



# ForeScout

## SecureConnector™ Advanced Features

How-to Guide

**ForeScout version 8.1**



## 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 Resources page on the Forescout website for additional technical documentation: <https://www.forescout.com/company/resources/>
- Have feedback or questions? Write to us at [documentation@forescout.com](mailto:documentation@forescout.com)

## Legal Notice

© 2019 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.

2019-03-19 13:51

# Table of Contents

|   |           |
|---|-----------|
| <b>About this How-to Guide .....</b>                                | <b>4</b>  |
| <b>Certificate-Based Rapid Authentication of Endpoints .....</b>    | <b>4</b>  |
| Requirements for Rapid Authentication .....                         | 4         |
| What to Do.....   | 5         |
| Rapid Authentication Certificate Components .....                   | 5         |
| Install Certificate Components .....                                | 6         |
| Use an Extended Key Usage Object ID .....                           | 6         |
| Install Rapid Authentication Client Certificates on Endpoints ..... | 7         |
| Install Rapid Authentication Certificates on Windows Endpoints..... | 7         |
| Install Rapid Authentication Certificates on Linux Endpoints.....   | 8         |
| Install Rapid Authentication Certificates on OS X Endpoints .....   | 8         |
| Detect and Authenticate Endpoints .....                             | 9         |
| Host Properties for Certificate-Based Authentication .....          | 10        |
| Tune CounterACT Devices for Rapid Authentication.....               | 10        |
| <b>Endpoint Roaming .....</b>                                       | <b>11</b> |
| Requirements .....  | 12        |
| Roaming for Windows Endpoints with SecureConnector.....             | 12        |
| Roaming for Linux Endpoints with SecureConnector.....               | 12        |
| Roaming for OS X Endpoints with SecureConnector .....               | 13        |
| <b>Additional Forescout Documentation.....</b>                      | <b>14</b> |
| Documentation Downloads .....                                       | 14        |
| Documentation Portal .....  | 15        |
| Forescout Help Tools.....   | 15        |

## About this How-to Guide

This guide describes the following advanced SecureConnector™ features:

- [Certificate-Based Rapid Authentication of Endpoints](#)
- [Endpoint Roaming](#)

## Certificate-Based Rapid Authentication of Endpoints

Typically Forescout endpoint detection capabilities are combined with endpoint authentication and compliance policies to enforce network access control: Upon connection, network access of endpoints is restricted (typically to the DHCP and DNS servers and to the Forescout platform for detection and remediation interactions) until the user/endpoint is authenticated and compliance is proven. Only then is the necessary network access granted. However, authenticating endpoints and verifying compliance can cause a delay during which even legitimate endpoints have only restricted access. If complex compliance policies are in place, this delay in network access may be noticeable, resulting in an unsatisfactory user experience for corporate users.

***Certificate-based rapid authentication*** provides a strong, secure and extremely fast endpoint authentication mechanism. It uses your corporate PKI (Public Key Infrastructure) to provide immediate, authenticated network access for corporate users and other known endpoints.

The following describes a typical scenario when endpoints connect to the network:

- Corporate endpoints and other trusted endpoints managed by SecureConnector immediately initiate certificate-based authentication as part of SecureConnector's TLS interaction with the Forescout platform. Endpoints are granted immediate network access based on a signed X.509 digital certificate. The Forescout platform continues the compliance checks defined in active policies, and may revoke or change endpoint access if these checks fail.
- A corporate policy may grant limited network access to endpoints without a valid rapid authentication certificate, or with an expired or revoked certificate, or endpoints not managed by SecureConnector, until normal, policy-driven compliance checks are run.

## Requirements for Rapid Authentication

This section describes requirements for working with rapid authentication.

Install the following modules:

- Endpoint Module version 1.0 or 1.1
- Network Module version 1.0 with the Switch Plugin running.

To use this feature, endpoints must be managed by SecureConnector. Versions of SecureConnector that support this feature identify rapid authentication client

certificates on endpoints, and submit them for authentication as part of SecureConnector initial connection. For best performance, SecureConnector should be installed as a service; this ensures that authentication and consequent actions to grant network access can take place before the user has logged on, minimizing the time end users must wait to access the network.

The ForeScout platform authenticates these client certificates based on certificates and CRL files generated by your PKI that are installed on each Appliance.

This feature requires your organization to have an existing Public/Private Key Infrastructure for certificate-based authentication, as described in the X.509 standard, including:

- A trusted Certificate Authority that can generate signed certificates
- Support for certificate revocation

Administrators use the PKI in your network to generate signed certificates unique to the rapid authentication feature, and to distribute and manage these certificates on corporate devices and other trusted endpoints. Authentication chain and CRL information for these certificate is also distributed to CounterACT devices to allow authentication of client certificates.

## What to Do

To implement certificate-based rapid authentication, do the following:

1. Review the [Requirements for Rapid Authentication](#) and plan deployment. You can implement different levels of network access based on certificate details. See [Detect and Authenticate Endpoints](#).
2. Work with the PKI/desktop team in your environment to generate [Rapid Authentication Certificate Components](#).
3. [Install Certificate Components](#).

If your environment uses the same Certificate Authority (CA) to generate several certificates, you may [Use an Extended Key Usage Object ID](#) to distinguish the rapid authentication certificate from other certificates.

4. [Install Rapid Authentication Client Certificates on Endpoints](#).  
SecureConnector on managed endpoints detects these certificates to allow rapid authentication.
5. Create policies that [Detect and Authenticate Endpoints](#) based on rapid authentication certificates.

## Rapid Authentication Certificate Components

This section describes certificates and revocation lists that must be generated by the PKI team in your environment. The complete certification chain for the rapid authentication certificate takes this form:

```
[Certificate_chain][certificate]
```

[Certificate\_chain] is the full certificate chain, including the root CA and any intermediate Certificate Authorities.

[**certificate**] is the signed client certificate installed on each endpoint.

In addition, a certificate revocation list [**CRL**] for this certificate chain is required. Because this list is updated at regular intervals, your PKI team should provide a URL to the most recent CRL. There are two ways to configure this:

- When you Install Certificate Components, URL information in the certificate chain is parsed and stored.
- When you configure Endpoint Module plugins, use configuration fields in the SecureConnector tab to specify CRL information.

The screenshot shows a configuration window with the following elements:

- SecureConnector client verifies CounterACT server certificate chain
- CounterACT server verifies SecureConnector client certificate chain
- Check SecureConnector client certificate revocation status:
- Additional CDPs for CRL:
- Soft-fail OCSP requests

## Install Certificate Components

In the Console, select **Tools > Options**, then select **Certificates > Trusted Certificates** from the Options tree. For details, see the *Certificate Interface Configuration Guide*.

## Use an Extended Key Usage Object ID

In some environments, the same issuing CA is used to sign certificates for different purposes. In these environments, clients have several certificates issued by the same CA and an Extended Key Usage extension is used to distinguish each certificate. Typically, an Object ID (OID) string is used as the key.

- 📖 *In Linux environments, use unique installation folders or other methods to distinguish different certificates signed by an issuing CA.*

### To use an Extended Key Usage extension with OS X endpoints:

1. Verify that the certificate chain was installed.
2. Log in to the Enterprise Manager CLI.
3. Submit the following commands to set the OID:
  - For Windows endpoints:
 

```
fstool va setproperty config.windows_client_auth_oid.value <OID>
fstool oneach fstool va setproperty
config.windows_client_auth_oid.value <OID>
```
  - For OS X endpoints:
 

```
fstool osx_pkg -c <OID> -o
```

 Omit the `-o` flag to implement OID changes only on this CounterACT device.

These commands set the Extended Key Usage Object ID to the value specified in *<OID>*. The `osx_pkg` command also adds the OID value to the SecureConnector installers used by the OS X Plugin.

Existing SecureConnector clients receive the OID value the next time they connect to the ForeScout platform. New OS X endpoints receive the OID value during SecureConnector installation.

## Install Rapid Authentication Client Certificates on Endpoints

When endpoints access the network:

- SecureConnector connects to the Forescout platform, making endpoints manageable.
- SecureConnector authenticates using rapid authentication certificates on endpoints, and the plugin reports authentication-related host property values. You can use these properties in Forescout policies to grant network access to endpoints with valid certificates.

When installed, the Forescout platform can find rapid authentication certificates on endpoints running different operating systems:

- [Install Rapid Authentication Certificates on Windows Endpoints](#)
- [Install Rapid Authentication Certificates on Linux Endpoints](#)
- [Install Rapid Authentication Certificates on OS X Endpoints](#)

Rapid authentication certificates are installed on endpoints by the team responsible for your PKI or desktop infrastructure in your environment. Any valid certificate enrollment procedure may be used to install certificates.

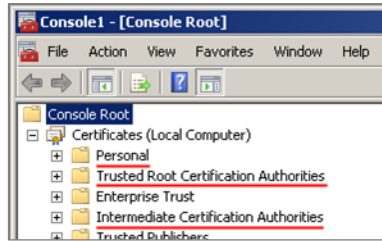
- 📖 *When you [Use an Extended Key Usage Object ID](#) to distinguish rapid authentication certificates, the object/OID value should be included in the client-side distribution. SecureConnector on endpoints searches certificate stores for the OID value that was configured during server-side certificate installation on CounterACT devices.*

## Install Rapid Authentication Certificates on Windows Endpoints

All certificates should be installed in the certificate store on the local computer.

### To install rapid authentication certificates on Windows endpoints:

- Install the rapid authentication certificate under the *Personal* certificate store.
  - The *Client Authentication* certificate purpose must be enabled.
- Install [root\_CA] – the certificate of the root Certification Authority – under the *Trusted Root Certification Authorities* store.
- Install [intermediate\_CAs] – the intermediate Certificate Authorities relevant to this feature – under the *Intermediate Certification Authorities* store.



## Install Rapid Authentication Certificates on Linux Endpoints

**To install rapid authentication certificates on Linux endpoints:**

1. For each client certificate, save the key pair as two files:
  - `fs_sc_cert.pem` contains the client certificate.
  - `fs_sc_cert_key.pem` contains the private key of the client certificate.
2. Create the following directory, and place both files in the directory:
  - When SecureConnector is run as permanent service or as dissolvable executable under the root user account:
    - `$HOME/etc/forescout/certs/`
  - When SecureConnector is run as dissolvable executable under another user account:
    - `<user_home>/forescout/certs/`

Where `<user_home>` is the home directory of the user account.

## Install Rapid Authentication Certificates on OS X Endpoints

**To install rapid authentication certificates on OS X endpoints:**

1. If necessary, convert the client certificate key pair file to `.pfx` format.
2. Copy the `.pfx` file to the endpoint.
3. Attach this `.pfx` file to the System Keychain. For example, the following command attaches a file copied to the desktop to the Keychain.

```
sudo security import ~/Desktop/<client_cert>.pfx -k
/Library/Keychains/System.keychain -f pkcs12 -A -P <pass>
```

Where `<client_cert>` is the name of the client certificate file in `.pfx` format, and `<pass>` is the passphrase used to unwrap the file.

