 -  - The Windows Applications Plugin is running on all Forescout devices.
3. If the Windows Applications Plugin is not running, select **Start**, and then select the relevant Forescout devices.
 4. Select **OK**.

Configuration

No configuration is required.

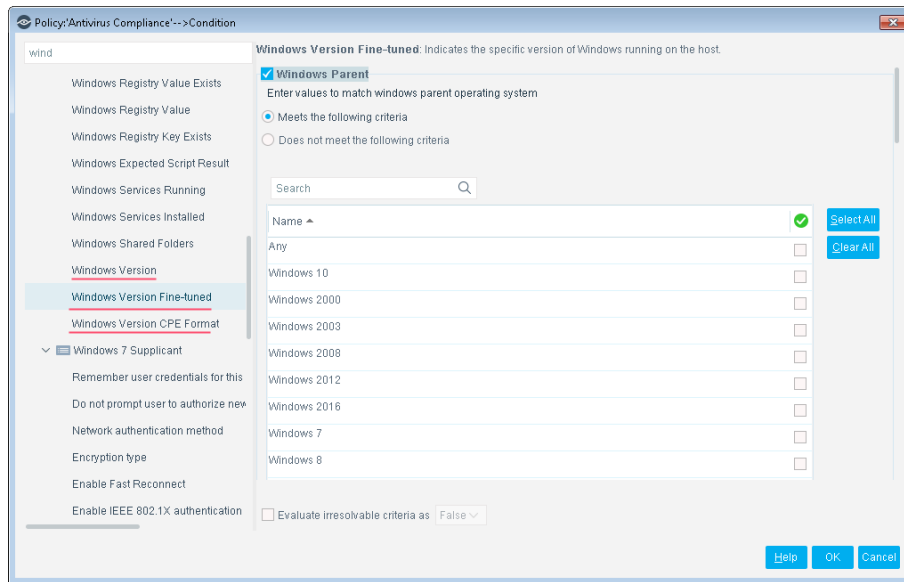
Working with Endpoint Information

The module provides host properties and actions to support the following policy-based detections and management actions:

- [Detect Windows Versions](#)
- [Detect Third-Party Applications](#)
- [Manage Third-Party Applications](#)

Detect Windows Versions

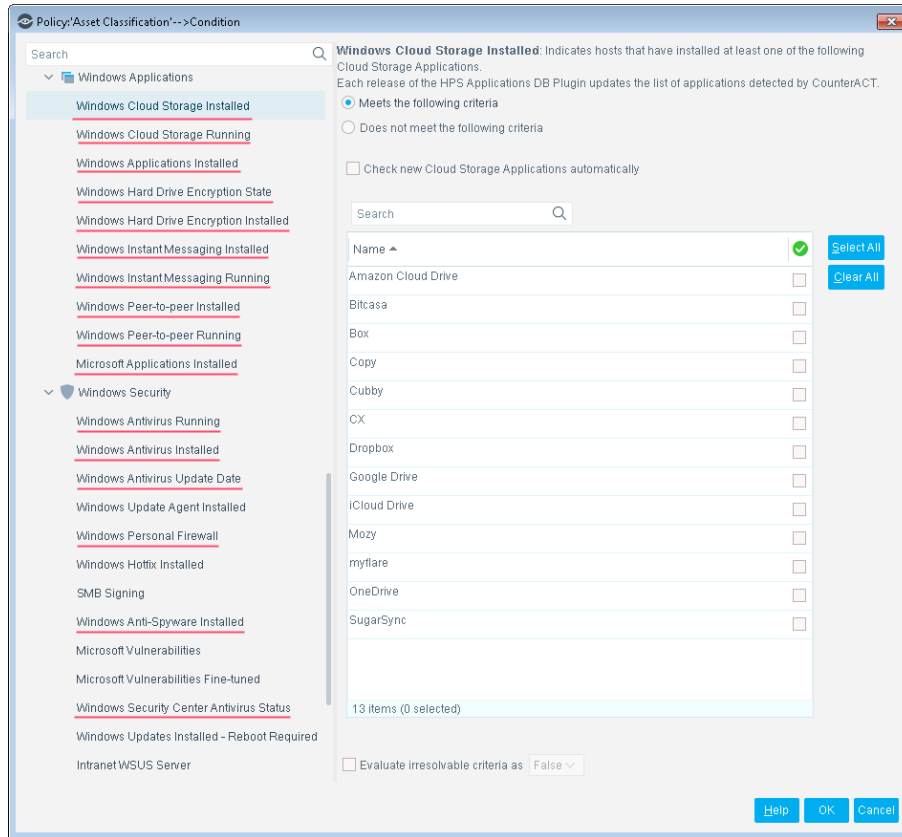
The module provides the following host properties to detect Windows applications.



| | |
|-----------------------------------|---|
| Windows Version | Identifies Windows versions detected on the endpoint. |
| Windows Version CPE Format | Identifies Windows versions running on an endpoint, in Common Platform Enumeration format. The property returns the full CPE 2.3 name string for each Windows version, as follows: cpe:2.3:o:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_edition>:<target_sw>:<target_hw>:<other> Use Forescout text matching tools to create policy conditions that identify logical parts or substrings of the CPE name string. |
| Windows Version Fine-tuned | Identifies Windows versions detected on the endpoint, based on detailed criteria such as Windows version, flavor, and service packs. |

Detect Third-Party Applications

The module provides the following host properties to detect third-party applications.



These host properties list the third-party applications that Forescout eyeSight detects. Each release of this module updates the applications that are listed, while eyeSight detects new applications.

The **Check new...** and **Detect new...** checkboxes determine whether new applications supported by subsequent updates are added to the condition you define.

- By default the checkbox is cleared, and the condition remains as you defined it. New applications are not included in the condition criteria.
- Select the checkbox to include new applications in the condition criteria.

| | |
|---------------------------------------|---|
| Windows Anti-Spyware Installed | Identifies the anti-spyware applications(s) installed on the Windows endpoint. |
| Windows Antivirus Installed | Identifies the antivirus applications(s) installed on the Windows endpoint, as detected by Forescout eyeSight. |
| Windows Antivirus Running | Identifies the antivirus application(s) running on the Windows endpoint, as detected by Forescout eyeSight. |
| Windows Antivirus Update Date | Identifies the most recent date and time that antivirus application(s) were updated on the Windows endpoint, as detected by Forescout eyeSight. |

| | |
|--|---|
| Windows Cloud Storage Application Installed | Identifies the cloud storage applications(s) installed on the Windows endpoint. |
| Windows Cloud Storage Application Running | Identifies the cloud storage application(s) running on the Windows endpoint. |
| Windows Hard Drive Encryption Installed | Identifies whether supported encryption applications are installed on the Windows endpoint. |
| Windows Hard Drive Encryption State | Identifies whether one or more drives/partitions on the Windows endpoint have been encrypted using supported encryption applications. |
| Windows Instant Messaging Installed | Identifies the instant messaging applications(s) installed on the Windows endpoint. |
| Windows Instant Messaging Running | Identifies the instant messaging application(s) running on the Windows endpoint. |
| Microsoft Applications Installed | Identifies the Microsoft application(s) installed on the Windows endpoint. |
| Windows Peer-to-peer Installed | Identifies the peer-to-peer applications(s) installed on the Windows endpoint. |
| Windows Peer-to-peer Running | Identifies the peer-to-peer application(s) running on the Windows endpoint. |
| Windows Personal Firewall | Identifies the personal firewall applications(s) installed on the Windows endpoint. |
| Windows Security Center Antivirus Status | Identifies the presence and status of antivirus applications installed on the Windows endpoint, as reported by the Windows Security Center. |

To create policy conditions based on these properties, choose from the list of supported third-party applications. Forescout has analyzed the structure, footprint, and related processes of these applications, so the module detects them more accurately and inspects them more deeply. New releases of the module typically add supported applications, or enhance support for known applications.

When you use these properties in policies rules, remember that these properties do not detect or inspect unsupported applications. For example:

- The **Windows Instant Messaging Installed** property detects supported messaging applications installed on endpoints. It does not detect other messaging applications that may be present on the Windows endpoint. When no *supported* applications are detected on the endpoint, the property resolves to the value *None* - but unsupported messaging applications may be present.
- Similarly, the **Windows Hard Drive Encryption State** property detects drives/partitions encrypted by supported applications. When no drives are encrypted by *supported* applications, the property resolves to the value *Not Encrypted* for each partition on the endpoint - but partitions may be encrypted by unsupported applications.

Use other host properties to create conditions that inspect endpoints and detect files or processes of unsupported applications.

Manage Third-Party Applications

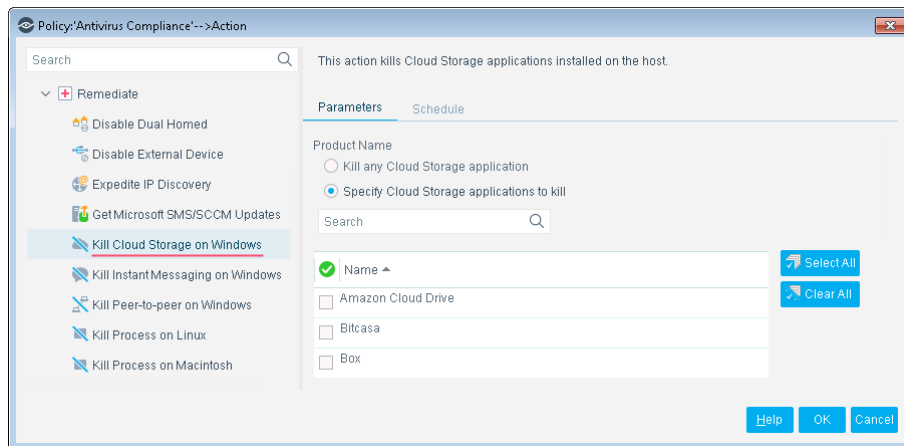
The module provides the following actions to remediate/manage third-party applications:

- [Kill Cloud Storage on Windows](#)
- [Kill Instant Messaging on Windows](#)
- [Kill Peer-to-Peer on Windows](#)
- [Start Antivirus on Windows](#)
- [Update Antivirus on Windows](#)

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.

Kill Cloud Storage on Windows

This action halts the specified cloud storage applications that are running on Windows endpoints.



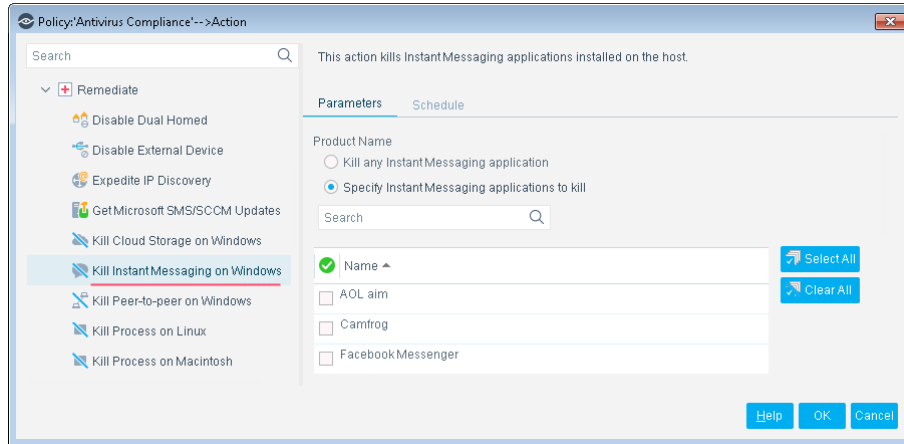
By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second.

To increase kill frequency, Forescout eyeSight can automatically install SecureConnector on endpoints when this action is applied to them. When you configure the HPS Inspection engine, select the **Automatically run SecureConnector on Windows endpoints to increase frequency of Kill Process, Kill IM and P2P actions** checkbox. See the *HPS Inspection Engine Configuration Guide* for details about SecureConnector configuration.

- 📄 *On endpoints managed using domain credentials, Forescout eyeControl runs an endpoint script to apply this action. See the HPS Inspection Engine Configuration Guide for details about scripts.*

Kill Instant Messaging on Windows

This action halts specific instant messaging applications that are running on Windows endpoints.



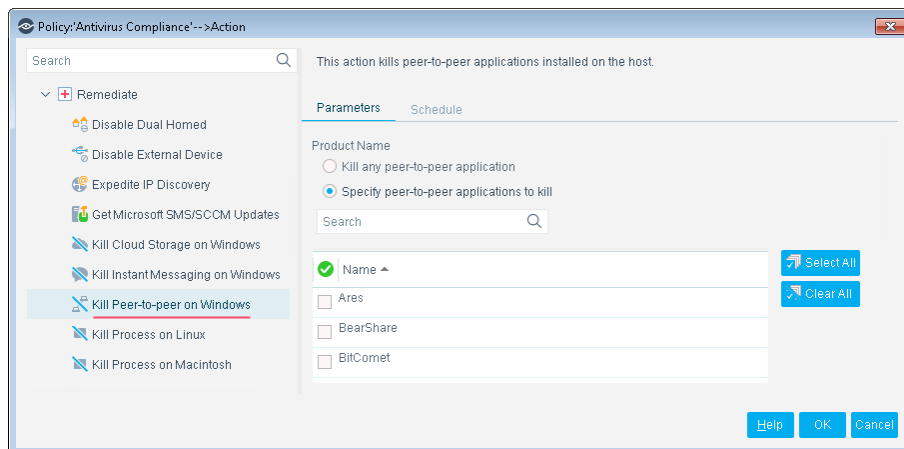
By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second.

To increase kill frequency, Forescout eyeSight can automatically install SecureConnector on endpoints when this action is applied to them. When you configure the HPS Inspection engine, select the **Automatically run SecureConnector on Windows endpoints to increase frequency of Kill Process, Kill IM and P2P actions** checkbox. See the *HPS Inspection Engine Configuration Guide* for details about SecureConnector configuration.

