Forescout

Authentication Module: RADIUS Plugin

Configuration Guide

Version 4.4.3
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.
# Table of Contents

**Overview** ........................................................................................................... 6
  About the 802.1X Protocol ............................................................................... 6
  Endpoints with Supplicant: Processing Sequence ......................................... 7
  Endpoints without Supplicant: Processing Sequence ...................................... 7
  About the Forescout RADIUS Plugin ............................................................. 8
  IPv6 Support ................................................................................................... 9
  RADIUS Plugin Components .......................................................................... 9
    Authentication Sources ............................................................................... 9
    Pre-Admission Authorization .................................................................. 10
  RADIUS Settings ...................................................................................... 11
  MAC Address Repository ........................................................................... 12
  Supported Authentication Protocols ............................................................. 12
  What to Do ..................................................................................................... 13

**Forescout Requirements** ............................................................................. 13

**Environment Readiness** ............................................................................... 13
  Certificate Readiness .................................................................................. 14
  System Certificate ...................................................................................... 14
  Trusted Certificate ...................................................................................... 14
  Network Device Readiness ......................................................................... 14
    Cisco Switch Readiness Template ........................................................... 15
    Cisco Switch Port Readiness Template ..................................................... 19
  Endpoint Readiness .................................................................................... 23
    Wired Windows 7 Endpoint Readiness Template ......................................... 23
  User Directory Readiness .......................................................................... 27
    User Directory Plugin: General Pane ......................................................... 28
    User Directory Plugin: Settings Pane ........................................................ 28
    Using Microsoft Active Directory: Other Issues ....................................... 29
    Using an External RADIUS Server ........................................................... 30

**Configure the Plugin** .................................................................................... 30
  Configure Authentication Sources ............................................................... 31
  Work with Authentication Sources .............................................................. 33
  Determine the Authentication Source to Query .......................................... 35
  Join CounterACT Devices to Active Directory Domains ............................ 35
  Test Authentication Source Functionality .................................................. 37
  Configure Pre-Admission Authorization ....................................................... 38
    Rule Configuration .................................................................................... 40
  Configure RADIUS Settings ...................................................................... 47
  Configure the Plugin Per Appliance ............................................................. 51
  Configure MAC Access Bypass .................................................................... 52
    What You See in the Repository .............................................................. 53
    Creating MAR Entries .............................................................................. 54
    Editing and Removing MAR Entries ......................................................... 58
  Verify That the Plugin Is Running ............................................................... 58
Overview

This document provides RADIUS Plugin configuration information and system certificate information, as well as information about working with CounterACT RADIUS policy templates and other RADIUS features. Use-case scenarios describe how to set up NAS devices, endpoints, and Forescout in order to meet a variety of important 802.1X use-case goals.

This section provides an overview of the following topics:

- About the 802.1X Protocol
- About the Forescout RADIUS Plugin
- RADIUS Plugin Components

About the 802.1X Protocol

IEEE 802.1X is the industry standard for port-based network access control. It provides an authentication mechanism for endpoints attempting to connect to wired or wireless networks. The 802.1X authentication process consists of the following participating entities:

- **Client**: The user or client endpoint attempting to access an organization's network. The organization's security requirements require these endpoints to undergo authentication evaluation in the following ways:
  - Endpoints that have a *supplicant* (i.e., embedded software that handles the endpoint's side of the 802.1X authentication sequence) can be authenticated based on either of the following:
    - User credentials or certificate
    - Device credentials or certificate
  - Endpoints that do not have a *supplicant*, such as printers, are authenticated based solely on their MAC address. This is known as the MAC address bypass (MAB) method of authentication.

- **Authentication Server**: The server that executes the authentication of endpoints, typically a RADIUS server.

- **Authenticator**: The network access entity (NAS), located between the client and the authentication server, to which the client connects in its attempt to gain network access. Wireless access points and switches are examples of authenticators.
Endpoints with Supplicant: Processing Sequence

The following diagram provides a high-level view of the 802.1X processing sequence for endpoints having a supplicant:

Endpoints without Supplicant: Processing Sequence

Endpoints without a supplicant undergo MAB authentication. In such a scenario there is no supplicant response and phase 1 times out. Then, the RADIUS server evaluates the source client, based on the endpoint MAC address.

The following diagram provides a high-level view of the 802.1X processing sequence for endpoints that do not have a supplicant:
About the Forescout RADIUS Plugin

The RADIUS Plugin is a component of the Forescout Authentication Module. See Authentication Module Information for details about the module.

The RADIUS Plugin broadens the scope of standard 802.1X authentication technology to include device profiling, endpoint compliance, and access and remediation enforcement.

The plugin ensures seamless, comprehensive 802.1X pre-connect security and post-connect control for both wired and wireless devices and both corporate and guest users.

The RADIUS Plugin enables the Forescout platform to authenticate 802.1X switch/wireless connections to the network. The plugin is compatible with the IEEE 802.1X specification and the RADIUS authentication protocol.

The plugin enables the Forescout platform to provide authentication and authorization instructions to NAS devices, to integrate with user directory servers, and to employ powerful Forescout 802.1X policies to detect, authenticate, and control network endpoints and associated user activity.

The plugin supports authentication, authorization, and accounting, enabling the Forescout platform to:

- Discover and monitor each 802.1X authenticating device's MAC address, IP address, and other properties.
- Monitor the real-time network connectivity status of 802.1X authenticating devices.
Automate endpoint control based on device profile and compliance.

IPv6 Support

The RADIUS Plugin provides IPv6 support for performing endpoint authentication, authorization, and guest centralized web authentication (CWA). The plugin handles the IPv6 addresses of NAS devices (switches, WLAN devices), Microsoft domain controllers, and external RADIUS servers with which it must interface. For information about overall Forescout IPv6-related support, refer to the Forescout 8.1 Release Notes. See Additional Forescout Documentation for information on how to access this document.

RADIUS Plugin Components

The following RADIUS Plugin components require configuration in order for the plugin to effectively operate:

- Authentication Sources
- Pre-Admission Authorization
- RADIUS Settings
- MAC Address Repository

Authentication Sources

In the Console, in the Authentication Sources tab of the Tools > Options > RADIUS window, select the RADIUS servers and the user directories that handle the validation of the credentials provided during endpoint authentication. Only authentication sources configured in the User Directory Plugin can be selected.
Pre-Admission Authorization

In the Console, in the Pre-Admission Authorization tab of the **Tools > Options > RADIUS** window, define the set of prioritized rules that the CounterACT RADIUS server uses to evaluate endpoints for authorization handling, after authentication by the applicable RADIUS server (a selected **Authentication Source**). These rules are evaluated against authenticated endpoints according to their assigned priority. For endpoints matching a rule's condition, the CounterACT RADIUS server applies the defined authorization handling to the endpoint in the ACCEPT message it sends to the NAS device.
RADIUS Settings

In the Console, in the RADIUS Settings tab of the Tools > Options > RADIUS window, configure settings that are relevant when the CounterACT RADIUS server functions as the authenticating RADIUS server. Regardless of whether the CounterACT RADIUS server functions as the authenticating RADIUS server, it always handles the authorization of authenticated endpoints.
MAC Address Repository

In the Tools > Options > MAC Address Repository pane, maintain the repository of MAC addresses of endpoints that do not have a functioning 802.1X supplicant and are permitted to be authenticated by the CounterACT RADIUS server using MAC address bypass (MAB).

Optionally, for each MAC address entry in this repository, you can define an authorization to be imposed by the CounterACT RADIUS server on the MAB-authenticated endpoint.

Supported Authentication Protocols

The RADIUS Plugin supports the following authentication protocols:

<table>
<thead>
<tr>
<th>Authentication Protocol</th>
<th>Detail</th>
<th>User</th>
<th>Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEAP-MS-CHAP v2</td>
<td>For authenticating against Microsoft Active Directory, version NTLMv1</td>
<td>User Domain Credentials</td>
<td>Device Domain Credentials</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>Versions supported: TLS 1.2 and below</td>
<td>User Certificate</td>
<td>Device Certificate</td>
</tr>
<tr>
<td>PEAP-EAP-TLS</td>
<td>Versions supported: TLS 1.2 and below</td>
<td>User Certificate</td>
<td>Device Certificate</td>
</tr>
<tr>
<td>PAP</td>
<td>Basic username and password authentication</td>
<td>Username and credentials against Microsoft Active Directory</td>
<td></td>
</tr>
</tbody>
</table>

For the supported RADIUS access request delimiters, see Determine the Authentication Source to Query.
What to Do

Perform the following steps to work with this plugin:

1. Verify that you have met all system requirements. See Forescout Requirements.
2. Verify that all environmental pre-conditions are met. See Environment Readiness.
3. Configure the plugin.
4. Test the plugin. See Testing and Troubleshooting.

Forescout Requirements

The RADIUS Plugin requires the following:

- Forescout version 8.1.
- 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
- 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.

Environment Readiness

This section provides an overview of the components you need to configure before working with the RADIUS Plugin.

It is recommended to verify that all aspects of your organization's IT environment are properly configured before enforcing access control. Plugin deployment and configuration might vary depending on the use-case scenario you want to address using the RADIUS Plugin. For details, see Use Cases.

This section includes the following topics:

- Certificate Readiness
- Network Device Readiness
- Endpoint Readiness
- User Directory Readiness
Certificate Readiness

Certificate management in Forescout 8.1 is accomplished using the Console certificates interface (Options > Certificates). For more information, refer to the Configuring the Certificate Interface section in the Forescout Administration Guide.

The following types of certificate can be used with the RADIUS Plugin:

- **System Certificate**
- **Trusted Certificate**

When defining and provisioning certificates, you can:

- Define a single certificate and provision it across all your CounterACT devices.
- Define multiple certificates and provision each certificate on one or more CounterACT devices.

**System Certificate**

Plugin operation requires that a valid RADIUS server certificate be available for validation by external network endpoints. Use the certificate interface (Options > Certificates > System Certificates) to define and provision RADIUS server certificates.

When you generate the certificate signing request (CSR) for the RADIUS Plugin (the CounterACT RADIUS server), you must designate the certificate for use by all Appliances or by a specific Appliance.

With a new Forescout deployment, the RADIUS Plugin generates a self-signed RADIUS server certificate that is issued by the Forescout certificate authority (CA). This self-signed RADIUS server certificate, which is necessary for the plugin to run, is listed in the System Certificates pane of the certificate interface. Replace the self-signed certificate with a RADIUS server certificate that is signed by an external, trusted certificate authority.

**Trusted Certificate**

Use the certificate interface (Options > Certificates > Trusted Certificates) to configure the certificate authority trust chains that are used by the RADIUS Plugin to authenticate external network endpoints.

**Network Device Readiness**

Configure NAS devices:

- To perform RADIUS-based network authentication
- With the necessary RADIUS secret to allow for successful endpoint authentication processing to occur with Forescout 8.1

NAS devices (switches, WLAN devices) must be managed by the appropriate plugin (the Switch Plugin or the Wireless Plugin). For plugin-managed NAS devices, make sure that each plugin is configured with the necessary RADIUS secret.
You can use the following templates to evaluate network readiness:

- Cisco Switch Readiness Template
- Cisco Switch Port Readiness Template

**Cisco Switch Readiness Template**

Prior to implementing 802.1X endpoint authentication, determine your network environment readiness. Use the **Cisco Switch Readiness** template to generate a policy that evaluates the readiness of Cisco switches to participate in 802.1X authentication.

It is recommended that you have a basic understanding of Forescout 8.1 policies before working with the templates. Refer to the Forescout Templates and Policy Management chapters of the Forescout Administration Guide.

**Prerequisites**

Before you run a policy based on this template, verify that the Switch Plugin is configured to manage the switch, including:

- CLI is selected for use and CLI credentials are configured
- The selected MAC read/write method includes CLI
- The `cdm` configuration flag is activated

Refer to the Network Module: Switch Plugin Configuration Guide for configuration details.

**Create a Policy**

This section describes how to create a policy based on the Cisco Switch Readiness template.

**To create a policy:**

1. In the Console, select the **Policy** tab.

2. Select **Add**. The Policy Wizard opens.
3. In the navigation tree, select **RADIUS > 802.1X > 802.1X Readiness** and then select **Cisco Switch Readiness**.

4. Select **Next**.

5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Use a name that clearly reflects what the policy does. Use a descriptive name that identifies what your policy verifies and what actions are taken.
   - Ensure that the name identifies whether the policy criterion must be met or not met.
   - Make policy names unique. Avoid policies with similar, generic names.
Policy names appear in the Policy Manager, the Views pane, Reports, and in other features. Precise names make working with policies and reports more efficient.

6. Select Next. The Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.

The following options are available:

− **All IPs**: Include all IP addresses in the Internal Network.
− **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box, and select Segments from the Scope pane.
− **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

You can filter the range by including only certain policy groups and/or excluding devices or users that should be ignored when using a policy.

8. Select Next. The Sub-Rules pane opens and lists the default sub-rules of the policy generated by the template. Sub-rules can be modified at this point if required.

9. Select Finish. The policy is created.

**Cisco Switch Readiness Main Rule**

Forescout 8.1-managed switches that meet the following criteria match the main rule of this policy:

- Switch vendor is Cisco
- The Switch Plugin has resolved Running Config property information for the switch
Cisco Switch Readiness Sub-Rules

Sub-rules of this policy are used to evaluate the readiness of Cisco switches to participate in 802.1X authentication. By default, these sub-rules are not defined with policy actions.

Switches are inspected against each sub-rule in the order listed. The sub-rules verify the following about a switch configuration:

- The commands verifying switch configuration use the Cisco IOS version 12.2 command syntax.

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. AAA Not Enabled</td>
<td>Verifies if any one of the following is true on the switch:</td>
</tr>
<tr>
<td></td>
<td>- <code>aaa new-model</code> is not configured</td>
</tr>
<tr>
<td></td>
<td>- <code>no aaa new-model</code> is configured</td>
</tr>
<tr>
<td></td>
<td>When the switch configuration matches one of these conditions, the switch is not ready for 802.1X authentication.</td>
</tr>
<tr>
<td>2. 802.1X Authentication Method List Not Created</td>
<td>Verifies if the following is true on the switch:</td>
</tr>
<tr>
<td></td>
<td>- <code>aaa authentication dot1x</code>... is not configured</td>
</tr>
<tr>
<td></td>
<td>When the switch configuration matches this condition, the switch is not ready for 802.1X authentication.</td>
</tr>
<tr>
<td>3. Dot1X Not Globally Enabled</td>
<td>Verifies if the following is true on the switch:</td>
</tr>
<tr>
<td></td>
<td>- <code>dot1x system-auth-control</code> is not configured</td>
</tr>
<tr>
<td></td>
<td>When the switch configuration matches this condition, the switch is not ready for 802.1X authentication.</td>
</tr>
<tr>
<td>4. RADIUS Server Not Configured</td>
<td>Verifies if the following is true on the switch:</td>
</tr>
<tr>
<td></td>
<td>- <code>radius-server host &lt;IP address&gt;</code> is not configured</td>
</tr>
<tr>
<td></td>
<td>When the switch configuration matches this condition, the switch is not ready for 802.1X authentication.</td>
</tr>
</tbody>
</table>
5. Key Between Switch and RADIUS Not Configured
Verifies if the following is true on the switch:
 `radius-server...key <string>` is not configured
When the switch configuration matches this condition, the switch is not ready for 802.1X authentication.

6. Using VSA Not Enabled
Verifies if the following is true on the switch:
 `radius-server vsa send` is not configured
When the switch configuration matches this condition, the switch is ready for 802.1X authentication, although unable to use VSAs for authorization, for example, ACLs.

7. RADIUS Re-Authentication Not Configured
Verifies if the following is true on the switch:
 `aaa server radius dynamic-author` is not configured
When the switch configuration matches this condition, the switch is ready for 802.1X authentication, although unable to respond to re-authentication (CoA) requests initiated by the plugin.

8. Switch Configuration Ready
When the inspected switch does not match any of the preceding policy sub-rules, the switch is ready for 802.1X authentication.

Following changes to a switch configuration, the Cisco Switch Readiness policy cannot immediately detect the applied configuration updates. Therefore, it is not recommended to immediately re-check this policy after making switch configuration changes. This is because the Cisco Switch Readiness policy evaluates a managed switch’s configuration using the Running Config property information that is periodically obtained by the Switch Plugin from the switch. The frequency at which the Switch Plugin obtains this information is defined by the device properties query rate, which is calculated per managed switch. By default, this query rate is every 10 minutes.

**Cisco Switch Port Readiness Template**

Prior to commencing with 802.1X endpoint authentication, determine your network environment readiness for deploying 802.1X authentication. Use the Cisco Switch Port Readiness template to generate a policy that evaluates the readiness of Cisco switch ports to participate in 802.1X authentication. The endpoints connected to a switch port are inspected to determine the configuration of that switch port.

It is recommended that you have a basic understanding of Forescout 8.1 policies before working with the templates. Refer to the Forescout Templates and Policy Management chapters of the Forescout Administration Guide.

**Prerequisites**
Before you run a policy based on this template:

- Verify that the Switch Plugin is configured to manage the switch, including:
  - CLI is selected for use and CLI credentials are configured
  - The selected MAC read/write method includes CLI
Create a Policy

This section describes how to create a policy based on the Cisco Switch Port Readiness template.

To create a policy:

1. In the Console, select the **Policy** tab.

2. Select **Add**. The Policy Wizard opens.

3. In the navigation tree, select **RADIUS > 802.1X > 802.1X Readiness** and then select **Cisco Switch Port Readiness**.

4. Select **Next**.
5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Use a name that clearly reflects what the policy does. Use a descriptive name that identifies what your policy verifies and what actions are taken.
   - Ensure that the name identifies whether the policy criterion must be met or not met.
   - Make policy names unique. Avoid policies with similar, generic names.

   Policy names appear in the Policy Manager, the Views pane, Reports, and in other features. Precise names make working with policies and reports easier.

Select Next. The Scope pane and the IP Address Range dialog box open.

6. Use the IP Address Range dialog box to define which endpoints are inspected.

The following options are available:
   - **All IPs**: Include all IP addresses in the Internal Network.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box, and select **Segments** from the Scope pane.
   - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
You can filter the range by including only certain policy groups and/or excluding devices or users that should be ignored when using a policy.

**7.** Select **Next**. The Sub-Rules pane opens and lists the default sub-rules of the policy generated by the template. Sub-rules can be modified at this point if required. For details, see **Cisco Switch Port Readiness Sub-Rules**.

**8.** Select **Finish**. The policy is created.

**Cisco Switch Port Readiness Main Rule**

The endpoints connected to a switch port are inspected to determine the configuration of that switch port. Switch ports of Forescout-platform-managed switches that meet the following criteria match the main rule of this policy:

- The switch vendor of the switch port being evaluated is Cisco
- The Switch Plugin has resolved *Switch Port Configurations* property information for the endpoints connected to the switch port being evaluated (configuration detail of the switch interface to which an endpoint is connected).

**Cisco Switch Port Readiness Sub-Rules**

Sub-rules of this policy are used to evaluate the readiness of Cisco switch ports to participate in 802.1X authentication. By default, these sub-rules are not defined with policy actions.

![Cisco Switch Port Readiness Sub-Rules](image)

The endpoints connected to a switch port are inspected against each sub-rule in the order listed and verify the following about a switch port configuration:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. PAE Authenticator Not Configured</td>
<td>Verifies if the following is true for the switch port:</td>
</tr>
<tr>
<td></td>
<td>- <em>dot1x pae authenticator</em> is not configured</td>
</tr>
<tr>
<td></td>
<td>When this condition is true, the switch port is not ready for 802.1X authentication.</td>
</tr>
</tbody>
</table>
2. **802.1X Authentication on the Port Not Enabled**

Verifies if the following is true for the switch port:
- `authentication port-control auto` is not configured

When this condition is true, the switch port is not ready for 802.1X authentication.

3. **MAB Not Configured**

Verifies if the following is true for the switch port:
- `mab` is not configured

When this condition is true, the switch port is not ready for 802.1X authentication.

4. **Switch Port Configuration Ready**

When the inspected endpoints connected to the switch port do not match any of the preceding policy sub-rules, the switch port is ready for 802.1X authentication.

---

**Endpoint Readiness**

This section provides information about what to do in order to determine your network environment readiness for deploying 802.1X authentication. See also Configure Endpoint Supplicant.

You can use the following template to evaluate endpoint readiness:

- Wired Windows 7 Endpoint Readiness Template

**Wired Windows 7 Endpoint Readiness Template**

Prior to commencing with 802.1X endpoint authentication, determine your network environment readiness for deploying 802.1X authentication. Use the **Wired Windows 7 Endpoint Readiness** template to generate a policy that evaluates the readiness for 802.1X authentication of wired endpoints, running Windows 7.

It is recommended that you have a basic understanding of Forescout 8.1 policies before working with the templates. Refer to the Forescout Templates and Policy Management chapters of the Forescout Administration Guide.

**Prerequisites**

Before you run a policy based on this template:

- Verify that endpoints are classified in the Windows group (can be accomplished by running the Forescout Primary Classification policy)
- Verify that endpoints are classified in the Corporate Hosts group (can be accomplished by running the Forescout Corporate/Guest Control policy)
- Verify that the Forescout HPS Inspection Engine, version 10.8 or above, manages the endpoints

**Create a Policy**

This section describes how to create a policy based on the Wired Windows 7 Endpoint Readiness template.
To create a policy:

1. In the Console, select the Policy tab.


3. In the navigation tree, select RADIUS > 802.1X > 802.1X Readiness and then select Wired Windows 7 Endpoint Readiness.

4. Select Next.
5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Use a name that clearly reflects what the policy does. Use a descriptive name that identifies what your policy verifies and what actions are taken.
   - Ensure that the name identifies whether the policy criterion must be met or not met.
   - Make policy names unique. Avoid policies with similar, generic names.

   Policy names appear in the Policy Manager, the Views pane, Reports and in other features. Precise names make working with policies and reports Select Next. The Scope pane and the IP Address Range dialog box open.

6. Select Next. The Scope pane and the IP Address Range dialog box open.

7. Use the IP Address Range dialog box to define which endpoints are inspected.

   The following options are available:
   - **All IPs**: Include all IP addresses in the Internal Network.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

You can filter the range by including only certain policy groups and/or excluding devices or users that should be ignored when using a policy.

8. Select **Next**. The Sub-Rules pane opens and lists the default sub-rules of the policy generated by the template. Sub-rules can be modified at this point if required. For details, see Wired Windows 7 Endpoint Readiness Sub-Rules.

9. Select **Finish**. The policy is created.

**Wired Windows 7 Endpoint Readiness Main Rule**

Forescout-platform-detected endpoints that meet the following criteria match the main rule of this policy:

- Classified as a member of the **Corporate Hosts** group
- Resolved as remotely managed (**Windows Manageable Domain** property) or as managed by Secure Connector (**Windows Manageable SecureConnector** property)
- Resolved as running the Windows 7 operating system (**OS Fingerprint** property)

**Wired Windows 7 Endpoint Readiness Sub-Rules**

Sub-rules of this policy are used to evaluate the readiness for 802.1X authentication of wired endpoints, running Windows 7. By default, these sub-rules are not defined with policy actions.
Wired Windows 7 endpoints are inspected against each sub-rule in the order listed and verify the following about an endpoint configuration:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1. Wired AutoConfig Service Not Running           | Verifies if the following is true on the endpoint: \[ Wired AutoConfig \] service is not running
When this condition is true, the endpoint is not ready for 802.1X authentication. |
| 2. 802.1X Authentication Not Enabled             | Verifies if the following is true for the supplicant installed on the endpoint:
- Enable IEEE 802.1X authentication configuration is not enabled
When this condition is true, the endpoint is not ready for 802.1X authentication. |
| 3. Required Authentication Method Not Selected    | Verifies if both of the following are true for the supplicant installed on the endpoint:
- Network authentication method is not PEAP
- Network authentication method is not Smart Card or other certificate
When both conditions are true, the endpoint is not ready for 802.1X authentication. |
| 4. Endpoint Is Ready                              | When the inspected endpoint does not match any of the preceding policy sub-rules, the endpoint is ready for 802.1X authentication. |

**User Directory Readiness**

This section provides the necessary User Directory Plugin configurations that enable and ensure use by the RADIUS Plugin of the configured user directories. The following topics are described:

- User Directory Plugin: General Pane
- User Directory Plugin: Settings Pane
- Using Microsoft Active Directory: Other Issues
- Using an External RADIUS Server
In the General pane of the User Directory Plugin consider the following configuration issues:

1. For the **Name** field:
   - A best practice is to enter the hostname of the configured domain server. This best practice is based on the possible use of this field by the RADIUS Plugin to join the machine to the domain.
   - This best practice is also applicable when adding a user directory replica and configuring its **Name** field in the Replicas pane of the User Directory Plugin.

   See User Directory Plugin: Settings Pane, bullet 2.

2. Make sure that both the **Use as directory** option and the **Use for authentication** option are enabled.

**User Directory Plugin: Settings Pane**

In the Settings pane of the User Directory Plugin consider the following configuration recommendations, best practices, and issues:

1. If the **DNS Detection** option is enabled, then the RADIUS Plugin automatically selects a user directory (Microsoft Active Directory) server FQDN. Take note of the following:
   a. The RADIUS Plugin queries domain to obtain the domain server FQDN list; the plugin uses the domain configured in the **Domain** field in the Directory section of the User Directory Plugin Settings pane.
   b. A domain controller FQDN is chosen based on quickest responder.
   c. The plugin uses the selected FQDN to join the Forescout machine to the domain.
2. However, if the **DNS Detection** option is not enabled, the RADIUS Plugin statically builds a domain server FQDN list by concatenating the Main/replicas configured **Name** field with its configured **Domain** field. Take note of the following:
   
   a. A domain controller FQDN is chosen based on quickest responder.
   
   b. The plugin uses the selected FQDN to join the Forescout machine to the domain.

3. Regardless of the state of the **DNS Detection** option is (enabled/not enabled), heartbeat verification is performed every minute.

4. For the Foescout RADIUS server to authenticate using Microsoft Active Directory, the CounterACT device must be bound to (join) the domain. When the RADIUS Plugin is started or when its configuration is saved, the CounterACT device joins the relevant domain using the user credentials that are defined in the **Administrator** field of the Settings pane for that domain.

5. In the Active Directory server, sufficient privileges for the **user**, defined in the **Administrator** field of the Settings pane, must include the following definition:

   a. Allow **user** to create computer objects with read/write [join Linux machine to domain] control. To delegate admin privileges see: [https://wiki.samba.org/index.php/Delegation/Joining_Machines_to_a_Domain](https://wiki.samba.org/index.php/Delegation/Joining_Machines_to_a_Domain)

6. When 802.1X authentication by an Appliance uses multiple user directories, then for each selected, authenticating user directory defined in the RADIUS Plugin Authentication Sources tab, verify that the following information is defined in the User Directory Plugin:

   a. Additional Domain Aliases: In the Additional Domain Aliases section of the Settings pane, in the **Specify** field, first define the user directory's NetBIOS domain name, followed by the definition of the NetBIOS domain name of each of its trusted domains, for example, a child domain. Use a comma to separate between NetBIOS domain entries.

   b. If the **Domain** field in the Directory section of the Settings pane already contains the NetBIOS domain name then there is no need to also enter this name in the **Specify** field. For example, the **Domain** field contains the entry `glbl.mycompany.com`, there is no need to also enter `glbl` in the **Specify** field.

---

**Using Microsoft Active Directory: Other Issues**

If you plan to use Microsoft Active Directory for authentication:

- To avoid difficulties when a Forescout machine attempts to join a domain, it is recommended that the Forescout machine hostname have a maximum length of 15 characters. Refer to [https://support.microsoft.com/en-gb/kb/909264](https://support.microsoft.com/en-gb/kb/909264)

- Network Time Protocol (NTP) configuration of CounterACT devices [Enterprise Manager, Appliances] must be aligned with the domain to successfully obtain a Kerberos ticket.
Using an External RADIUS Server

If you plan to use an external RADIUS server as an authentication source for the RADIUS Plugin, configure (add) the server in the User Directory Plugin.

- Failover time between a configured, external RADIUS server, and its replicas is 1 minute. Once a failed, external RADIUS server comes back to life, it is marked as alive again.

Configure the Plugin

This section describes how to configure the various plugin components in order for the RADIUS Plugin to provide authentication and authorization of the endpoints attempting to access your organization's network. This section presents the following topics:

- Configure Authentication Sources
- Configure Pre-Admission Authorization
- Configure RADIUS Settings
- Configure the Plugin Per Appliance
- Configure MAC Access Bypass

Use the Forescout Console, running on the Enterprise Manager, to configure the plugin.

To configure the plugin:

1. In the Console, select **Tools > Options > Modules**. The Modules pane opens.

2. In the Modules pane, select the **Authentication** module. The plugins, which are installed as part of the Forescout Authentication Module, are listed beneath the Authentication entry.

3. In the Modules pane, select the **RADIUS** entry in the table.
4. Select **Configure**. The RADIUS pane opens in the Options window. Configure the plugin in each of the tabs, as required.

**Configure Authentication Sources**

Use the Authentication Sources tab to select the servers that the CounterACT RADIUS server can query to perform 802.1X authentication of endpoints.

Supported authentication sources:

- Microsoft Active Directory Server
- External RADIUS server
(Centralized Licensing only) If you do not have a valid Forescout eyeControl (ForeScout CounterACT Control) license, you cannot add authentication sources.

To add an authentication source:

1. In the Authentication Sources tab, select Add. The Add Authentication Sources dialog box opens.

   The Active Directory servers and the external RADIUS servers listed in this dialog box are configured in the User Directory Plugin. For details about the necessary User Directory Plugin configurations, see User Directory Readiness.

2. In the dialog box, select one or more entries. You can select RADIUS servers, Microsoft Active Directory servers, or a combination of both types.

3. Select OK. The Authentication Sources tab displays the added authentication sources.

The tab presents the following information for each authentication source entry:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the authentication source as configured in the User Directory Plugin. Authentication sources that the CounterACT RADIUS server cannot use (query) display the text (Source NOT in USE) immediately after their name. For an explanation, see the Domains column description.</td>
</tr>
<tr>
<td>Type</td>
<td>The server type of the authentication source as configured in the User Directory Plugin. For CounterACT RADIUS servers, the supported types are Microsoft Active Directory and RADIUS (external RADIUS server).</td>
</tr>
<tr>
<td>Domains</td>
<td>The domains that the authentication source is assigned to handle; these are domains that could be supplied in 802.1X authentication requests.</td>
</tr>
</tbody>
</table>
- **For Microsoft Active Directory** authentication sources:
  The information appearing in this column comes from the domain and additional domain aliases that are configured in the User Directory Plugin. Column information is view-only.
- **For RADIUS** authentication sources:
  Domain assignment must be manually configured. For details, see the **Configure** button in Work with Authentication Sources.

Authentication sources must fulfill at least one of the following criteria, in order for the CounterACT RADIUS server to be able to use (query) them:
- The source has an assigned domain
- The source is designated as the **DEFAULT Source**. See the **Set Default** button in Work with Authentication Sources.
- The source is designated to handle the **NULL Domain**. See the **Set NULL** button in Work with Authentication Sources.

---

**Work with Authentication Sources**

The following buttons on the Authentication Sources tab let you handle authentication sources:

- **Add**: Opens the Add Authentication Sources dialog box. In the dialog box, select one or more entries to add as an authentication source in the Authentication Sources tab. You can select RADIUS servers, Microsoft Active Directory servers, or a combination of both types.

- **Configure**: Opens a configuration dialog box for a selected authentication source:
  - For a **Microsoft Active Directory** authentication source, the Configure Active Directory dialog box opens:
    - This dialog box lists the domain and domain aliases that are configured in the User Directory Plugin for the source. This information is view-only.
    - In the **Saved Test Credentials** pane, select an entry in the Domain list above this pane. Then, in the pane, enter credentials that the plugin uses to access and test the functionality of that authentication source.
  - For a **RADIUS** authentication source, the Edit Radius Proxy dialog box opens:
    - In the **Domain** field, enter a domain NetBIOS name, as it would appear in the RADIUS access request, and select **+Add**. Repeat this step to enter additional domain NetBIOS names, as necessary, as a RADIUS authentication source can be assigned to handle multiple domains.
• **Set Default**: Designates the authentication source as the default authentication source, and the text *DEFAULT Source* appears in the **Domains** column. Only one authentication source can be designated as the default authentication source.

• **Set Null**: Designates the authentication source as the null domain handler, and the text *NULL Domain* appears in the **Domains** column. At any given time, only one authentication source can be designated as the null domain handler.

  An authentication source can be assigned multiple domains and/or can be designated the default authentication source and/or can be designated the null domain handler. See [Determine the Authentication Source to Query](#).

• **Join**: (For a selected *Microsoft Active Directory* authentication source only) Opens the Join Domain: Provide Credentials dialog box and lets you:
  - Provide administrator credentials that the plugin uses to join CounterACT device(s) to the Active Directory domain.
  - Select **Join** to launch a plugin attempt to join CounterACT devices to the Active Directory domain, using the provided credentials.

  For further information, see [Join CounterACT Devices to Active Directory Domain](#).

• **Test**: Runs a plugin test of the functionality of a selected authentication source. For further information, see [Test Authentication Source Functionality](#).

• **Remove**: Removes a selected authentication source from the Authentication Sources tab.

After changing authentication source information, select **Apply** to save these updates in the plugin configuration.
**Determine the Authentication Source to Query**

Per endpoint authentication request (RADIUS *access request*), the CounterACT RADIUS server decides on the authentication source to query, using the following ordered decision criteria:

1. When the RADIUS *access request* provides an explicit domain, attempt to identify a regular expression (regex) match between the NetBIOS/domain name, as provided in the request, and the relevant expression that is defined in the **Domains** column of an authentication source. The CounterACT RADIUS server queries the matching authentication source. Supported RADIUS *access request* delimiters are:
   - `domain\user`
   - `user@domain`

2. When the RADIUS *access request* provides an explicit domain, and no authentication source is identified using criterion 1, and an authentication source is designated as the **DEFAULT Source** in the **Domains** column, the CounterACT RADIUS server queries the designated, default authentication source.

3. When the RADIUS *access request* does not provide an explicit domain and an authentication source is designated as the **NULL Domain** handler in the **Domains** column, the CounterACT RADIUS server queries the authentication source designated to handle requests containing no domain.

For cases where the UserPrincipalName (UPN) does not match the sAMAccountName (SAM), see the **UserPrincipalName does not match sAMAccountName** use case.

**Authenticating with Domains Not Directly Mapped to a Configured Authentication Source.**

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

To define a list of domains to map back to the default RADIUS domain, complete the following steps:

1. Log in to the CLI on the Appliance.
2. Run the following command: `fstool set_property config.default_domain_map_list.value <value1>,<value2>..<valueN>`

   For Example: `fstool set_property config.default_domain_map_list.value test.some.domain.com, test2.another.domain.com`

**Join CounterACT Devices to Active Directory Domains**

Before the CounterACT RADIUS server can query a *Microsoft Active Directory* authentication source, the RADIUS Plugin must first join all CounterACT devices to each of the authentication source’s assigned domains. The credentials (administrator level) that the plugin uses for the join must already be configured via the Join Domain: Provide Credentials dialog box. To access this dialog box and initiate a plugin join attempt, select **Join**.
After providing the credentials and confirming the Join Domain: Confirmation window opens and presents the following information:

**Join the following CounterACT device(s) to domain:** <active directory domain>

- <CounterACT device-1>
- 
- ...
- <CounterACT device-n>

**Continue?**

When you select Yes, the Results of Join Domain: <active directory domain> window opens and presents the following information:

**Attempting to join domain:** <active directory domain>

**Selected domain controller name (FQDN):** <domain controller FQDN>

**Result:** <result>

- If the join is successful, the following information is displayed:
  
  **Result: SUCCESS**
  
  **CounterACT Appliance is joined to domain.**

- If the join is not successful, the following information is displayed:
  
  **Result: FAILURE**
  
  **CounterACT Appliance is not joined to domain.**

  **CAUSE:** <error message>

Once a CounterACT device is successfully joined to an Active Directory domain, it remains joined.

Forescout recommends performing the join at step 4 of the authentication source configuration flow, as follows:
1. Add a Microsoft Active Directory authentication source.
2. Configure the source's test credentials.
3. Repeat steps 1 through 2 as necessary for multiple authentication sources.
4. Initiate plugin join attempt per authentication source.
5. Run plugin test of the authentication source functionality per source.
6. Select **Apply** to save the modified plugin configuration.

**Test Authentication Source Functionality**

Initiate a plugin test of a selected authentication source's functionality by selecting the **Test** button in the Authentication Sources tab. The **Test Authentication Source: Confirmation** window opens and presents the following information:

- For a **Microsoft Active Directory** authentication source:
  
  **Test functionality of Active Directory** `<NetBIOS name>` **with the following CounterACT device(s):**

- For a **RADIUS** authentication source:

  **Test functionality of RADIUS server** `<RADIUS server name>` **with the following CounterACT device(s):**

- The CounterACT devices to be tested with the selected authentication source:
  - `<CounterACT device-1>`
  - 
  - 
  - `<CounterACT device-n>`

**Continue?**

If you select **Yes**, the **Results of Test Authentication Source:** window opens.

**Testing with Microsoft Active Directory Server**

If the test is performed with a **Microsoft Active Directory** authentication source, the **Results of Test Authentication Source:** window presents the following information:

**Testing functionality of authentication source** `<NetBIOS name>` **of type**

**Active Directory**

**Domain controller name (FQDN):** `<domain controller FQDN>`

If the CounterACT device being tested is joined to the domain, the test proceeds and the following information is displayed:

**CounterACT Appliance is joined to domain**

**Testing authentication using configured test credentials for joined Appliance**

**Authentication test:** `<result>`

- If the test is successful, the `<result>` displayed is:
  
  **SUCCEEDED**
− If the test is not successful, the <result> displayed is:

**FAILED**

The test does not proceed, and an applicable error message is displayed, when one or more of the following conditions are true:

• The CounterACT device being tested is not joined to the domain
• The RADIUS Plugin is stopped
• Test credentials are not configured for CounterACT RADIUS Plugin use

**Testing with RADIUS Server**

When the test is performed with a RADIUS authentication source, the Results of Test Authentication Source: window presents the following information:

- **Testing functionality of authentication source** <RADIUS server name> of type RADIUS
- **Testing external server RADIUS service status on port** <port #>: <result>
  - If the test is successful, the <result> displayed is: **SUCCESS**
  - If the test is not successful, the <result> displayed is: **FAILURE**

If the preceding test fails, the plugin subsequently performs a connectivity test with the RADIUS server, and the following information is displayed:

- **Testing external server connectivity status (ping):** <result>
  - If the test is successful, the <result> displayed is: **SUCCESS**
  - If the test is not successful, the <result> displayed is: **FAILURE**

For information about the full plugin configuration test, see Testing and Troubleshooting.

**Configure Pre-Admission Authorization**

Use the Pre-Admission Authorization tab to define the set of prioritized rules that the CounterACT RADIUS server uses to authorize authenticated endpoints. The rules are evaluated against authenticated endpoints in order of priority.

The CounterACT RADIUS server evaluates pre-admission authorization rules when no other Forescout 8.1 source, such as policy action or MAC Address Repository, provides the authorization to impose on an authenticated endpoint. For example, prior to an endpoint being admitted to an organization’s network. See Authentication-Authorization Processing Flow.

• Pre-admission authorization rules are evaluated in order of priority. A rule’s evaluation priority is displayed in the Rule Priority column of the Pre-Admission Authorization table.
Once an endpoint matches a pre-admission authorization rule, no subsequent rules are evaluated for the endpoint.

- The plugin supplies a default rule in the Pre-Admission Authorization table - *deny network access to any user*. You cannot remove this rule. However, you can edit this rule and modify its detail.

In the CounterACT RADIUS Server's reply message it sends to the NAS device:

- For authenticated endpoints matching a rule's condition, the CounterACT RADIUS server imposes the rule's authorization on the endpoint.

The Pre-Admission Authorization tab displays the current set of defined pre-admission authorization rules.

In the Pre-Admission Authorization tab, you can perform the following actions:

- **Add** new pre-admission authorization rules. Select **Add**. The Add Pre-Admission Authorization Rule window opens. Define rule details [Condition, Authorization]. Selecting **OK** adds the rule to the top of the list of entries in the Pre-Admission Authorization table.

- **Edit** rules. Select a rule and then select **Edit**. The Edit Pre-Admission Authorization Rule window opens. Modify the existing details [Condition, Authorization] of the rule. Selecting **OK** updates the rule in the Pre-Admission Authorization table.
- **Remove** rules. Select a rule and then select **Remove**. The rule is removed from the Pre-Admission Authorization table.

- **Duplicate** rules. Select a rule and then select **Duplicate**. The Duplicate Pre-Admission Authorization Rule window opens. Maintain or modify the existing details [Condition, Authorization] of the rule. Selecting **OK** adds the rule to the bottom of the list of entries in the Pre-Admission Authorization table.

- Change the order (priority) in which rules are evaluated. Select a rule and then select **Move Up** or **Move Down**. Rule evaluation priority is displayed in the **Rule Priority** column.

- **Export** the rules defined in the Pre-Admission Authorization table to a CSV file.

- **Import** rules from a CSV file into the Pre-Admission Authorization table.

After you perform any of the above actions, select **Apply** to save the modified plugin configuration.

**(Centralized Licensing only) If you do not have a valid Forescout eyeControl (ForeScout CounterACT Control) license, you cannot add, edit, or import pre-admission authorization rules.**

**Rule Configuration**

Each pre-admission authorization rule includes the following sections:

- Condition
- Authorization
Rule Condition

The rule condition is evaluated by the CounterACT RADIUS server to identify a match with authenticated endpoints. A condition can be composed of a single criterion or multiple criteria. For a condition with multiple criteria, the authenticated endpoint must match all criteria of the condition to be evaluated as matching the condition.

You can perform the following actions in the Condition section:

- **Add** a new rule condition.
- **Edit** a rule condition. Select a rule condition and then select *Edit*.
- **Remove** a rule condition. Select one or more rule conditions and then select *Remove*.

After you add, edit, or remove rule conditions, select **OK** in the Pre-Admission Authorization Rule window to update the rule in the Pre-Admission Authorization table. Select **Apply** to save the modified plugin configuration.
Each criterion in a rule condition includes the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criterion Name</td>
<td>Select a supplied endpoint attribute that the CounterACT RADIUS server uses to evaluate authenticated endpoints for a match. Unless otherwise noted, the attributes are standard RADIUS request attributes that are also RADIUS Plugin properties. For a description of these attributes, see Properties for Use in Policy Conditions.</td>
</tr>
</tbody>
</table>

The attributes available for configuration are:

- **Authentication-Type**
- **Called-Station-ID**
- **Calling-Station-ID**
- **Certificate-Common-Name**
- **Certificate-Issuer**
- **Certificate-Subject**
- **Certificate-Subject-Alternate-Name-Email**
- **Day and Time Restriction** – This attribute is compared with the day/time of the received endpoint authentication request.
- **EAP-Type**
- **LDAP-Group** – This attribute is compared with the user LDAP groups defined in the Microsoft Active Directory server of the domain in the User-name. By default, the plugin uses TLS to perform a secure LDAP query to the Active Directory server. Valid servers are configured in the Authenticating User Directories table of the Authentication Sources tab.

In order for the plugin to perform this comparison, the CA certificate of the Microsoft Active Directory server must be defined as a trusted certificate in the Console certificate interface. Refer to the Configuring the Certificate Interface section in the Forescout Administration Guide for instructions. See Additional Forescout Documentation for information on how to access this guide.

The following are examples of valid text to enter in this field:

- **Straightforward text**, as in Students_Eng or Hospital_Admin
- **Text containing the use of the wildcard character**, as in Hospital* (any user in a group beginning with Hospital is matched) or as in *Admin (any user in a group ending with Admin is matched).
- **Using LDAP group in a Pre-admission authorization rule where the authentication method is EAP-TLS Authentication using Certificates causes the authentication to fail. The failure occurs because the plugin is unable to query an AD server based on the user name presented in the certificate.**
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Found in MAR</td>
<td>This attribute is compared with the MAC addresses listed in the MAC Address Repository, and the NAS device also requested the evaluated endpoint to be authenticated using MAC address bypass (MAB).</td>
</tr>
<tr>
<td>MAR Comment</td>
<td>Free text. Use this attribute to assign a tag to endpoints that are listed in the MAC Address Repository, to later support their appropriate authorization, based on the assigned MAR comment.</td>
</tr>
<tr>
<td>NAS-IP-Address</td>
<td>The IPv4 address of the switch or the WiFi AP/Controller</td>
</tr>
<tr>
<td>NAS-IPv6-Address</td>
<td>The IPv6 address of the switch or the WiFi AP/Controller</td>
</tr>
<tr>
<td>NAS-Port-Type</td>
<td></td>
</tr>
<tr>
<td>SSID</td>
<td></td>
</tr>
<tr>
<td>Tunneled-Method</td>
<td>The authentication method used in a protected EAP (PEAP) tunnel</td>
</tr>
<tr>
<td>Tunneled-User-Name</td>
<td>The user name used for the inner authentication phase of both Protected EAP-MSCHAPv2 and Protected EAP-TLS authentication processes. Usually, both inner and outer user names are the same. However, when the supplicant's Identity Privacy field is configured, then the inner user-name (the Tunneled User Name) is the supplicant's true user name.</td>
</tr>
<tr>
<td>User-Name</td>
<td></td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Criterion Value</strong></td>
<td>For the selected attribute, define the attribute value used by the CounterACT RADIUS server to evaluate authenticated endpoints for a match. Depending on the selected attribute, one of the following methods is used to define the attribute value:</td>
</tr>
<tr>
<td></td>
<td>- Select from a menu of evaluation instruction options [Contains, Matches, Starts With, Ends With, Matches Expression, Any Value] combined with an Expression field. In this field, enter any combination of alphanumeric and special characters or a regular expression. The following rules apply to data being entered in the Expression field:</td>
</tr>
<tr>
<td></td>
<td>- This field is case sensitive.</td>
</tr>
<tr>
<td></td>
<td>- To escape any special character except the backslash, prefix the special character with four (4) consecutive backslashes. For example, <code>.engineering</code> must be provided in the field as <code>\\\\.engineering</code>.</td>
</tr>
<tr>
<td></td>
<td>- To escape a backslash special character, enter a total of eight (8) consecutive backslashes. For example, <code>finance\eastern</code> must be provided in the field as <code>finance\\\\\\\\\eastern</code>.</td>
</tr>
<tr>
<td></td>
<td>- For both the Called Station ID and the Calling Station ID attributes, only lowercase alphanumeric characters, without any separating space or special character, are valid.</td>
</tr>
<tr>
<td></td>
<td>- Select from a table the days of the week and/or hours of the day to evaluate and/or not evaluate.</td>
</tr>
<tr>
<td></td>
<td>- Choose from a menu of available values.</td>
</tr>
<tr>
<td></td>
<td>- Select between evaluation instruction buttons [Meets this criterion, Does not meet this criterion].</td>
</tr>
<tr>
<td></td>
<td>- In an Expression field, enter any combination of alphanumeric and special characters.</td>
</tr>
</tbody>
</table>

**Rule Authorization**

For an authenticated endpoint that matches the rule condition, the CounterACT RADIUS server imposes the defined rule authorization on the endpoint in the reply message it sends to the NAS device.

In the Authorization section, the authorization options that can be defined are:

- **Deny Access**: Select this option to deny the authenticated endpoint access to the organization's network. When selected, the VLAN field is disabled. This option is selected by default.

- **VLAN**: Define the VLAN to which the NAS device must assign the authenticated endpoint. Enter the VLAN ID or the VLAN name. This field accepts alphanumeric characters.

- **Attribute-Value Pair**: Attribute-value pair (AVP) assignments are imposed on the connection that the NAS device maintains for the authenticated endpoint. Multiple AVPs can be defined.
You can perform the following AVP configuration actions in the Authorization section:

- **Add** a new AVPs. For details, see Adding/Editing Attribute-Value Pairs.
- Use a template to add new AVPs. Select Templates to use one of several different templates to add an AVO. Each template provides AVPs that address a specific authorization use case. For details, see Attribute-Value Templates.
- **Edit** an existing AVP. Select an AVP and then select Edit.
- **Remove** AVPs. Select one or more AVPs and then select Remove.

After you add, edit, or remove AVPs, select OK in the Pre-Admission Authorization Rule window to update the rule in the Pre-Admission Authorization tab. Select **Apply** to save the modified plugin configuration.

After an endpoint is admitted to the network, additional or updated post-connect authorizations can be applied to such endpoints via Forescout 8.1 policies using the RADIUS Authorize action. For information about defining the RADIUS Authorize action, see Actions.

**Adding/Editing Attribute-Value Pairs**

In the Authorization section of the Add Pre-Admission Authorization Rule window, selecting Add opens the Add Attribute-Value Pair dialog box. This dialog box provides you with access to a repository of attributes from which to select and define the necessary values.

On the left side of the Add Attribute-Value Pair dialog box, select Attributes to reveal the following attribute groups:

- **Vendors**: Expand this group to display a wealth of vendor-specific attribute groups. Opening any of these groups displays vendor-specific attributes that are available to select for value assignment.
- **General**: Expand this group to display primarily RFC-specific attribute groups. Opening any of these groups displays the RFC-specific attributes that are available to select for value assignment.

You can also locate attributes using the Search field.

After assigning the necessary values for a selected attribute, select OK. The AVP is listed in the Authorization section of the Add Pre-Admission Authorization Rule window.
If you select an AVP in the Authorization section, and select **Edit**, the Edit Attribute-Value Pair dialog box opens. On left side, the **Attributes** option is open to the attribute you selected. On the right side, the selected attribute and its paired value are displayed.

**Attribute-Value Templates**

In the Authorization section of the Add Pre-Admission Authorization Rule window, selecting **Templates** opens the Add Attribute Template dialog box. This dialog box provides you with the option to add an attribute using an AVP template. Each template addresses a specific authorization use-case through its attribute(s) content.

- **Aruba-Guest**: Provides one Aruba-User-Role that requires you to assign it the necessary values. The authorization handling provided by the user-role attribute is required to either redirect user traffic to the controller or to forward the traffic locally.
- **Cisco-ACL (ingress)**: Provides two Cisco AVPs that impose access control list (ACL) authorization on each authenticated endpoint found to match the associated rule condition endpoint.
• **Cisco-Guest**: Provides two Cisco AVPs that require you to assign their necessary values. The authorization handling provided by these AVPs is required for the RADIUS Plugin to deliver enhanced Forescout guest management in the Forescout centralized web authentication solution. For details, see [Centralized Web Authentication](#).

• **Cisco-Network Device Administration**: Provides two AVPs, a RADIUS one and a Cisco one. The Cisco attribute requires you to assign it the necessary value. The authorization handling provided by these AVPs is required for the RADIUS Plugin to perform authentication and initial authorization on the administrators of an organization's network devices. For details, see [Network Device Administration](#).

• **HPE-Guest**: Provides one HPE-User-Role that requires you to assign it the necessary values. The authorization handling provided by the user-role attribute is required to either redirect user traffic to the controller or to forward the traffic locally.

• **Meraki-Guest**: Provides one Cisco AVP that requires you to assign it the necessary values. The authorization handling provided by this AVP is required for the RADIUS Plugin to deliver enhanced Forescout guest management in the Forescout centralized web authentication solution. For details, see [Centralized Web Authentication](#).

After assigning the necessary values for the template-provided attributes, select **OK**. The AVPs you added are listed in order in the Authorization section of the Add Pre-Admission Authorization Rule window.

### Configure RADIUS Settings

Use the RADIUS Settings tab to configure settings that are relevant when the CounterACT RADIUS server is the authenticating RADIUS server.

This tab includes the following settings:

- [RADIUS Server Basic Settings](#)
- [RADIUS OCSP Settings](#)
- [RADIUS CRL Settings](#)
- [RADIUS Advanced Settings](#)
## RADIUS Server Basic Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CounterACT RADIUS Logging</strong></td>
<td>By default, this option is disabled (not selected). When this option is selected, the CounterACT RADIUS server runs in debug mode, and CounterACT captures and logs RADIUS traffic processing details. Select this option to troubleshoot CounterACT RADIUS server processing issues. <strong>To avoid performance degradation, Forescout recommends disabling it after troubleshooting is complete.</strong></td>
</tr>
<tr>
<td><strong>CounterACT RADIUS Authentication Port</strong></td>
<td>The UDP port for receiving authentication requests from switches and wireless controllers. Default: 1812</td>
</tr>
<tr>
<td><strong>CounterACT RADIUS Accounting Port</strong></td>
<td>The UDP port for receiving accounting requests from switches and wireless controllers. Default: 1813</td>
</tr>
</tbody>
</table>
### Active Directory Port for LDAP Queries

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The LDAP port that the CounterACT RADIUS server uses to query domains. The available menu options are as follows:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Global Catalog</strong> – Uses port 3268.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Global Catalog over TLS</strong> – Uses port 3269. This is the default and recommended method.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Standard LDAP</strong> – Uses port 389.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Standard LDAP over TLS</strong> – Uses port 636.</td>
</tr>
<tr>
<td></td>
<td>- <strong>User Directory plugin port per AD</strong> – Per domain, as configured in User Directory Plugin.</td>
</tr>
</tbody>
</table>

### RADIUS OCSP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable OCSP</strong></td>
<td>By default, this option is disabled (not selected). When this option is selected, the CounterACT RADIUS server looks for an OCSP responder URL in the client certificate and verifies the revocation status of the client certificate against the OCSP responder. This makes it possible to immediately revoke certificates without the distribution of a new Certificate Revocation List (CRL). When this option is selected, the following options are available for selection:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Override Certificate OCSP URL</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>OCSP Use Nonce</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Ignore OCSP Responder Errors</strong></td>
</tr>
<tr>
<td><strong>Override Certificate OCSP URL</strong></td>
<td>By default, this option is disabled (not selected). When this option is selected, the CounterACT RADIUS server ignores the certificate's OCSP URL and uses the URL defined in the <strong>OCSP Responder URL</strong> field to obtain the revocation status of the certificate. When this option is selected, the <strong>OCSP Responder URL</strong> field is enabled for input.</td>
</tr>
<tr>
<td><strong>OCSP Responder URL</strong></td>
<td>Enter the URL of the OCSP responder that is used to obtain the revocation status of the client certificate. Use to override the certificate's OCSP URL.</td>
</tr>
<tr>
<td><strong>OCSP Use Nonce</strong></td>
<td>By default, this option is enabled (selected). For security reasons, it is recommended to use nonce in the OCSP query. This checkbox should be cleared only if the nonce setting is not supported by or cannot be enabled on the OCSP server.</td>
</tr>
<tr>
<td><strong>Soft-fail OCSP Requests</strong></td>
<td>By default, this option is disabled (not selected). When this option is selected, the CounterACT RADIUS server accepts the client certificate even if the CounterACT RADIUS server does not receive an OCSP response about the client certificate's revocation status.</td>
</tr>
</tbody>
</table>
### RADIUS CRL Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable CRL         | By default, this option is disabled (not selected). When this option is selected, the CounterACT RADIUS server consults the Appliance’s Certificate Revocation List (CRL) to verify the revocation status of the client certificate provided by an endpoint supplicant. If the CRL contains an entry for the certificate, then one of the following statuses are in effect for that certificate:  
  - The issuing certificate authority has permanently revoked that certificate  
  - The issuing certificate authority has temporarily revoked that certificate  
  CounterACT only supports the use of HTTP to download CRLs. When this option is selected, you can enter additional data in the Additional CDPs field. |

| Additional CDPs    | Additional CRL distribution points (CDPs).  
  (Optional) Enter one or more additional URLs from which the CounterACT RADIUS server downloads additional CRLs that it uses to verify the revocation status of the client certificate provided by an endpoint supplicant. Use a comma (,) to separate between multiple URLs.  
  Forescout only supports the use of HTTP to download CRLs. |

### RADIUS Advanced Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Fast-Reauthentication Cache</td>
<td>This option enables reconnection to wireless access points by using cached session keys, thereby enabling quick roaming between wireless access points.</td>
</tr>
<tr>
<td>Enable PAP-Authentication (Username and password only)</td>
<td>By default, this option is disabled (not selected). When this option is selected, the CounterACT RADIUS server authenticates endpoints using PAP (password authentication protocol).</td>
</tr>
</tbody>
</table>
| Enable Kerberos Authentication for LDAP Queries | When this option is selected, the CounterACT RADIUS server uses Kerberos, version 5, for querying an Active Directory server about user group membership (LDAP-Group). By default, this option is:  
  - Disabled (not selected) when upgrading from a previous Network Module version  
  - Enabled (selected) for a new installation of the Network Module  
  When this option is selected, the **Authenticate Using Machine Trust Account** option is available for selection. |
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Authenticate Using Machine Trust Account (requires Kerberos)** | When this option is selected, the CounterACT RADIUS server uses the machine trust account of the CounterACT device, instead of using user directory credentials, to access an Active Directory server for the purpose of querying the server about user group membership (LDAP-Group). By default, this option is: 
  - Disabled (not selected) when upgrading from a previous Network Module version 
  - Enabled (selected) for a new installation of the Network Module |

---

## Configure the Plugin Per Appliance

In the RADIUS Pane of the Console, configure the plugin in one of the following ways:

- In the **Default** tab, define a RADIUS Plugin configuration [Authentication Source, Pre-Admission Authorizations, Server Certificate, and RADIUS Settings]. By default, this RADIUS Plugin configuration is applied to all CounterACT devices that do not have a unique RADIUS Plugin configuration.

- Define additional, unique RADIUS Plugin configurations and designate each additional configuration to apply to either a single CounterACT device or multiple CounterACT devices.

In the example shown, the following RADIUS Plugin configurations are defined:

- A **Default** configuration
- A configuration for Appliance **20.33.1.24**
To create a unique 802.1X configuration for a single device:

1. Select the add tab. The Select CounterACT devices to configure dialog box opens and lists all your CounterACT devices [Enterprise Manager, Appliance1 - Applianceₙ].

2. Select a device and select, OK. A tab for the selected Appliance appears. This tab contains the full complement of RADIUS Plugin configuration tabs [Authentication Source, Pre-Admission Authorizations, Server Certificate and RADIUS Settings].

To create a unique 802.1X configuration for a group of devices:

1. Select the Add tab. The Select CounterACT devices to configure dialog box opens and lists all your CounterACT devices [Enterprise Manager, Appliance1 - Applianceₙ].

2. In the dialog box, take the following actions:
   a. Select the devices to include in the group.
   b. Type a name in the Name (Optional) field.

3. Select OK. A tab for the group of Appliances appears. This tab contains the full complement of RADIUS Plugin configuration tabs [Authentication Source, Pre-Admission Authorizations, Server Certificate, and RADIUS Settings].

To edit/delete a unique 802.1X configuration:

1. Select the tab of the unique 802.1X configuration.

2. Select the Edit icon or Delete icon to update the scope of the configuration. If you delete the configuration, the settings of the RADIUS Plugin configuration defined in the Default tab are re-applied to the affected CounterACT device(s).

Configure MAC Access Bypass

The MAC Address Repository (MAR) contains the MAC addresses of endpoints that do not have a functioning 802.1X supplicant but can be authenticated by the CounterACT RADIUS server using MAC address bypass (MAB).

The CounterACT RADIUS server handles MAB authentication for the endpoints listed in the MAC Address Repository (MAR). Endpoints that require MAB authentication and are not listed in the MAR are authenticated by the external RADIUS server that is configured in the Authentication Sources tab as the Null Domain handler for RADIUS access requests.

The CounterACT RADIUS server always handles the authorization of endpoints that require MAB authentication. Make sure that your Pre-Admission Authorization rules are well defined, to ensure that these endpoints are not denied access by default.
Optionally, per MAC address entry in this repository, define an authorization that is imposed on the MAB-authenticated endpoint by the CounterACT RADIUS server in its reply to the NAS device. Possible authorizations include: Deny access, VLAN assignment, and/or one or more attribute-value pair (AVP) assignments.

When a MAC address entry does not have an authorization defined in the repository, the CounterACT RADIUS server evaluates the pre-admission authorization rules to authorize the MAB-authenticated endpoint. For authenticated endpoints not matching any of the pre-admission authorization rules, the NAS device determines the authorization to impose on the endpoint. For details, see Configure Pre-Admission Authorization.

What You See in the Repository
The following information is defined, per entry in the MAC Address Repository (MAR), for endpoints that authenticate using MAB.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The MAC address of the endpoint that authenticates using MAB.</td>
</tr>
<tr>
<td>MAR Comment</td>
<td>(Optional) A descriptive comment about the endpoint.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Edited By</td>
<td>Read-only information. Identifies the method last used to add or edit the MAR entry. Possible methods are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Manually by CounterACT Operator</strong>: Forescout user manually added/edited the MAR entry.</td>
</tr>
<tr>
<td></td>
<td>- <strong>CounterACT Policy</strong>: The 802.1X Update MAR action, whether initiated by policy or manually by user, added/edited the MAR entry.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Imported</strong>: The entry was imported into the MAR.</td>
</tr>
<tr>
<td></td>
<td>Note: The obsolete <strong>Last Edited by</strong> method, <strong>Automatically Learned</strong>, is displayed in existing MAR entries until these entries are next edited or removed from the MAR.</td>
</tr>
<tr>
<td>Authorization</td>
<td>(Optional) The authorization that is imposed on the MAB-authenticated endpoint by the CounterACT RADIUS server in its reply to the NAS device. Possible authorizations include: Deny access, VLAN assignment, and/or one or more attribute-value pair (AVP) assignments.</td>
</tr>
</tbody>
</table>

In the MAR, enable/disable the **Accept MAB authentication for endpoints not defined in this repository** option. By default, this option is disabled. When the checkbox is selected (enabled), endpoints that do not have a MAR entry are permitted to be authenticated by the CounterACT RADIUS server using MAC address bypass (MAB). As needed, impose an authorization on such endpoints by defining pre-admission authorization tab rule(s) with a condition that includes the criterion **MAC Found in MAR** and uses the evaluation instruction **Does not meet this criterion**.

**Creating MAR Entries**

The following options are available for populating the MAR:

- **Automatically Add Entries**
- **Manually Add Entries**
- **Import and Export MAR Entries**

**Automatically Add Entries**

You can create a policy that automatically adds detected endpoints to the MAR or edits existing MAR entries.

**To add MAR entries based on a policy:**

1. Create a new policy or edit an existing policy.
2. Navigate to the Manage > 802.1X Update MAR policy action.
   
   The action lets you designate updates to MAR entries to be applied in one of the following ways:

   a. Only apply the defined information/setting update to new MAR entries.
   b. Apply the defined information/setting update to new and existing MAR entries.
Manually Add Entries
You can manually add endpoints to the MAR.

(Centralized Licensing only) If you do not have a valid Forescout eyeControl (ForeScout CounterACT Control) license, you cannot add entries to the MAC Address Repository.

1. Select Options from the Tools menu. The Options window opens.
2. Navigate to and select the MAC Address Repository folder.
3. In the MAC Address Repository pane, select Add.

4. In the Endpoint MAC Address field, enter the MAC address of an endpoint which authenticates by MAB.
5. The Last Edited By field is automatically populated by the plugin and cannot be edited. See What You See in the Repository for details.
6. (Optional) In the MAR Comment field, provide a descriptive comment about the endpoint.
7. (Optional) In the Authorization section, define the authorization that is imposed on the MAB-authenticated endpoint by the CounterACT RADIUS server in its reply to the NAS device. For details, see Rule Authorization.
8. Select **OK**.

### Import and Export MAR Entries

You can import MAR entries into the MAC Address Repository from a CSV file. See [Guidelines for Creating a CSV File](#).

You can also export MAR entries from the repository to a CSV file. (Exporting MAR entries does not affect existing MAR entries.)

(Centralized Licensing only) If you do not have a valid Forescout eyeControl (ForeScout CounterACT Control) license, you cannot import entries to the MAC Address Repository.

To import MAR entries:

1. Select **Import** on the MAC Address Repository toolbar.

2. Browse to and select the CSV file and select **Import**.

To export MAR entries to a CSV file:

- Do one of the following:
  - Select **Export** from the MAC Address Repository toolbar. Selecting **Export** results in the entire MAR content being exported and, therefore, is the Forescout recommended method to use.
Right-click any MAR entry and select **Export Table**.

Guidelines for Creating a CSV File

Follow these guidelines when creating a CSV file of MAR entries to import:

<table>
<thead>
<tr>
<th>MAR Entry Field</th>
<th>CSV File Column Name</th>
<th>CSV File Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAC Address</strong></td>
<td>dot1x_mac</td>
<td>Required field column Enter a MAC address. Information is displayed in MAR.</td>
</tr>
<tr>
<td></td>
<td>dot1x_auth_method</td>
<td>Required field column Enter the text <strong>bypass</strong>. Information does not display in MAR. By definition, all MAR entries authenticate using MAC authentication bypass (MAB).</td>
</tr>
</tbody>
</table>
| **Authorization** | dot1x_target_access | Optional field column Keep field entry blank. After successfully importing the CSV file into the MAR, add MAR entry authorizations, by doing one of the following activities:  
- In the Console, manually add required MAR entry authorizations. See **Manually Add Entries**.  
- Contact Forescout Customer Support for assistance. Information is displayed in MAR. |
|                 | dot1x_enforce_access | Keep field blank. |
|                 | dot1x_last_assigned_access | Keep field blank. |
### Editing and Removing MAR Entries

Edit a MAR entry by selecting the entry and then selecting **Edit**. The Edit MAR Entry window opens.

Remove one or more MAR entries by selecting the entries and then selecting **Remove**. The selected entries are removed from the MAR.

After you edit or remove entries, select **Apply** to save the modified MAC Address Repository.

> (Centralized Licensing only) If you do not have a valid Forescout eyeControl (ForeScout CounterACT Control) license, you cannot edit entries in the MAC Address Repository.

### Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

**To verify:**

1. Select **Tools > Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

### Testing and Troubleshooting

The section describes the test of the RADIUS Plugin and the 802.1X troubleshooting policy templates.

- **Test Full Plugin Configuration**
- **Troubleshooting Policy Templates**
**Test Full Plugin Configuration**

The full test of the plugin configuration accomplishes the following:

- Verifies that a RADIUS server certificate is correctly defined and provisioned in each CounterACT device.
  - If this test is successful, the `<result>` displayed is:
    
    **RADIUS Plugin certificate test: SUCCEEDED**
  - If the test is not successful, the `<result>` displayed is:
    
    **RADIUS Plugin certificate test: FAILED**

- Tests the functionality of each authentication source with each relevant CounterACT device. For details, see [Test Authentication Source Functionality](#).

It is recommended to perform the full test of the plugin configuration after the following plugin configuration activities are completed:

- The plugin joined each CounterACT device to the Active Directory domain(s), using the credentials previously defined using the Join button
- You have defined and provisioned a valid RADIUS server certificate for each CounterACT device

**To run the test:**

1. In the Console Modules pane, select the **Authentication** module. The plugins, which are installed as part of the Forescout Authentication Module, are listed below the Authentication entry.
2. In the Modules pane, select the **RADIUS** entry from the table listing.
3. Select **Test**.
4. When prompted to confirm that you want to test the RADIUS plugin, select **Yes**.

   The test proceeds, and the **Testing RADIUS Plugin** window opens and displays the test results.
Troubleshooting Policy Templates

The section describes the 802.1X troubleshooting policy templates provided by the plugin. The troubleshooting policy templates are as follows:

- **Troubleshoot Rejected Authentications Policy Template**

It is recommended that you have a basic understanding of Forescout 8.1 policies before working with the templates. Refer to the Forescout Templates and Policy Management chapters of the Forescout Administration Guide.

Troubleshoot Rejected Authentications Policy Template

Use the Troubleshoot Rejected Authentications template to generate a policy that categorizes, by cause, rejected 802.1X authentications.

Endpoints may be rejected by the RADIUS server for any of the following reasons:

- Failure to authenticate endpoint identity (invalid credentials, invalid certificate, no MAR entry)
- Failure in the processing or communication of an authentication-related component, for example, the Active Directory server does not respond.
- Verification of the certificate provided by the endpoint supplicant identifies that this certificate is revoked by the issuing certificate authority.
- Authorization denial (after being authenticated). A denial of access has any one of the following sources:
  - Policy action authorization
  - MAR authorization
− Pre-admission authorization rule

**Prerequisites**

Before you run a policy based on this template:

- It is recommended to run *802.1X Readiness* policies, and that network devices and endpoints were determined ready for 802.1X authentication.
- Verify that the RADIUS Plugin is running, and 802.1X endpoint authentication is operating in the organization's network.
- *(Optional)* To identify rejections caused by authorization denial, verify that one or more sources of authorization denial are defined and operating.

**Create a Troubleshoot Rejected Authentications Policy**

This section describes how to create a policy based on the Troubleshoot Rejected Authentications template.

**To create a policy:**

1. In the Console, select the **Policy** tab.

2. Select **Add**. The Policy Wizard opens.

3. In the navigation tree, select **RADIUS > 802.1X > 802.1X Enforcement** and then select **Troubleshoot Rejected Authentications**.
4. Select **Next**.

![Policy Wizard Step 2 of 4]

5. Define a unique name for the policy you are creating based on this template and enter a description.
   
   - Use a name that clearly reflects what the policy does. Use a descriptive name that identifies what your policy verifies and what actions are taken.
   
   - Ensure that the name identifies whether the policy criterion must be met or not met.
   
   - Make policy names unique. Avoid policies with similar, generic names.

   *Policy names appear in the Policy Manager, the Views pane, Reports, and in other features. Precise names make working with policies and reports more efficient.*

6. Select **Next**. The Scope pane opens. By default, the policy inspects the following range of endpoints: all IP addresses and unknown IP addresses.

![Policy Wizard Step 3 of 4]
7. Select **Next**. The Sub-Rules pane opens and lists the default sub-rules rules of the policy generated by the template. Sub-rules can be modified at this point if required. For details, see **Troubleshoot Rejected Authentications Sub-Rules**.

> It is recommended to maintain both the order and content of the sub-rules provided in the policy.

8. Select **Finish**. The policy is created.

In the policy, do not remove *Unknown IP Addresses* from the policy scope.

**Troubleshoot Rejected Authentications Main Rule**

Forescout-platform-detected endpoints that meet the following criterion match the main rule of this policy:

- Endpoint was rejected by the RADIUS server.

> All other main rule criteria are for the purposes of displaying specific property information about a selected endpoint in the Home view.

**Troubleshoot Rejected Authentications Sub-Rules**

Sub-rules of this policy are used to categorize, by cause, RADIUS server-rejected 802.1X endpoint authentications, including authorization denials (imposed by the RADIUS server after endpoints successfully authenticate). By default, these sub-rules are not defined with policy actions.

> It is recommended to maintain both the order and content of the sub-rules provided in the policy.
Rejected endpoint authentications are inspected against each sub-rule in the order listed to determine their cause, as follows:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1. Denied by Authorization        | Endpoints matching this sub-rule had their authentication accepted by the RADIUS server, however, endpoint access was then denied by the defined authorization imposed by the RADIUS server. A denial of access has any one of the following sources:  
  - Policy action authorization  
  - MAR authorization  
  - Pre-Admission authorization rule |
<p>| 2. Rejected by External RADIUS Server | Endpoints matching this sub-rule had their authentication rejected by the external RADIUS server. When Forescout 8.1 acts as a proxy to an external RADIUS server, the cause of rejected authentications cannot be determined. |
| 3. MAC Bypass Rejected            | Endpoints matching this sub-rule attempted MAC address bypass (MAB) and were rejected by the CounterACT RADIUS server.                                                                                     |
|                                    | <strong>CAUSE:</strong> The endpoint MAC address was not listed in the plugin’s MAR (the warehouse of endpoints that authenticate using MAB).                                                                               |
| 4. Invalid Credentials Supplied   | Endpoints matching this sub-rule had their authentication rejected by the RADIUS server.                                                                                                                      |
|                                    | <strong>CAUSE:</strong> Computer-supplied or user-supplied credentials did not match the credentials in the Active Directory of the domain.                                                                              |
| 5. Domain Controller Detected Error | Endpoints matching this sub-rule had their authentication rejected by the CounterACT RADIUS server.                                                                                                       |
|                                    | <strong>CAUSE:</strong> The domain controller did not provide an adequate response to the RADIUS server.                                                                                                                |
| 6. Certificate Revoked by CRL Verification | Endpoints matching this sub-rule had their authentication rejected by the CounterACT RADIUS server.                                                                                                        |
|                                    | <strong>CAUSE:</strong> Certificate verification by CRL reported that the issuing certificate authority revoked the certificate provided by the endpoint supplicant                                                    |</p>
<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Certificate Revoked by OCSP Verification</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the <em>CounterACT</em> RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>CAUSE</strong>: Certificate verification by the issuing certificate authority, accomplished by OCSP, reported that the certificate provided by the endpoint supplicant is revoked.</td>
</tr>
<tr>
<td>8. Server Certificate Issuer Not Trusted</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the <em>CounterACT</em> RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>CAUSE</strong>: The endpoint supplicant did not trust the certificate authority that issued the RADIUS server's server certificate.</td>
</tr>
<tr>
<td>9. Client Certificate Issuer Not Trusted</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the <em>CounterACT</em> RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>CAUSE</strong>: The <em>CounterACT</em> RADIUS server did not trust the certificate authority that issued the endpoint supplicant's client certificate.</td>
</tr>
<tr>
<td>10. Client Issued TLS Alert</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the <em>CounterACT</em> RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>CAUSE</strong>: The endpoint supplicant stopped the TLS handshake with the RADIUS server. This might indicate that the server certificate is invalid.</td>
</tr>
<tr>
<td>11. Server Issued TLS Alert</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the <em>CounterACT</em> RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>CAUSE</strong>: The RADIUS server stopped the TLS handshake with the endpoint supplicant. This might indicate that the client certificate is invalid.</td>
</tr>
<tr>
<td>12. EAP Negotiation Failure</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the <em>CounterACT</em> RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>CAUSE</strong>: The EAP negotiation between the RADIUS server and the endpoint supplicant stopped for a reason not covered by any of the preceding sub-rules. For example, the two parties did not agree on the EAP method.</td>
</tr>
<tr>
<td>13. Other Rejections</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the <em>CounterACT</em> RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>CAUSE</strong>: The authentication stopped for a reason not matched by any of the preceding sub-rules.</td>
</tr>
</tbody>
</table>
Technical Support

When the plugin test fails, the test results describe the failure. For more information, contact technical support at support@forescout.com. It is recommended to send the test results of the failed plugin test to the Forescout customer support team for review/analysis.

To send test failure output:
1. Log in to the CounterACT device CLI.
2. Run the following commands:
   a. `fstool tech-support debug dot1x --level 6`
   b. `fstool dot1x test normal`
   Test results display in the screen.
3. Copy the test output and paste it into a text file.
4. Send this file to Forescout technical support.

Plugin Properties and Custom Policies

This section provides information about the following plugin topics:

- Properties for Use in Policy Conditions
- Create Custom Policies

Properties for Use in Policy Conditions

Forescout 8.1 policy conditions and properties let you define how Forescout 8.1 detects endpoints authenticating via 802.1X. When adding or editing a policy rule, the main rule, or a sub-rule, you can add and edit policy conditions for the rule. In the navigation pane of the Condition window, the following folders supply the 802.1X properties that are available for use in policy conditions:

- Advanced Properties
- Authentication Decision Properties
- Authentication Details Properties
- Authentication Events Properties
- Authorization Properties
- Client Certificate Properties
- MAR Properties
- NAS Device Properties
- Windows 7 Supplicant Properties
### Advanced Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Accounting Session Id</td>
<td>The Accounting Session Id, RADIUS attribute (44), used on the last accounting request.</td>
</tr>
<tr>
<td>802.1X RADIUS Log Details</td>
<td>The debug log messages of the last, failed authentication.</td>
</tr>
<tr>
<td>802.1X User Login Result</td>
<td>User credentials validation result, according to the ntlm_auth process.</td>
</tr>
</tbody>
</table>

### Authentication Decision Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Authenticating Appliance</td>
<td>The IP address of the appliance performing the authentication.</td>
</tr>
</tbody>
</table>
| 802.1X Last Authentication State - Computer Credentials | The result of the last authentication attempt made by the endpoint using computer credentials.  
  - RADIUS-Accepted – The RADIUS server successfully authenticated the endpoint.  
  - RADIUS-Rejected – The endpoint failed to authenticate with the RADIUS server. |
| 802.1X Last Authentication State - MAC Based | The result of the last authentication attempt made by the endpoint using its MAC address (MAB).  
  - RADIUS-Accepted – The RADIUS server successfully authenticated the endpoint.  
  - RADIUS-Rejected – The endpoint failed to authenticate with the RADIUS server. |
### Property | Description
--- | ---
**802.1X Last Authentication State - User Credentials** | The result of the last authentication attempt made by the endpoint using user credentials.
  - **RADIUS-Accepted** – The RADIUS server successfully authenticated the user.
  - **RADIUS-Rejected** – The user failed to authenticate with the RADIUS server.

**802.1X RADIUS Authentication State** | The result of the last authentication performed by the RADIUS server (Accept or Reject).
Note that the final reply might be different, due to any imposed authorization.

### Authentication Details Properties

| Property | Description |
--- | ---
**802.1X Authenticated Entity** | How an entity was authenticated:
  - **User - Authenticated** using user credentials
  - **Computer - Authenticated** using computer credentials
  *Note:* For computer authentication of a Macintosh endpoint, the plugin always resolves this property as **User**.
  - **MAC - Authenticated** using MAC address bypass (MAB).

**802.1X Authenticating Domain** | The domain that the plugin used for endpoint 802.1X authentication.

**802.1X Authentication Type** | Identifies the selected **EAP Type** in the last authentication. Supported types are:
  - EAP-TLS
  - MAB
  - PEAP
  - PEAP-EAP-TLS

**802.1X Calling Station Id** | Calling-Station-Id, RADIUS attribute (31), used on last authentication request

**802.1X Default Domain** | Per Appliance handling 802.1X authentication, the domain configured for the default authenticating user directory.
This information is defined in the Authentication Source tab of the RADIUS Plugin.

**802.1X Host Name** | The User-Name, RADIUS attribute (1), used in last authentication request, when computer credentials are used to authenticate.

**802.1X Reauthentication Method** | The method used with the last re-authentication of the endpoint. For plugin supported methods, see [Re-Authentication Methods](#).

**802.1X Requested Domain** | The domain that an endpoint requested to use for 802.1X authentication.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.1X Tunneled User Name</strong></td>
<td>The user name used for the inner authentication phase of Protected EAP-MSCHAPv2 and Protected EAP-TLS authentication processes. Inner and outer user names are usually the same. However, when the supplicant's <strong>Identity Privacy</strong> field is configured, the inner user-name (the Tunneled User Name) is the supplicant's true user name.</td>
</tr>
<tr>
<td><strong>802.1X User Name</strong></td>
<td>The User-Name, RADIUS attribute (1), used in last authentication request.</td>
</tr>
</tbody>
</table>

**Authentication Events Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.1X Last Authentication Time</strong></td>
<td>The last time an authentication completed for the endpoint with a <strong>RADIUS Accept</strong> or <strong>RADIUS Reject</strong> message.</td>
</tr>
<tr>
<td><strong>802.1X Last Authorize Action Failure</strong></td>
<td>The last time the RADIUS Authorize action failed.</td>
</tr>
<tr>
<td><strong>802.1X Last Rejected Authentication Time</strong></td>
<td>The last time an authentication completed with <strong>RADIUS-Reject</strong> for this endpoint.</td>
</tr>
<tr>
<td><strong>802.1X Last Successful Authentication Time</strong></td>
<td>The last time an authentication completed with <strong>RADIUS-Accept</strong> for this endpoint.</td>
</tr>
</tbody>
</table>

**Authorization Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.1X Authorization Source</strong></td>
<td>The source of the authorization imposed on the authenticated endpoint. Source can be any one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Policy Action Authorization</td>
</tr>
<tr>
<td></td>
<td>- MAC Address Repository Authorization</td>
</tr>
<tr>
<td></td>
<td>- Pre-Admission Authorization Rule</td>
</tr>
<tr>
<td><strong>802.1X Authorize Action Summary</strong></td>
<td>A summary of the processing decisions involved with applying the RADIUS Authorize action, for example, reported errors, re-authentication handling information, and success/failure reason.</td>
</tr>
<tr>
<td><strong>802.1X RADIUS Imposed Authorization</strong></td>
<td>The most recent authorization imposed by the RADIUS server on the endpoint.</td>
</tr>
<tr>
<td><strong>802.1X Requested Authorize Action</strong></td>
<td>The authorization provided by the most recent RADIUS Authorize action for the RADIUS server to impose on the endpoint.</td>
</tr>
</tbody>
</table>
Client Certificate Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Client Cert Alternate Subject</td>
<td>The alternate subject of the client certificate.</td>
</tr>
<tr>
<td>802.1X Client Cert commonName</td>
<td>The common-name of the client certificate.</td>
</tr>
<tr>
<td>802.1X Client Cert Expiration</td>
<td>The expiration date of the client certificate.</td>
</tr>
<tr>
<td>802.1X Client Cert Issuer</td>
<td>The issuer of the client certificate.</td>
</tr>
<tr>
<td>802.1X Client Cert Serial</td>
<td>The serial number of the client certificate.</td>
</tr>
<tr>
<td>802.1X Client Cert Subject</td>
<td>The subject of the client certificate.</td>
</tr>
</tbody>
</table>

MAR Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X MAR Comment</td>
<td>Descriptive, free text defined in the MAR for this endpoint.</td>
</tr>
<tr>
<td>802.1X MAR Restrict To</td>
<td>The authorization defined in the MAR for this endpoint.</td>
</tr>
</tbody>
</table>

NAS Device Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Called Station ID</td>
<td>The Called-Station-ID, RADIUS attribute (30), used on the last authentication request.</td>
</tr>
<tr>
<td>802.1X Endpoint SSID</td>
<td>The WLAN SSID used in the 802.1X authentication.</td>
</tr>
<tr>
<td>802.1X NAS IP Address</td>
<td>The 802.1X NAS-IP-Address, RADIUS attribute (4), as appears in the RADIUS Request (IPv4 address of the switch or the WiFi AP/Controller).</td>
</tr>
<tr>
<td>802.1X NAS IPv6 Address</td>
<td>The 802.1X NAS-IPv6-Address, RADIUS attribute (95), as appears in the RADIUS Request (IPv6 address of the switch or the WiFi AP/Controller).</td>
</tr>
<tr>
<td>802.1X NAS Port Number</td>
<td>The NAS-port, RADIUS attribute (5), as reported in RADIUS Request. This RADIUS attribute contains the port number of the switch, if available. Wireless access points do not have physical ports. Therefore, a unique association ID is assigned to every mobile station upon a successful association exchange. As a result, for a wireless access point, if the association exchange was completed prior to authentication, the NAS-port attribute contains the association ID, which is a 16-bit, unsigned integer.</td>
</tr>
</tbody>
</table>
### 802.1X NAS Port Type

The NAS-port-type, RADIUS attribute (61), as appears in RADIUS Request. Supported port types are:

- Ethernet LAN
- Virtual
- Wireless LAN

### Windows 7 Supplicant Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatically use Windows logon, password, and domain</strong></td>
<td>Automatically use Windows login, password, and domain.</td>
</tr>
<tr>
<td><strong>Do not prompt user to authorize new servers or trusted certification authorities</strong></td>
<td>Do not prompt users to authorize new servers or trusted certification authorities.</td>
</tr>
</tbody>
</table>
| **Enable Fast Reconnect**                                    | Valid values: True, False. Provides the ability to reconnect to wireless access point by using cached session keys, which allows for:  
<p>|                                                              | ▪ Quick roaming between wireless access points                              |
| <strong>Enable IEEE 802.1X authentication</strong>                        | Enable IEEE 802.1X authentication.                                          |
| <strong>Encryption type</strong>                                          | Supported encryption types are:                                             |
|                                                              | ▪ AES                                                                        |
|                                                              | ▪ TKIP                                                                       |
|                                                              | ▪ WEP                                                                        |
|                                                              | ▪ None                                                                       |
| <strong>Fallback to unauthorized network access</strong>                  | Fall back to unauthorized network access.                                   |
| <strong>Network authentication method</strong>                            | The authentication method used to connect to the network.                   |
| <strong>Remember user credentials for this connection for each logon</strong> | Remember the user credentials for this connection for future log ins.       |
| <strong>Security Type</strong>                                            | Supported security types are:                                              |
|                                                              | ▪ 802.1X                                                                     |
|                                                              | ▪ No authentication (Open)                                                   |
|                                                              | ▪ Shared                                                                     |
|                                                              | ▪ WPA-Enterprise                                                             |
|                                                              | ▪ WPA-Personal                                                               |
|                                                              | ▪ WPA-2 Enterprise                                                           |
|                                                              | ▪ WPA-2 Personal                                                             |
| <strong>Use simple certificate selection</strong>                         | Use simple certificate selection.                                           |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate server certificate</td>
<td>Validate server certificate.</td>
</tr>
</tbody>
</table>

Create Custom Policies

Although it is recommended to tailor the policies you create using the 802.1X policy templates, you might decide to create a custom policy, to address issues not handled by the policies generated using the 802.1X policy templates. Custom policy tools provide you with an extensive range of options for detecting and handling endpoints.

This section describes the policy properties that are available when the RADIUS Plugin is installed. For a description of the available actions, see Actions.

To create a policy:

1. Log in to the Forescout Console.
2. Select the Policy icon from the Console toolbar.
3. Create or edit a policy. For information about working with policies, select Help from the policy wizard.

Policy Scope

When defining a policy scope where pre-connect is applied, a best practice is to select the Unknown IP addresses in the IP Address Range dialog box, in addition to using any of the other IP address options. This option lets you detect and handle endpoints based on their MAC address when an IP address is not yet available to Forescout 8.1.
The Unknown IP addresses option is available with Forescout. Refer to Forescout 8.1 Online Help for more information.

**Actions**

The RADIUS Plugin provides the following actions for application on detected endpoints.

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.

- **RADIUS Authorize Action**
- **802.1X Update MAR Action**

**RADIUS Authorize Action**

Use the RADIUS Authorize action to define the authorization to be imposed on authenticated endpoints by the CounterACT RADIUS server.

An applied RADIUS Authorize action can be canceled. When canceling this action, the RADIUS Plugin removes the imposed authorization from the CounterACT RADIUS server's cache.
When the CounterACT RADIUS server must impose authorization on managed, authenticated endpoints, it uses the authorization provided from the following hierarchy of sources:

1. Policy action authorization – If available, first preference.
2. MAR authorization – If available, second preference.
3. Pre-admission authorization rule – Third preference. The CounterACT RADIUS server evaluates pre-admission authorization rules when no other source (no policy action, no MAC Address Repository) provides the authorization to impose on an authenticated endpoint; for example, prior to an endpoint being admitted to an organization’s network.

When none of the above sources provide the CounterACT RADIUS server with the necessary authorization, the CounterACT RADIUS server does not include any authorization in its reply to the NAS device. In this case, the NAS device determines the authorization to impose on the endpoint.

Policies you create using the Endpoint Authorization Policy Template or the Centralized Web Authentication Policy Template include sub-rules that apply the RADIUS Authorize action to evaluated endpoints found to match the sub-rule. It is recommended to tailor the authorization defined in each policy sub-rule RADIUS Authorize action, to address your organization’s unique authorization needs.

To define authorization in the action:

1. When defining the action in a policy, do the following:
   a. In the Console Policy tab, select a policy and select Edit.
   b. Select a main rule or a sub-rule and select Edit.
   c. In the Actions pane of the rule, select Add. The Action window opens.
   d. Navigate to Actions > Restrict and select the RADIUS Authorize action. The action’s Parameters tab opens.
   e. Continue with step 3.

2. When manually invoking the action on detected endpoints, do the following:
   a. In the Detections pane of the Home view, right-click one or more selected endpoint entries.
   b. In the displayed menu, navigate to Restrict and select the RADIUS Authorize action. The action’s Parameters tab opens.
   c. Continue with step 3.

3. In the Parameters tab, define any of the following authorization options:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny Access</td>
<td>For details about defining authorization options, see Rule Authorization.</td>
</tr>
<tr>
<td>VLAN</td>
<td></td>
</tr>
<tr>
<td>Attribute-Value Pair</td>
<td></td>
</tr>
</tbody>
</table>
4. When defining the action in a policy, do the following:
   a. Select OK.
   b. Select Apply to save the updated plugin configuration.

Canceling the RADIUS Authorize Action

Canceling the RADIUS Authorize action removes the authorization applied by the action and allows authorization to be applied as provided from the hierarchy of Forescout authorization sources.

Cancellation of the authorization imposed on an endpoint only takes effect at the next authentication of the targeted endpoint.

Action cancellation occurs:

- Following policy evaluation. For endpoints that no longer match a policy sub-rule and the action is defined for that sub-rule.
- When the Forescout user manually cancels it.
- When the settings of this action are changed, and the action is re-applied on matching endpoints.

802.1X Update MAR Action

Use the 802.1X Update MAR action to add new entries to the MAC Address Repository (MAR) or to edit existing entries in the MAR. As is standard for all Forescout actions, this action can be incorporated in a policy and can be manually invoked on detected endpoints. Defining a MAR entry for an endpoint designates that endpoint for authentication by MAC address bypass (MAB).

This action lets you designate updates to MAR entries to be applied in one of the following ways:

- Only apply the defined information/setting update to new MAR entries.
• Apply the defined information/setting update to both existing and new MAR entries.

MAR entries contain the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The MAC address of the endpoint, which authenticates using MAB.</td>
</tr>
<tr>
<td>MAR Comment</td>
<td>(Optional) Descriptive comment about the endpoint.</td>
</tr>
<tr>
<td>Last Edited By</td>
<td>Read-only information. Identifies the method last used to add or edit the MAR entry. Possible methods are:</td>
</tr>
<tr>
<td></td>
<td>• Manually by CounterACT Operator: Forescout user manually added/edited the MAR entry.</td>
</tr>
<tr>
<td></td>
<td>• CounterACT Policy: The 802.1X Update MAR action, whether initiated by policy or manually by user, added/edited the MAR entry</td>
</tr>
<tr>
<td></td>
<td>• Imported: The entry was imported into the MAR.</td>
</tr>
<tr>
<td>Authorization</td>
<td>(Optional) The authorization imposed on the MAB-authenticated endpoint by the CounterACT RADIUS server in its reply to the NAS device. When a MAC address entry does not have an authorization defined in the repository, the CounterACT RADIUS server evaluates the pre-admission authorization rules to authorize the MAB-authenticated endpoint. For authenticated endpoints not matching any of the pre-admission authorization rules, the NAS device determines the authorization to impose on the endpoint.</td>
</tr>
</tbody>
</table>

To define the Update MAR action:

1. When defining the action in a policy, do the following:
   a. In the Console Policy tab, select a policy and select Edit.
   b. Select a main rule or a sub-rule and select Edit.
   c. In the Actions pane of the rule, select Add. The Action window opens.
   d. Navigate to Actions > Manage and select the 802.1X Update MAR action. The action's Parameters tab opens.
   e. Continue with step 3.

2. When manually invoking the action on detected endpoints, do the following:
   a. In the Detections pane of the Home view, right-click one or more selected endpoint entries.
   b. In the displayed menu, navigate to Manage and select the 802.1X Update MAR action. The action's Parameters tab opens.
   c. Continue with step 3.

3. In the Parameters tab, define the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny Access</td>
<td>For details about defining authorization options, see Rule Authorization.</td>
</tr>
<tr>
<td>VLAN</td>
<td></td>
</tr>
<tr>
<td>Attribute-Value Pair</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Apply authorization settings to new entries only** | Selecting this option instructs the CounterACT RADIUS server to impose the action's defined authorization only on MAR entries being added.  
If this option is not selected, the action’s defined authorization is imposed on both new and existing MAR entries. |
| **MAR Comment**                                | A descriptive comment about the endpoint.                                                                                                                                                          |
| **Apply comment to new entries only**          | Selecting this option instructs the plugin to record the **MAR Comment** only in MAR entries being added.  
If this option is not selected, the **MAR Comment** is recorded in both new and existing MAR entries.                                       |
| **Initiate endpoint re-authentication**         | Selecting this option instructs the CounterACT RADIUS server to trigger the re-authentication (force DHCP renew) of the MAR entry (the endpoint), whether added or edited.  
Use this option alone or in combination with other information/setting updates, defined in the action's Parameters tab. When used in combination with other information/setting updates, re-authentication of an endpoint is only initiated following successful update MAR entry processing. |
4. When defining the action in a policy, do the following:
   a. Select **OK**.
   b. Select **Apply** to save the updated plugin configuration.

**Use Cases**

This section presents information about the following plugin use cases:

- **Categorize Endpoint Authorizations**
- **Monitor Successful Authentications and Apply Authorizations**
- **Corporate Wired and Wireless Authentication**
- **Centralized Web Authentication**
- **Edu-Roam**
- **MAC Address Bypass**
- **Network Device Administration**

**Categorize Endpoint Authorizations**

Read this section if you want to:

- Categorize authenticated endpoints according to their Forescout source of authorization.

Possible Forescout sources providing authorization are:

- Policy Action Authorization
- MAC Address Repository (MAR) Authorization
- Pre-Admission Authorization Rule

See Authentication-Authorization Processing Flow. In the event of authenticated endpoints not having their authorization provided by any of the above sources, the NAS device determines the authorization to impose on the endpoint.

**Authorization Source Policy Template**

Use the **Authorization Source** template to generate a policy to accomplish the following objective:

- Categorization of authenticated endpoints.

It is recommended to tailor the policy to address your organization's unique authorization needs.

**Prerequisites**

Before you run a policy based on this template:

- It is recommended to run 802.1X Readiness policies, and that network devices and endpoints were determined ready for 802.1X authentication.
• Verify that the RADIUS Plugin is running, and 802.1X endpoint authentication is operating in the organization's network.
• Verify that active 802.1X Endpoint Authorization policies have their sub-rule actions enabled.

Create an Authorization Source Policy
This section describes how to create a policy based on the Authorization Source template.

To run the template:
1. In the Console, select the Policy tab.
3. In the navigation tree, select RADIUS > 802.1X > 802.1X Enforcement and then select Authorization Source.
4. Select Next.
5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Use a name that clearly reflects what the policy does. Use a descriptive name that identifies what your policy verifies and what actions are taken.
   - Ensure that the name identifies whether the policy criterion must be met or not met.
   - Make policy names unique. Avoid policies with similar, generic names.

Policy names appear in the Policy Manager, the Views pane, Reports, and in other features. Precise names make working with policies and reports more efficient.

6. Select Next. The Scope pane and the IP Address Range dialog box open.

7. Use the IP Address Range dialog box to define which endpoints are inspected.

The following options are available:

- All IPs: Include all IP addresses in the Internal Network.
- Segment: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box and select Segments from the Scope pane.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

You can filter the range by including only certain policy groups and/or excluding devices or users that should be ignored when using a policy.

8. Select **Next**. The Sub-Rules pane opens and lists the default sub-rules of the policy generated by the template. Sub-rules can be modified at this point if required. For details, see Authorization Source Sub-Rules.

9. Select **Finish**. The policy is created.

**Authorization Source Main Rule**

Forescout-platform-detected endpoints that meet the following criterion match the main rule of this policy:

- Endpoint authentication state is accepted by the RADIUS server

**Authorization Source Sub-Rules**

Sub-rules of this policy are used to:

- Categorize the Forescout source of endpoint authorization. Authorization is imposed on successfully authenticated endpoints.

By default, policy sub-rules do not include an action.
Endpoint authorizations are inspected against each sub-rule in the order listed, as follows:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Policy</td>
<td>Endpoints matching this sub-rule had their authorization supplied by the RADIUS Authorize action; application of this action result from policy evaluation or be manually initiated by the Forescout user.</td>
</tr>
</tbody>
</table>
| 2. MAR          | Endpoints matching this sub-rule had their authorization supplied by a MAR entry. Endpoint MAC addresses listed in the MAR authenticate using MAC address bypass (MAB). If the MAR entry of the endpoint has a defined authorization, that authorization that is imposed on the endpoint. **Note:** When a MAC entry in the MAR does not have a defined authorization, the CounterACT RADIUS server evaluates:  
  ▪ The pre-admission authorization rules to authorize the MAB-authenticated endpoint.  
  ▪ For authenticated endpoints not matching any of the pre-admission authorization rules, the NAS device determines the authorization to impose on the endpoint. |
| 3. Pre-admission other rules | Endpoints matching this sub-rule had their authorization supplied by a defined pre-admission authorization rule that is assigned any rule priority 3 and greater. **Note:** For authenticated endpoints not matching any of the pre-admission authorization rules, the NAS device determines the authorization to impose on the endpoint. |
| 4. NAS          | Endpoints matching this sub-rule did not match any of the preceding sub-rules. The NAS device determined the authorization to impose on the endpoint and not any Forescout source (not policy action, not MAR, not any pre-admission authorization rule). |

**Monitor Successful Authentications and Apply Authorizations**

Read this section if you want to:

- Categorize successful authentications according to the method used to authenticate the endpoint. For example, user authentication, computer authentication, certificate authentication, MAC address bypass (MAB) authentication.

- Apply authorization restrictions according to endpoint authentication status.
Endpoint Authorization Policy Template

Use the Endpoint Authorization template to generate a policy to accomplish the following objectives:

- Categorization of successful authentications according to the method used to authenticate the endpoint
- Application of authorization restrictions according to endpoint authentication status. Initially, you can choose not to limit the network access of successful authentications (policy sub-rule actions disabled by default). As 802.1X authentication becomes fully operational in the network, you can choose to limit the network access of successful authentications (policy sub-rule actions enabled).

It is recommended to tailor the policy you create, using the Endpoint Authorization template to address your organization’s unique authorization needs.

Prerequisites

Before you run a policy based on this template:

- It is recommended to run 802.1X Readiness policies, and that network devices and endpoints were determined ready for 802.1X authentication.
- Verify that the RADIUS Plugin is running, and 802.1X endpoint authentication is operating in the organization’s network.

Create an Endpoint Authorization Policy

This section describes how to create a policy based on the Endpoint Authorization template.

To create a policy:

1. In the Console, select the Policy tab.


3. In the navigation tree, select RADIUS > 802.1X > 802.1X Enforcement and then select Endpoint Authorization.
4. Select **Next**.

5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Use a name that clearly reflects what the policy does. Use a descriptive name that identifies what your policy verifies and what actions are taken.
   - Ensure that the name identifies whether the policy criterion must be met or not met.
   - Make policy names unique. Avoid policies with similar, generic names.

   *Policy names appear in the Policy Manager, the Views pane, Reports, and in other features. Precise names make working with policies and reports more efficient.*
6. Select **Next**. The Endpoint Authentication Methods pane opens.

The Endpoint Authentication Methods pane lets you define the endpoint authentication methods to be included as sub-rule criteria in the generated policy. These sub-rules categorize successful endpoint authentications according to their authentication method.

7. Select the endpoint authentication methods that the policy uses to categorize successful endpoint authentications. The following options are available:

- **Distinguish between computer/machine and user**: Categorize successful authentications accomplished using computer/machine-provided information or user-provided information.

- **Distinguish between certificate and credentials**: Categorize successful authentications accomplished using a certificate or credentials.

- **Distinguish MAC Address Bypass**: Categorize successful authentications accomplished based only on the endpoint MAC address.

Not selecting any endpoint authentication method is valid. When no authentication methods are selected, the policy identifies successful authentications (accepted by the RADIUS server) but does not categorize them according to the method used to authenticate the endpoint.

8. Select **Next**. The Sub-Rules pane opens and lists the default sub-rules of the policy generated by the template. Sub-rules can be modified at this point if required. For details, see [Endpoint Authorization Sub-Rules](#).

9. Select **Finish**. The policy is created.

By default, the policy inspects the following range of endpoints: all IP addresses and unknown IP addresses. In the policy, do not remove **Unknown IP Addresses** from the policy scope.
**Endpoint Authorization Main Rule**

Forescout-platform-detected endpoints that meet the following criterion match the main rule of this policy:

- Endpoint authentication state is accepted by the RADIUS server

**Endpoint Authorization Sub-Rules**

Sub-rules of this policy are used to:

- Categorize successful authentications according to the method used to authenticate the endpoint (when endpoint authentication methods are selected for the policy).

- Apply network access authorization to the endpoints, which is accomplished by applying policy sub-rule action(s). By default, these sub-rule action(s) are disabled.

Endpoint authentications are inspected against each sub-rule in the order listed, as follows:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. MAC Bypass</strong></td>
<td>Endpoints matching this sub-rule authenticated using only their MAC address, provided that these endpoint MAC addresses are listed in the MAC Address Repository (MAR) of the RADIUS Plugin. The MAR is the plugin’s warehouse of endpoints that authenticate using MAC address bypass (MAB). If the RADIUS Authorize action of this sub-rule is enabled, the authorization defined in this action is imposed on matching endpoints. Edit the sub-rule action and review the defined authorization provided by the policy template.</td>
</tr>
<tr>
<td>Sub-Rule Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 2. Accepted by Computer Certificate | Endpoints matching this sub-rule had their authentication accepted by the RADIUS server given the following conditions:  
  - A machine certificate was presented by the endpoint.  
  - The network authentication method of the endpoint supplicant was EAP-TLS.  
If the RADIUS Authorize action of this sub-rule is enabled, the authorization defined in this action is imposed on matching endpoints. Edit the sub-rule action and review the defined authorization. |
| 3. Accepted by a Certificate     | Endpoints matching this sub-rule had their authentication accepted by the RADIUS server given the following conditions:  
  - A client certificate (issued to the machine or to the user) was presented by the endpoint.  
  - The network authentication method of the endpoint supplicant was EAP-TLS.  
If the RADIUS Authorize action of this sub-rule is enabled, the authorization defined in this action is imposed on matching endpoints. Edit the sub-rule action and review the defined authorization.  
See the known limitation when using this method as described under LDAP group on page 42. |
| 4. Accepted by Computer Authentication | Endpoints matching this sub-rule had their authentication accepted by the RADIUS server given the following condition:  
  - Computer-supplied credentials or a machine certificate was used to authenticate the endpoint.  
If the RADIUS Authorize action of this sub-rule is enabled, the authorization defined in this action is imposed on matching endpoints. Edit the sub-rule action and review the defined authorization. |
| 5. Accepted                      | Endpoints matching this sub-rule had their authentication accepted by the RADIUS server and used an authentication method not detected by any previous sub-rule.  
If the RADIUS Authorize action of this sub-rule is enabled, the authorization defined in this action is imposed on matching endpoints. Edit the sub-rule action and review the defined authorization. |

The authorization options that can be defined in the **RADIUS Authorize** action are:

- Deny Access only
- VLAN Assignment only
- VLAN Assignment and one or more attribute-value pair (AVP) assignments
- One or more attribute-value pair (AVP) assignments only
It is recommended to tailor the authorization defined in each sub-rule action of the policy you created using the Endpoint Authorization template, to address your organization's unique authorization needs. For information about defining authorization in the action, see Actions.

**Corporate Wired and Wireless Authentication**

In order to work with the 802.1X solution to handle both wired and wireless corporate endpoints, it is recommended to verify that all aspects of your organization's IT environment are properly configured before enforcing access control. Plugin deployment/configuration might vary depending on the use case scenarios you want to address using the RADIUS Plugin. For details, see Environment Readiness.

The RADIUS Plugin can be configured to interoperate with any of the following authentication sources:

- **Single Domain Authentication**: A single user directory domain
- **Multi-Domain Authentication**: Multiple user directory domains
- **CounterACT RADIUS Server as a Proxy**: External RADIUS server(s)

**Single Domain Authentication**

When the RADIUS Plugin (the CounterACT RADIUS server) must interoperate with a single user directory domain, perform the following configuration tasks in the plugin's Authentication Sources tab:

1. Add an organizational domain as the authentication source; the available domains are configured in the User Directory Plugin.
   
   The entry's **Domains** column is populated with the local authentication source(s) (Microsoft Active Directory) as configured in the User Directory Plugin.

2. In the entry's **Domains** column, set the local authentication source to be both the **Default Source** and the **Null Domain** handler. Doing so ensures that the CounterACT RADIUS server attempts to authenticate all RADIUS access requests against this source. RADIUS access requests can include any of the following:
   
   - **User Authentication**
     - Child domain
     - Null domain
     - Unknown domain
   
   - **Machine Authentication**
     - Child domain
     - