802.1X Plugin 4.2.3

CounterACT® Plugin Update

Release Notes

October 2018

Version Information

802.1X Plugin, version 4.2.3

Supported CounterACT® Versions

Customers who are working with the following CounterACT version can install the plugin:

- 7.0.0

Requirements

- An active Maintenance Contract for CounterACT devices.
- Hotfix 1.7.1 or above.
  - Install Service Pack 3.0.0 or above for the plugin to provide its full support of CounterACT centralized web authentication. For details, reference the section *Configure Pre-Admission Authorization* in the *CounterACT 802.1X Plugin Configuration Guide*.

  It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.
- Switch Plugin 8.5.7 or above.
- Wireless Plugin 1.3.2 or above.
  - To work with Meraki access points, Wireless Plugin 1.6.0 or above is required.
- User Directory 5.4.3 or above.

What's New

This version contains important feature enhancements and fixed issues. See Feature Enhancements and Fixed Issues.

Installing this release also installs fixes and enhancements provided in previous releases. See Previous Releases for more information. See How to Install for installation details.

Fixed Issues

The following issues have been fixed for this release.

Issue	Description
DOT-3680	COA was not triggered when attempting to apply an 802.1x action with specified attributes.

Issue	Description
DOT-3159	The plugin did not support the Protected EAP-TLS (*PEAP-EAP-TLS)* authentication protocol, and did not extract the supplicant user name (tunneled user name) used for the inner authentication phase of Protected EAP-MSCHAPv2.
DOT-3650	Support was added for the Framed IP-Address attribute sent from the Account Request when accounting is enabled to collect the current Host IP address.
DOT-3552 **DOT-3229**	Temporary files were not being cleaned up properly, and as a result, the 802.1x Plugin occasionally failed to start.
DOT-3651	Support has been added in the 802.1x Plugin for the *Accounting Stop* packet.

Working with This Release

This section describes changes in this plugin that affect the way you work with CounterACT.

SMB Version Support

With the current version, the plugin supports working with Active Directory servers using an SMB version above SMBv1.

Track to issue DOT-3171

Attribute Removed for Use in Rule Condition

With the current version, the **Guest Member** attribute is no longer an available criterion for configuration in a Pre-Admission Authorization rule condition.

Track to issue DOT-2541

Upgrade Considerations and Issues

Read the following section before you upgrade to the current plugin version. The considerations and issues described in this section are in effect after upgrading to the current version:

- Change of Default Port
- Plugin as Proxy to an External RADIUS Server
- Upgrade/Rollback Outcomes to Be Aware Of
- Pre-Admission Authorization Rule Definition

Change of Default Port

After upgrading to the current version, port 3269 (Global Catalog over TLS method) is the default port used by the CounterACT RADIUS server to query Microsoft Active Directory servers when evaluating the **LDAP-Group** criterion in a pre-admission authorization rule condition. Prior to upgrade, that default port was 389.

Plugin as Proxy to an External RADIUS Server

When upgrading from version 4.1.x to the current version and the 802.1X Plugin functioned in version 4.1.x as a proxy to an external RADIUS server, then the following upgrade configuration processing occurs:

When only a Primary Proxy server is configured (the **Authentication Sources** tab) for plugin use:

1. The plugin defines a RADIUS server entry in the User Directory Plugin using the Primary Proxy's RADIUS Server Address and RADIUS Server Secret.
2. The RADIUS server entry, defined in the User Directory Plugin, is listed as an available authentication source in the upgraded 802.1X Plugin's **Authentication Sources** tab.

When both a Primary Proxy server and a Secondary Proxy server are configured (the **Authentication Sources** tab) for plugin use:

1. The plugin defines a RADIUS server entry in the User Directory Plugin using the Primary Proxy RADIUS Server Address and RADIUS Server Secret.
2. For the defined RADIUS server entry, the plugin creates a ***replica*** RADIUS server entry in the User Directory Plugin using the Secondary Proxy's RADIUS Server Address and the Primary Proxy's RADIUS Server Secret.
3. The RADIUS server entry, defined in the User Directory Plugin, is listed as an available authentication source in the upgraded 802.1X Plugin's **Authentication Sources** tab.

Upgrade / Rollback Outcomes to Be Aware Of

This section describes several upgrade-rollback outcomes to be aware of.

Scenario 1

1. The 802.1X Plugin is running version 4.1.0.x. The plugin is defined such that the CounterACT RADIUS server operates as a proxy to an external RADIUS server.
2. Upgrade plugin to version 4.2.3. As part of this upgrade, the plugin creates a RADIUS server entry in the User Directory Plugin.

3. Rollback plugin to version 4.1.0.x.

   OUTCOME: The RADIUS server entry created by the plugin in step 2 remains defined in the User Directory Plugin. The entry can be manually deleted, if desired.

Scenario 2

1. The 802.1X Plugin is running version 4.1.0.x and is configured to use an Active Directory authentication source.
2. Upgrade plugin to version 4.2.3.
3. In the upgraded plugin, modify the Active Directory authentication source.
4. Rollback plugin to version 4.1.0.x.