- On endpoints managed using domain credentials, Forescout eyeControl runs an endpoint script to apply this action. See the *HPS Inspection Engine Configuration Guide* for details about scripts.

Kill Peer-to-Peer on Windows

This action halts specific peer-to-peer applications installed at Windows endpoints.



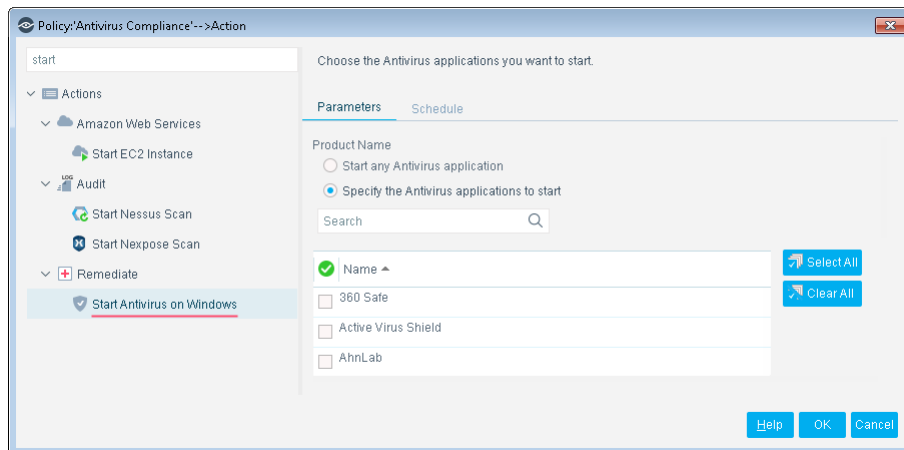
By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second.

To increase kill frequency, Forescout eyeSight can automatically install SecureConnector on endpoints when this action is applied to them. When you configure the HPS Inspection engine, select the **Automatically run SecureConnector on Windows endpoints to increase frequency of Kill Process, Kill IM and P2P actions** checkbox. See the *HPS Inspection Engine Configuration Guide* for details about SecureConnector configuration.

- On endpoints managed using domain credentials, Forescout eyeControl runs an endpoint script to apply this action. See the *HPS Inspection Engine Configuration Guide* for details about scripts.

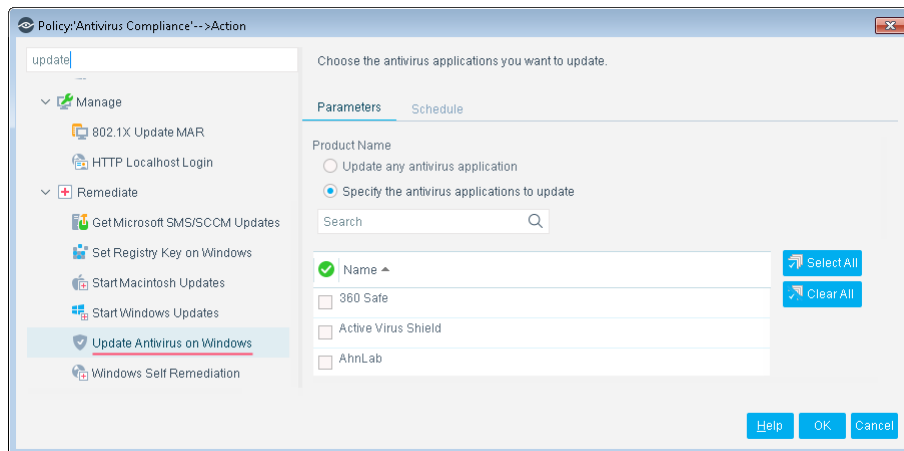
Start Antivirus on Windows

Launch antivirus applications that have been halted at Windows endpoints.



Update Antivirus on Windows

Update outdated antivirus applications at Windows endpoints.



You might need to select more than one application if you think several antivirus applications are installed on endpoints in the policy scope. If more than one antivirus application is installed on an endpoint, Forescout eyeControl updates only the first of the selected applications that it detects.

- 📄 *On endpoints managed using domain credentials, eyeControl runs an endpoint script to apply this action. See the HPS Inspection Engine Configuration Guide for details about scripts.*

Additional Forescout Documentation

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

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

Documentation Downloads

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

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

📄 *Software downloads are also available from these portals.*

To identify your licensing mode:

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

Technical Documentation Page

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

To access the Technical Documentation page:

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

Product Updates Portal

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

To access the Product Updates Portal:

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

Customer Support Portal

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

To access documentation on the Customer Support Portal:

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

Documentation Portal

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

To access the Documentation Portal:

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

Forescout Help Tools

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

Console Help Buttons

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

Forescout Administration Guide

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

Plugin Help Files

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

Content Module, eyeSegment Module, and eyeExtend Module Help Files

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

Documentation Portal

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