About the Network Module

The Forescout® Network Module provides network connectivity, visibility and control through the following plugin integrations:

- Centralized Network Controller Plugin
- Rogue Device Plugin
- Switch Plugin
- VPN Concentrator Plugin
- Wireless Plugin

The Network Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation of Forescout.

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

Refer to the relevant configuration guides for detailed information about how to work with and configure plugins included with this module. See Additional Forescout Documentation for information about how to access these guides, and other documentation.

Forescout Requirements

Minimum of Forescout version 8.1.

Components described in this document may have additional requirements and dependencies.

About This Release

This section describes updates and important information related to the components delivered in this version of the Network Module. This release also includes enhancements and fixes provided in previous releases.

The following table identifies the plugins that are updated in this module version:

Component	Requirements	Feature Enhancements	Fixed Issues	Known Issues	Upgrade Considerations
Centralized Network Controller Plugin 1.1.2		✓	✓	✓	
Rogue Device Plugin 1.0					
Switch Plugin 8.13.3		✓	✓	✓	✓
VPN Concentrator Plugin 4.2.2			✓		
Wireless Plugin 1.9.2			✓	✓	

Only components providing new features/enhancements are released with an updated configuration guide (help) that matches the updated version number of the component.

Centralized Network Controller Plugin 1.1.2

Forescout integrates its offering with the following Centralized Network Controller solutions:

- Cisco Application Centric Infrastructure
- Cisco Meraki Cloud-Managed Network

Cisco Application Centric Infrastructure

This section describes important information about the Centralized Network Controller Plugin version 1.1 and the plugin's integration with Cisco ACI software-defined networks. Refer to the *Forescout Network Module: Centralized Network Controller Plugin Configuration Guide* for details.

Requirements

This section describes requirements for this component.

- Network Requirements
- Third-Party Product Requirements

Network Requirements

Perform the following enterprise firewall configurations to support communication between Forescout and the Cisco ACI:

- Permit communication from the Connecting CounterACT Device(s) to the ACI Application Policy Infrastructure Controllers (APICs) on TCP/443 for the ACI fabrics that are being monitored by the Centralized Network Controller Plugin
- If a proxy server is required for use between Forescout and the ACI APICs, you must permit the proxy server to connect to the APICs on TCP/443

Third-Party Product Requirements

The following Cisco ACI products and software versions are verified for interoperation with Forescout Centralized Network Controller Plugin:

Vendor	Network Device Type	Network Device Model	Software Version
Cisco ACI	APIC	APIC-SERVER-M2 and L2	▪ 2.X ▪ 3.X

The CNC Plugin supports Cisco ACI multi-pod and does not support ACI multi-site.

When planning for a single Connecting CounterACT Device to monitor multiple Cisco ACI fabrics, you must make sure to configure each of these fabrics with a unique name.

Authentication

The CNC Plugin requires read-only permissions on an account defined in APIC. This account can be authenticated using any of the following methods:

- Username and password
- TACACS+
- Active Directory

The plugin does not support:

- Username and password authentication with token
- Certificate-based authentication.

Endpoint Requirements

The CNC Plugin supports retrieval and display of information only for endpoints connected directly or indirectly to the ACI fabric and only for endpoints having a 1:1 MAC address-IP address assignment.

The plugin does not support visibility of endpoints that are using the same MAC address for multiple IP Addresses.

Discovery behavior of endpoints having the identical IP address, whether under the same tenant or under different tenants, is not predictable. The last/recent discovered endpoint could overwrite the information/properties of the endpoint having the identical IP address, which was previously discovered.

Feature Enhancements

This section describes the new features and/or feature enhancements for this release of the Centralized Network Controller Plugin.

Added Plugin Monitoring of Juniper Mist Wireless LAN Platform Cloud-Managed Networks

The Centralized Network Controller Plugin can monitor a Juniper Mist cloud-managed network and query the Mist Cloud Management Service via its Dashboard API to retrieve and report information about the following entities:

- The enterprise organizations being served by the cloud-managed network. For example, finance, sales, system engineering.
- The Juniper Mist *sites* (networks) that belong to the cloud-managed network.
- The network devices - Mist wireless access points (***AP***) - that serve a Juniper Mist site.
- The endpoints connected to these network devices.