   OUTCOME: In the downgraded plugin, the Active Directory authentication source that was configured in step 1 is back in effect.

Scenario 3

1. The 802.1X Plugin is running version 4.1.0.x and is configured to use an Active Directory authentication source.
2. Upgrade plugin to version 4.2.3.
3. Rollback plugin to version 4.1.0.x.
4. In the downgraded plugin, modify the Active Directory authentication source.
5. Upgrade plugin to version 4.2.3.

   OUTCOME: In the upgraded plugin, the Active Directory authentication source that was configured in step 1 is back in effect.

Track to issue 76133

Pre-Admission Authorization Rule Definition

After either an upgrade to or an initial installation of the current version, make sure that your pre-admission authorization rules are properly defined in order to impose the authorizations that you require. Reference section *Authentication-Authorization Processing Flow* in the *CounterACT 802.1X Plugin Configuration Guide*.

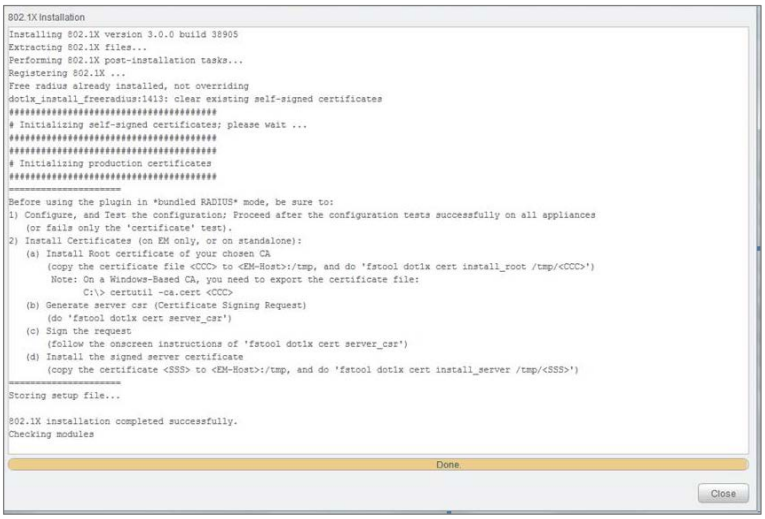
How to Install

Perform the following steps to download the plugin from the Web site and install it on the Console.

To download and install the plugin:

1. Navigate to the Customer Support, Base Plugins page and download the plugin **`.fpi`** file.

2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin **`.fpi`** file.
7. Select **Install**.
8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
9. The following dialog box opens:



10. The installation screen provides instructions for working with certificates. See the *CounterACT 802.1X Plugin Configuration Guide* for details.
11. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.
12. Select **Start**.

More Plugin Information

Refer to the plugin configuration guide for more information about the plugin.

To access the plugin configuration guide:

1. After the plugin is installed, select **Options** from the Console **Tools** menu.
2. Navigate to and select the **Plugins** folder. The Plugins pane opens.
3. Select the plugin from the Plugins pane and then select **Help**.

More Release Information

This section provides the following release information:

Rollback Support

Under certain circumstances you may want to roll back the plugin to a previously installed release. This may happen, for example, if your system does not operate as expected after the plugin upgrade.

You can roll back this plugin to a previous version. In section Upgrade Considerations and Issues, see Upgrade/Rollback Outcomes to Be Aware Of.

Plugins on Appliances connected to the Enterprise Manager are rolled back to the selected version. Plugins 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 view rollback versions and perform the roll back:

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

Currently Available Releases

You can view information about 802.1X Plugin releases supported by specific CounterACT versions. To view, click the following link:

http://updates.forescout.com/support/files/plugins/dot1x/Updates.pdf

New features or fixes may be provided after this release. These items will be made available as Beta releases to the upcoming plugin version until the final version is posted on the ForeScout Customer Support page.

In addition, you can contact the ForeScout Beta Manager at beta@forescout.com to request Beta plugin updates.

Previous Releases

Installing this release also installs fixes and enhancements provided in the releases listed in this section. To view Release Notes of previous version releases, see:

https://updates.forescout.com/support/files/plugins/dot1x/4.2.2/4.2.2-42020001/RN.pdf

http://updates.forescout.com/support/files/plugins/dot1x/4.2.0.1010/4.2.0.1010-42001010/RN.pdf

https://updates.forescout.com/support/files/plugins/dot1x/4.2.0/4.2.0-42000551/RN.pdf

http://updates.forescout.com/support/files/plugins/dot1x/4.1.0.1/4.1.0.1-410201/help.pdf

Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- Documentation Portal
- Product Updates Portal
- CounterACT Console Online Help Tools

Documentation Portal

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

To access the Documentation Portal:

1. Go to https://updates.forescout.com/support/files/counteract/docs_portal/.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

Console User Manual

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Plugins**.
2. Select the plugin and then select **Help**.

Documentation Portal

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

Legal Notice

2018-10-25 17:13