4. Verify that SecureConnector can access this client certificate. If necessary, change key permissions.

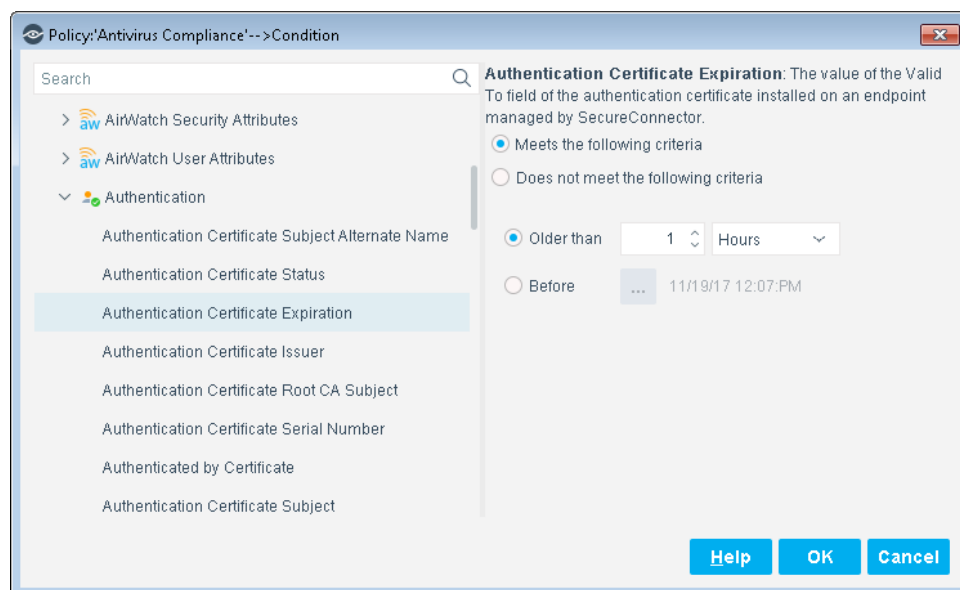


## Detect and Authenticate Endpoints

When you install plugin releases that support this feature, new host properties are available. You can use these properties to create policies that detect endpoints with valid rapid authentication certificates, and to grant them network access. Most of these properties report fields of the client certificate, and several of these properties track the certificate-based authentication process. See [Certificate-Based Authentication Host Properties](#).

Consider creating the following policies to support certificate-based rapid authentication. In some cases, you can incorporate new rules in existing policies:

- *Detect and install SecureConnector:* It may be necessary to detect corporate endpoints and other trusted devices not yet managed by SecureConnector, and install or upgrade SecureConnector.
- *Manage the rapid authentication process:* Use the **Authentication Certificate Status** and the **Authenticated by Certificate** host properties to track the rapid authentication process, and to troubleshoot endpoints that fail to authenticate.
- *Grant network access based on certificate details:* Use host properties to detect endpoints based on the subject or other fields of the certificate, and to provide a specific network access profile based on the information in the certificate on the endpoint. This enables definition of several basic levels of access, determined by the rapid authentication certificate.
- *Handle non-compliant trusted devices:* Detect certificate-authenticated endpoints that subsequently fail one or more of your environment's standard policy-based compliance checks. If endpoints are significantly non-compliant, you may want to revoke the certificates of these endpoints to prevent rapid authentication the next time they connect.
- *Troubleshoot rapid authentication certificates:* Use the host properties to detect endpoints with invalid or expired certificates.



## Host Properties for Certificate-Based Authentication

|  |   |
|--|---|
| <b>Authentication Certificate Subject Alternate Name</b> | The value of the Subject Alternate Name field of the certificate installed on the endpoint for certificate-based authentication.  |
| <b>Authentication Certificate Status</b>                 | The state of the certificate installed on the endpoint for certificate-based authentication, and any verification errors for the certificate. If a certificate for this feature is not found on the endpoint, this property returns the value <i>No certificate</i> . |
| <b>Authentication Certificate Expiration</b>             | The value of the Valid To field of the certificate installed on the endpoint for certificate-based authentication.  |
| <b>Authentication Certificate Issuer</b>                 | The value of the Issuer field of the certificate installed on the endpoint for certificate-based authentication.  |
| <b>Authentication Certificate Root CA Subject</b>        | The value of the Subject field of the certificate installed on the endpoint for certificate-based authentication.   |
| <b>Authentication Certificate Serial Number</b>          | The value of the Serial Number field of the certificate installed on the endpoint for certificate-based authentication.   |
| <b>Authenticated by Certificate</b>                      | The status of the certificate-based authentication process. If a certificate for this feature is not found on the endpoint, this property returns the value <i>No</i> .   |
| <b>Authentication Certificate Subject</b>                | The value of the Subject field of the certificate installed on the endpoint for certificate-based authentication.   |

## Tune CounterACT Devices for Rapid Authentication

This section describes information regarding tuning of internal processes to improve performance of the Certificate Based Rapid Authentication feature.

To minimize the time it takes to detect new endpoints on the network and authenticate them, and similarly, to detect their disconnection, use the following procedure to change default settings on CounterACT devices.

### To configure CounterACT devices for rapid authentication:

1. Log in to the Enterprise Manager or a standalone Appliance as root.
2. Submit the following commands:

```
fstool va set_property conf.agent_close_state_timeout.value 0
```

This internal parameter specifies the interval, in seconds, which the HPS Inspection Engine Plugin waits before reporting an endpoint as *Not Manageable* after two expected keep-alive messages are not received.

```
fstool va set_property config.kpa_rcv_interval.value 60
```

This internal parameter specifies the timeout interval, in seconds, which the HPS Inspection Engine Plugin waits for keep-alive messages from SecureConnector agents on managed endpoints.

Modifying these values precipitates reconnection if an endpoint managed by SecureConnector fails to connect to its Appliance.

3. Submit the following command to restart the HPS Inspection Engine Plugin with these new settings:

```
fstool va restart
```

4. (Enterprise Manager only) Submit the following commands to implement these configuration settings on each CounterACT device in the network:

```
fstool oneach fstool va set_property  
conf.agent_close_state_timeout.value 0
```

```
fstool oneach fstool va set_property config.kpa_rcv_interval.value  
60
```

```
fstool oneach fstool va restart
```

#### To restore default settings for these parameters:

1. Log in to the Enterprise Manager or a standalone Appliance as root.

2. Submit the following commands:

```
fstool va remove_property conf.agent_close_state_timeout.value
```

```
fstool va remove_property config.kpa_rcv_interval.value
```

3. Submit the following commands to restart the HPS Inspection Engine Plugin with these new settings:

```
fstool va restart
```

4. (Enterprise Manager only) Submit the following commands to implement these configuration settings on each CounterACT device in the network:

```
fstool oneach fstool va remove_property  
conf.agent_close_state_timeout.value
```

```
fstool oneach fstool va remove_property  
config.kpa_rcv_interval.value
```

```
fstool oneach fstool va restart
```

## Endpoint Roaming

This feature enables endpoints managed by SecureConnector to roam to various corporate Forescout deployments and still remain managed. For example, in a large organization, separate Forescout deployments may support geographically disperse segments of the corporate network. When an endpoint managed by SecureConnector in one Forescout deployment roams to a segment of the corporate network managed by another Forescout deployment, it is recognized, allowed to connect, and is managed by SecureConnector.

This section describes how to configure Forescout so that SecureConnector can work with several independent Enterprise Managers or standalone Appliances.

- 📄 *Endpoints must initially connect to their home ForeScout deployment after defining this configuration to receive the roaming capabilities.*

## Requirements

Install the following plugin releases:

- For SecureConnector on Windows: Endpoint Module version 1.0 with the HPS Inspection Engine running.
- For SecureConnector on OS X: Endpoint Module version 1.0 with the OS X Plugin running.
- For SecureConnector on Linux: Endpoint Module version 1.0 with the Linux Plugin running.

## Roaming for Windows Endpoints with SecureConnector

You can allow Windows endpoints managed by SecureConnector to roam to other Forescout deployments in your corporate network while remaining manageable.

### To support roaming for Windows:

1. On each Enterprise Manager:
  - a. Log in to the Enterprise Manager CLI.
  - b. If roaming endpoints can still connect to their home Appliance over the corporate network, submit the following command:

```
fstool va set_property config.disconnect_unassigned_sc.value true
```

From the Forescout Console, restart the HPS Inspection Engine plugin.
  - c. In the Console, select **Options** from the **Tools** menu.
  - d. Select **Modules > Endpoint Module > HPS Inspection Engine** and select **Configure**.
  - e. Select the SecureConnector tab. In the **Additional Appliance Connections** field, enter a comma-separated list of IP addresses for the other Enterprise Managers:

```
<EM_IP1>,<EM_IP2>,...,<EM_IPn>
```
  - f. If several configurations are defined for the plugin, repeat step e in all configurations.
  - g. Select **Apply** to save the changes.

## Roaming for Linux Endpoints with SecureConnector

You can allow Linux endpoints managed by SecureConnector to roam to other Forescout deployments in your corporate network while remaining manageable.

### To support roaming for Linux endpoints:

1. Prepare a file named `multiple_em_ips.conf`. Each row of the file has the following format:

```
<EM_IP>;<EM_public_key>
```

Where

<EM\_IP> is the IP address of an Enterprise Manager

<EM\_public\_key> is the public key found on the Enterprise Manager at:

```
/root/.ssh/id_rsa.pub
```

This file must contain all Enterprise Managers in all Forescout deployments.

2. Place this file at the following location on all Enterprise Managers:
 

```
/usr/local/forescout/plugin/mac/multiple_em_ips.conf
```
3. On each Enterprise Manager:
  - a. Log in to the Enterprise Manager CLI.
  - b. Submit the following commands:
 

```
fstool mac set_property config.use_multiple_em.value true
fstool oneach fstool mac set_property config.use_multiple_em.value true
fstool oneach scp
/usr/local/forescout/plugin/mac/multiple_em_ips.conf
```
  - c. If roaming endpoints can still connect to their home Appliance over the corporate network, submit the following command:
 

```
fstool mac set_property config.disconnect_unassigned_sc.value true
```
  - d. From the Console, restart all instances of the plugin.

## Roaming for OS X Endpoints with SecureConnector

You can allow OS X endpoints managed by SecureConnector to roam to other Forescout deployments in your corporate network while remaining manageable.

### To define Enterprise Manager roaming for OS X endpoints:

1. On each Enterprise Manager:
  - a. Log in to the Enterprise Manager CLI.
  - b. Submit the command `fstool osx additional_sites`.  
Output containing a certificate and other information is generated.
  - c. Select the information including the curly brackets, as indicated below. Save this information to a file.

```
{
  "resource" : "/sc",
  "client_auth_oid" : "1.3.6.1.4.1.694.21.8.815",
  "servers" :
  [
    {
      ...
      "reconnect_interval" : "2",
    }
  ]
}
```

```
        "server" : "10.34.1.14",
        "port" : 10005,
        "compliance_center_url" :
            "http://10.34.1.14/status?cc=true&fromsc=true"
    }
]
}
```

2. In each Forescout environment with its own Enterprise Manager:
  - a. Create a file named **additional\_sites**. Edit the file and paste in the Enterprise Manager data you prepared in Step 1. Do not include data for this Enterprise Manager; the file should contain only data from other Enterprise Managers. The **additional\_sites** file should have the following structure:

```
[{EM_1_info},{EM_2_info},...,{EM_n_info}]
```

    - Curly brackets enclose information from each Enterprise Manager.
    - A comma separates information from different Enterprise Managers.
    - Enclose the entire comma-separated list in square brackets.
  - b. Log in to the Enterprise Manager as root.
  - c. Save the **additional\_sites** file you prepared in Step 2 to the following location on the Enterprise Manager:

```
/usr/local/forescout/plugin/osx/
```
  - d. Submit the following command:

```
fstool oneach scp /usr/local/forescout/plugin/osx/additional_sites
```
  - e. From the Forescout Console, restart all instances of the OS X Plugin in this Forescout environment.

## 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](#), or 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 will 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.

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

**To access the Documentation Portal:**

- Go to [https://updates.forescout.com/support/files/counteract/docs\\_portal/](https://updates.forescout.com/support/files/counteract/docs_portal/) and use your customer support credentials to log in.

**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 **Forescout Help** from the **Help** menu.

***Plugin Help Files***

- After the plugin is installed, 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).