Actions

The plugin can apply the following new Forescout eyeControl actions on connected endpoints in support of the Juniper Mist cloud-managed network:

- *Assign Mist Label* action - assigns the selected Mist label to endpoints connected to Mist wireless access points. This action only supports the assignment of *WiFi Client* type labels at the *site* level. The action does not support the assignment of Mist labels of any other label type or label level.

- *Cancel Mist Label Assignment* action - removes the Mist label currently assigned to the connected endpoint.

Properties

The plugin resolves the following new properties in support of the Juniper Mist cloud-managed network:

- Assigned Mist Label: The Mist label currently assigned to the detected endpoint by the *Assign Mist Label* action.
- Assigned Mist Label Change: A Track Changes property identifying that a change in value occurred in the Assigned Mist Label property.

These are in addition to all the existing properties that the plugin resolves for a cloud-managed wireless network – properties about detected endpoints that are connected to the plugin-monitored, cloud-managed network, a subset of Wireless properties and various Track Changes properties.

Forescout Console Display

The Console *All Hosts* pane (in the Home tab) displays the following information about the wireless access points that the plugin discovers:

- Vendor
- WLAN AP Name
- Network Function – Lightweight AP (Access Point)
- Network ID (Site ID)
- Network Name (Site Name)
- Organization ID
- Organization Name

The Console *Asset Inventory* tab provides the following new inventory view in support of the Juniper Mist cloud-managed network:

- Assigned Mist Label: The list of endpoints to which the *Assign Mist Label* action is currently applied, due to either Forescout platform policy evaluation or manual application.

Added Plugin Monitoring of FORTINET Centrally Managed Campus Switch Network

The Centralized Network Controller Plugin can monitor the FORTINET centrally managed FortiSwitch campus switch network. The plugin interacts with FORTINET centralized management by querying any of the following devices, using their API:

- A FortiGate – manages a group of FortiSwitches; such a group is termed a virtual domain (VDOM)
- A FortiManager - manages a group of FortiGate devices; such a group is termed an administrative domain (ADOM). FortiManager is an optional device of the FORTINET centralized management solution.

Plugin retrieves information about the following network entities:

- FORTINET VDOM and ADOM
- FortiSwitches grouped in VDOM and/or in ADOM

- Endpoints connected to the managed FortiSwitches, including endpoints connected to VoIP devices that are connected to managed FortiSwitches

Properties

The plugin resolves the following new properties in support of the FortiSwitch campus switch network:

- ADOM Device ID: ID of the FortiManager ADOM managing the FortiSwitch to which the detected endpoint is connected.
- FortiGate Device ID: ID of the FortiGate managing the FortiSwitch to which the detected endpoint is connected.
- FortiManager Device ID: ID of the FortiManager managing the FortiSwitch to which the detected endpoint is connected.
- Managed FortiSwitch ID: ID of the managed FortiSwitch to which the detected endpoint is connected.
- VDOM Device ID: ID of the FortiGate VDOM managing the FortiSwitch to which the detected endpoint is connected.

In the Forescout Console, find the new properties in the FORTINET property group. These properties are in addition to all the existing properties that the plugin resolves for a centrally managed switch network – a subset of Switch properties and various Track Changes properties.

Forescout Console Display

The plugin displays information it obtains about a monitored FORTINET centrally managed FortiSwitch campus switch network in the tabs of the Console's Centralized Network Controller pane – the Controller tab, the Networks tab and the Devices tab.

The Console All Hosts pane (in the Home tab) displays the detected endpoints, which are connected to FortiSwitches, with their associated property information.

Merged Hotfixes

The following, previously released hotfixes are merged into this version Centralized Network Controller plugin:

Hotfix	Fix Content	Up to Version
1.1.1.1	Refer to Hotfix Release Notes	1.1.1.1064

Known Issues

This section describes known issues for this version of the Centralized Network Controller Plugin and the plugin's integration with Cisco ACI software-defined networks.

Issue	Vendor	Description
CN-67		The plugin does not currently support the Forescout platform's Failover Clustering functionality. However, the plugin does support the Forescout platform High Availability functionality.

Cisco Meraki Cloud-Managed Network

This section describes important information about the Centralized Network Controller Plugin version 1.1 and the plugin's integration with Cisco Meraki cloud-managed networks. Refer to the *Forescout Network Module: Centralized Network Controller Plugin Configuration Guide* for details.

Requirements

- It is recommended that the Centralized Network Controller (CNC) Plugin use received syslog events to detect endpoint connections/disconnections. For this plugin processing to take place, the following is required:
  - Core Extensions Module version 1.1 or above with the Syslog Plugin 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.

