

## About the Authentication Module

The ForeScout Authentication Module provides secure network access across wired, wireless, and guest networks through the following plugin integrations:

- RADIUS Plugin
- User Directory Plugin

The Authentication 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 ForeScout installation.

The User Directory and RADIUS Plugins are installed and rolled back with the Authentication Module.

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

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

This module requires a 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 Authentication Module. This release also includes enhancements and fixes provided in previous releases.

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

Component	Requirements	Feature or Security Enhancements	Fixed Issues	Known Issues	Upgrade Considerations
<a href="#">RADIUS Plugin 4.4.3</a>		✓	✓		
<a href="#">User Directory Plugin 6.4.3</a>		✓	✓		

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

## RADIUS Plugin 4.4.3

This section describes important information about the RADIUS Plugin version 4.4.3.

### Requirements

- Minimum of Network Module version 1.1 with the following components running:
  - Switch Plugin, for wired network RADIUS-based deployment
  - Wireless Plugin, for wireless network RADIUS-based deployment
- Minimum of Authentication Module version 1.1 with the User Directory Plugin running - for authentication-authorization against Microsoft Active Directory and external RADIUS.
- 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 Radius Plugin

#### Support for user log on when UserPrincipalName does not match sAMAccountName

For cases where users log on using the UserPrincipalName (UPN) account and the UPN account name is not the same as the sAMAccountName (SAM), the Forescout administrator should set **fstool dot1x set\_property config.upn.doesntmatch.samflag** to be **true**.

Setting the flag to true allows the Forescout Platform to conduct an additional query to collect the SAM information from the LDAP using the UPN. Restarting the plugin is required after the flag is enabled and before authentication.

#### Authenticating with Domains Not Directly Mapped to a Configured Authentication Source

Authenticate with a domain that may not be directly mapped to one of the configured authentication sources by defining a list of Domains or Fully Qualified Domain Names (FQDM) you wish to map back to the default RADIUS domain.

#### Arista Support

The RADIUS plugin now supports Arista switches.

### Mojo Networks Support

The RADIUS plugin now supports Mojo Networks' wireless switches.

### Fixed Issues

This section identifies the fixed issues for this release of the RADIUS Plugin.

- [Merged Hotfixes](#)
- [Fixed for This Version](#)

### Merged Hotfixes

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

Hotfix	Fix Content	Up to Version
<b>4.2.3.1</b>	Refer to <a href="#">Hotfix 4.2.3.1 Release Notes</a>	4.2.3.1009
<b>4.3.1.1</b>	Refer to <a href="#">Hotfix 4.3.1.1 Release Notes</a>	4.3.1.1022
<b>4.4.1.1</b>	Refer to <a href="#">Hotfix 4.4.1.1 Release Notes</a>	4.4.1.1013
<b>4.4.2.1</b>	Refer to <a href="#">Hotfix 4.4.2.1 Release Notes</a>	4.4.2.1021

### Fixed for This Version

No new issues were fixed for this version of the RADIUS Plugin.

### Known Issues

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

Issue	Description
<b>DOT-3795</b>	In the <i>Troubleshoot Rejected Authentications</i> policy template, the <i>Rejected by External RADIUS Server</i> sub-rule does not work.
<b>DOT-3796</b>	When an Appliance is configured as a RADIUS client for itself, the User Directory Plugin sends an unexpected access request to the RADIUS server. Workaround: Uncheck <i>Use for authentication</i> in the User Directory Plugin settings for this RADIUS server.
<b>DOT-3882</b>	If the authentication method is EAP-TLS authentication using certificates, and the LDAP-Group criterion is used in a pre-admission authorization rule in the RADIUS Plugin, authentication fails. Workarounds: <ul style="list-style-type: none"> <li>▪ Use the regular username authentication.</li> <li>▪ Check the LDAP-Group in the policy rather than in a pre-admission authorization rule.</li> </ul>

## User Directory Plugin 6.4.3

This section describes important information about the User Directory Plugin version 6.4.3.

### Requirements

This section describes requirements for this component.

#### ForeScout Requirements

- Appliance or Enterprise Manager access to the User Directory servers.
- 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.

#### Supported Guest Management Portal Browsers

The Guest Management Portal can be accessed using any of the following browsers:

- Internet Explorer 11x, Edge
- Safari 9.0 and above on MAC OS; Safari 8.3 and above on iOS
- Chrome 46 and above
- Firefox 43.0 and above
- Android Browser 1.5 and above

#### Supported Servers

The following user directory and authentication servers are supported:

- Microsoft Active Directory
- Novell eDirectory
- Oracle Directory
- IBM Lotus Notes
- OpenLDAP Server
- RADIUS
- TACACS

You can work with more than one server type simultaneously. For example, if your organization uses Microsoft Active Directory for retrieving user details and a RADIUS server for verifying authentication, you can configure the plugin to work with both these server types.