Known Issues

This section describes known issues for this version of the Centralized Network Controller Plugin version 1.1 and the plugin's integration with Cisco Meraki cloud-managed networks.

Issue	Vendor	Description
CN-15	Cisco Meraki	When the plugin only uses periodic polling of the Meraki Dashboard to retrieve information about monitored Meraki networks, there is a supply delay of +/- a couple of minutes when retrieving information about new endpoint detections. In light of this delay, ForeScout recommends enabling the option **Use Events to Expedite Detection** to expedite plugin endpoint detection via its receipt of syslog events. ***Note***: With *wired-only* cloud-managed networks, even if the **Use Events to Expedite Detection** option is enabled, the plugin might still experience the supply delay.
CN-113	Cisco Meraki	There can be instances in which the Console cannot report endpoint online/offline in real-time. This issue most typically manifests itself in the following scenario: ▪ Endpoint is displayed as online, but is actually offline.
CN-67		The plugin does not currently support the Forescout platform's Failover Clustering functionality. However, the plugin does support the Forescout platform High Availability functionality.
	Cisco Meraki	Meraki Dashboard does not report IPv6 addresses of connected endpoints to the Forescout platform (the Meraki Dashboard displays these addresses). Given this limitation, the Console only displays the MAC address of connected IPv6-only endpoints that the plugin discovers from Meraki.

Rogue Device Plugin 1.0

This plugin is not updated and retains its existing version number.

Requirements

This section describes requirements for this component.

Forescout Requirements

- 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 Module Requirements

The following plugins and their version must be running in all your CounterACT devices:

- Rogue Device Plugin, version 1.0
- Switch Plugin, version 8.13 or above

Core Extensions Module Requirements

The following plugin and version is ***optionally*** running in all your CounterACT devices:

- DHCP Classifier Plugin, version 2.2 or above
  - Resolves endpoint property information that the Rogue Device Plugin uses for the **Detect Changes in Character of Device** detection method.

Endpoint Module Requirements

The following plugin and version is ***optionally*** running in all your CounterACT devices:

- HPS Inspection Engine, version 11.0 or above
  - Resolves endpoint property information that the Rogue Device Plugin uses for the **Detect Changes in Character of Device** detection method.
  - The Rogue Device Plugin requests the HPS Inspection Engine to verify, via Nmap query, the connection status of endpoints.

Known Issues

This section describes known issues for this version of the Rogue Device Plugin.

Issue	Description
RGD-276	When all the following conditions are true, a small possibility exists that the RGD Plugin makes a false positive, MAC spoofing detection, based on changes in the character of the device: ▪ The Forescout packet engine is either not running or running, but not monitoring specific IP segment(s). ▪ The Flow Collector Plugin is running ▪ Network DHCP server(s) work with a small IP address pool that results in a high frequency of IP address re-allocations ▪ Plugin-managed Layer 3 switches are neither Juniper's nor Cisco's for which the plugin is configured to read the ARP table using CLI. ▪ The plugin's query rate of the ARP table of the managed Layer 3 switches is <= 60 seconds

Switch Plugin 8.13.3

This section describes important information about the Switch Plugin version 8.13.2

Requirements

- 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.

Feature Enhancements

This section describes the new features and/or feature enhancements for this release of the Switch Plugin.

Added Plugin Management of the Juniper MX Router

For the Juniper MX router, plugin management provides the following Forescout ***eyeSight*** and ***eyeControl*** capabilities:

- **eyeSight**
  - Connected Endpoint Detection:
    - read MAC Table
    - read/write ARP Table and read VRF ARP Table (IPv4)
    - read Neighbor Table (IPv6)
  - SNMP Trap Receipt (link up/link down)
  - Auto-Discovery
  - VoIP Detection
- **eyeControl**

  - Apply the *Assign to VLAN* action on connected endpoints
  - Apply the *Switch Block* action on connected endpoints
  - Apply the *Endpoint Address ACL* action on connected endpoints

When configuring the plugin to manage a Juniper MX router, select the new, vendor option **Juniper MX**.

For details about plugin management of this Layer 3 device and the provided Switch Plugin capabilities, refer to the *Forescout Network Module: Switch Plugin Configuration Guide*.

Track to issue SW-4506, 4507, 4508, 4509, and 4510.

Added Plugin Management of the HPE-ArubaOS-CX Switch

For HPE switches running an ArubaOS-CX operating system version, plugin management provides the following
Forescout ***eyeSight*** and ***eyeControl*** capabilities:

- **eyeSight**
  - Connected Endpoint Detection:
  - read MAC Table
  - read ARP Table and VRF ARP Table (IPv4)
  - read Neighbor Table (IPv6)
  - SNMP Trap Receipt (link up/link down)
  - Auto-Discovery
- **eyeControl**
  - Apply the *Assign to VLAN* action on connected endpoints
  - Apply the *Switch Block* action on connected endpoints

For details about plugin management of this Layer 2/Layer 3 vendor switch and the provided Switch Plugin capabilities, refer to the *Forescout Network Module: Switch Plugin Configuration Guide*.

Track to issue SW-4742

Fixed Issues

This section identifies the fixed issues for this version of the Switch Plugin.

- Merged Hotfixes

Merged Hotfixes

The following, previously released hotfixes are merged into this version of the Switch Plugin:

Hotfix	Fix Content	Up to Version
8.11.3.3	Refer to Hotfix 8.11.3.3 Release Notes	8.11.3.3163
8.12.2.2	Refer to Hotfix 8.12.2.2 Release Notes	8.12.2.2508
8.13.2.1	Refer to Hotfix 8.13.2.1 Release Notes	8.13.2.1249

Known Issues

This section describes known issues for this version of the Switch Plugin.

Issue	Vendor	Description
SW-4622	H3C	When the Switch Plugin only uses SNMP to manage an H3C S3100-16TP-PWR-EI switch running Hangzhou H3C Comware Platform Software Version 3.10, the *Assign to VLAN* action always fails with the following error message: *Cannot perform the VLAN assignment: The switch port* {port number} *properties were changed by an external source.* ***Workaround:*** To apply the *Assign to VLAN* action, configure the plugin to manage the H3C switch using both CLI and SNMP. Note: Ignore the plugin configuration test step *Assign to VLAN* failure message.
SW-3010		When the plugin is configured with the fully qualified domain name (FQDN) of the managed switch, a switch IP address change might cause plugin management of the switch, using SNMP, to fail. ***Workaround***: In the event that you experience this known issue, restart the Switch Plugin.
SW-190270304	Cisco	While the Switch Plugin is running, if the Forescout user disables the **Enable ACL** option (the option checkbox is cleared) and then saves the updated Switch Plugin configuration, the Switch Plugin does not cancel the ACL rules and port restrictions that it applied on the managed Cisco switch, as a result of ACL actions (*Access Port ACL*, *Endpoint Address ACL*). This issue has the following operational impact: ▪ Affected endpoints remain restricted, even when these endpoints no longer match policy conditions that resulted in the application of ACL actions. The plugin cannot cancel the ACL restrictions. It is ***recommended*** to first stop the Switch Plugin, prior to disabling the **Enable ACL** option (as part of stopping, the plugin removes ACL rules that it applied on managed switches). ***Workaround***: In the event that you experience this known issue, use the Clear ACLs capability to manually clear ACLs from a managed switch. For the procedure to clear ACLs, reference section *Clear ACLs from All Switch Ports* in the *Forescout Network Module: Switch Plugin Configuration Guide*.
SW-4622		The Switch plugin *Assign to VLAN* (SNMP) action fails with the following error: "Cannot perform the VLAN assignment: The switch port properties were changed by an external source" on endpoints connected to H3C S3100-16TP-PWR-EI running Hangzhou H3C Comware Platform Software, Software Version 3.10.

Upgrade Considerations

This section describes upgrade considerations for this release.

Use CLI for Brocade and Dell IPv4 Switches Being Managed

After upgrading the Switch Plugin to 8.13.3 -

- From a plugin version ***below*** 8.11.0 for managed Brocade IPv4 switches

  or

- From a plugin version ***below*** 8.12.0 for managed Dell IPv4 switches

then, during your first edit of the plugin configuration for these managed switches, the Console requires you to enable the **Use CLI** option.

Track to issues SW-1583, SW-2912

VPN Concentrator Plugin 4.2.2

This section describes important information about the VPN Concentrator Plugin version 4.2.2

Requirements

- 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.

Fixed Issues

This section identifies the fixed issues for this version of the VPN Concentrator Plugin.

- Merged Hotfixes

Merged Hotfixes

The following, previously released hotfixes are merged into this version of the VPN Concentrator Plugin:

Hotfix	Fix Content	Up to Version
4.0.9.1	Refer to Hotfix 4.0.9.1 Release Notes	4.0.9.1003
4.1.1.2	Refer to Hotfix 4.1.1.2 Release Notes	4.1.1.2007
4.2.1.1	Refer to Hotfix 4.2.1.1 Release Notes	4.2.1.1008

Wireless Plugin 1.9.2

This section describes important information about the Wireless Plugin version 1.9.2.

Requirements

This section describes requirements for this component.

Forescout Requirements

- 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.
- In order for Wireless Plugin *IP address range* to enable Forescout RADIUS-based management of wireless clients, the Authentication Module version 1.1 or above with the RADIUS Plugin running is required.

Networking Requirements

Network connectivity between the CounterACT Appliance and a WLAN device is required for plugin management of the WLAN device.

Fixed Issues

This section identifies the fixed issues for this version of the Wireless Plugin.

- Merged Hotfixes

Merged Hotfixes

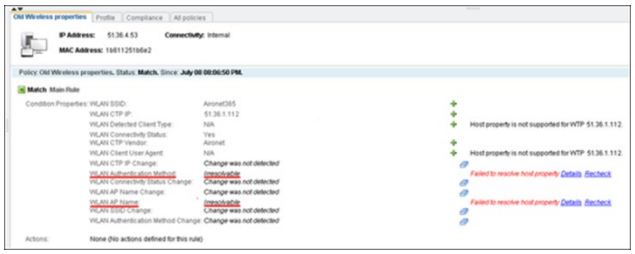
The following, previously released hotfixes are merged into this version of the Switch Plugin:

Hotfix	Fix Content	Up to Version
1.7.3.2	Refer to Hotfix 1.7.3.2 Release Notes	1.7.3.2011
1.8.2.2	Refer to Hotfix 1.8.2.2 Release Notes	1.8.2.2034
1.9.1.1	Refer to Hotfix 1.9.1.1 Release Notes	1.9.1.1003

Known Issues

This section describes known issues for this version of the Wireless Plugin.

Issue	Vendor	Description
WRL-45672417	Motorola	Whenever the Wireless Plugin is started, it queries the managed WLAN device for some basic information about the device itself, including operating system (OS), location and number of connected wireless clients. With a managed Motorola WLAN device running the WiNG 5.8 OS, the plugin query fails to retrieve the location information of the WLAN device. As a result, in the Console Wireless pane, the **Location** column entry of the managed Motorola WLAN device remains empty.

Issue	Vendor	Description
63473	Cisco Aironet	When the plugin's configured Read method for a managed Cisco Aironet access point is CLI, the plugin does not resolve the properties **WLAN AP Name** and **WLAN Authentication Method** for detected endpoints connected to the access point. The Home tab's Detections pane lists these properties as *Irresolvable*. 

Upgrading the Module

New module releases may become available between Forescout releases. This section describes how to install the module when a new release becomes available.

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.

Module and Component Rollback

The following rollback/upgrade activities are not supported:

- Rolling back this module (or one of its components) to a version released prior to Forescout 8.1.
- If you are running a version of Forescout lower than 8.1 with the corresponding version of this module installed, you cannot upgrade to this module version (or one of its components).

If you upgrade to a newer module or component version that becomes available after this release, you may be able to roll it back. When rollback is supported, the Rollback button is enabled in the Console.

Modules/components on Appliances connected to the Enterprise Manager are rolled back to the selected version. Modules/components on Appliances that are not connected to the Enterprise Manager during the rollback are rolled back when the Enterprise Manager next reconnects to the Appliances.

To roll back the module or component:

1. Select **Options** from the Console **Tools** menu.
2. Navigate to the **Modules** folder.
3. In the Modules pane, select the module or component to be rolled back.
4. Select **Rollback**. A dialog box opens listing the versions to which you can roll back.
5. Select a version and select **OK**. A dialog box opens showing you the rollback progress.

Previous Module Versions

Installing this module version also installs fixes and enhancements provided in the previous module versions listed in this section. To view Release Notes for previous module versions, see:

https://www.forescout.com/company/resources/network-module--release-notes-1-1-2/

https://www.forescout.com/company/resources/network-module-1-1-1-release-notes/

https://www.forescout.com/company/resources/network-module-1-1-release-notes/

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

Access documentation downloads 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 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/ 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 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).

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

Legal Notice

2019-11-20 11:09