## Feature Enhancements

This section describes the new features for this release.

### Customizable Verification Codes

The *HTTP Login* action requires guests to register before the Guest Registration request is processed. A customizable 8-character alphanumeric verification code validates the email address or phone number entered by the guest in the Guest Registration form is valid.

The 8-character alphanumeric verification code can be configured to be numeric only, and the length set to a minimum of 4 characters and a maximum of 16 characters.

*To customize verification codes:*

To enable *numeric-only* verification codes, enter the following FS CLI command:

**fstool ad set\_property signin.verifyid.pass.numeric 1**

To customize the *length* of the verification codes, enter the following FS CLI command:

**fstool ad set\_property signin.verifyid.pass.len <length>**

Restart the plugin after making configuration property changes with the following FS CLI command:

**fstool ad restart**

If there is more than one appliance, set the **signin.verifyid** properties on the Enterprise Manager and then on all the appliances. Whichever device is managing hosts should have these properties set for the verification code to be customized.

See the [User Directory Plugin Server and Guest Management Configuration Guide](#) for details.

## Security Enhancements

This release of the User Directory Plugin includes updates that address security issues that are identified in, but not limited to, the following Common Vulnerabilities and Exposures (CVE):

Issue	CVE
UD-2018	CVE-2011-1498
	CVE-2014-3577
	CVE-2015-9251
	CVE-2018-1404
	CVE-2018-14040
	CVE-2019-11358

## Fixed Issues

This section identifies the fixed issues for this release of the User Directory Plugin.

- [Fixed for This Version](#)
- [Merged Hotfixes](#)

### Fixed for This Version

No new issues were fixed for this version of the User Directory Plugin.

### Merged Hotfixes

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

Hotfix	Fix Content	Up to Version
<b>6.3.1.1</b>	Refer to <a href="#">Hotfix 6.3.1.1 Release Notes</a>	6.3.1.1065
<b>6.4.2.1</b>	Refer to <a href="#">Hotfix 6.4.2.1 Release Notes</a>	6.4.2.1029
<b>6.4.0.1</b>	Refer to <a href="#">Hotfix 6.4.0.1 Release Notes</a>	6.4.0.1006
<b>6.1.4.1</b>	Refer to <a href="#">Hotfix 6.1.4.1 Release Notes</a>	6.1.4.1011

## Known Issues

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

Issue	Description
<b>UD-1222</b>	The status in the Forescout Console is not updated properly when a registered guest logs in following endpoint proxy server configuration for HTTP Login that does not include the "X-Forwarded-For" HTTP header.
<b>UD-1240</b>	Pending Self-Registration guest list is not copied properly after switch-over to a Recovery Manager.
<b>UD-1427</b>	The User Directory Plugin does not support IPv6 TACACS authentication servers.
<b>UD-1668</b>	The session ID is not changed after a user changes their password in the Guest Management Portal.
<b>UD-1760</b>	If the user is unable to log in to the Console and the error message says that the connection and authentication to the Console failed but that the certificate was valid, the certificate might actually be invalid.
<b>UD-2019</b>	Scheduled Web Report email is no longer received from CounterACT after switching over to the recovery Enterprise Manager.
<b>UD-2022</b>	The Guest Terms and Conditions text message contains multiple empty lines, causing the message to be unclear to the Guest user.
<b>UD-2023</b>	Attempting to log in with the Corporate domain user via HTTP Login policy action fails. Therefore, the Corporate/Guest Control Policy evaluates Corporate endpoints as Guest endpoints.  Although it is possible to log in with the same Corporate LDAP user to the Enterprise Manager console, and Sponsor Portal, the HTTP Login policy action fails.

## 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.x.
- 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/authentication-module-release-notes-1-1-2/>

<https://www.forescout.com/company/resources/authentication-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

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

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

 *Software downloads are also available from these portals.*

### To identify your licensing mode:

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

## ForeScout Resources Page

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

### To access the ForeScout Resources page:

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

## Product Updates Portal

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

### To access the Product Updates Portal:

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

## Customer Portal

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

### To access documentation on the ForeScout Customer Portal:

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

## Documentation Portal

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

### To access the Documentation Portal:

- Go to [https://updates.foreScout.com/support/files/counteract/docs\\_portal/](https://updates.foreScout.com/support/files/counteract/docs_portal/)

## ForeScout Help Tools

Access information directly from the Console.

### **Console Help Buttons**

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

### **ForeScout Administration Guide**

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

### **Plugin Help Files**

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

### **Online Documentation**

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

## 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](mailto: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.

2020-05-14 10:59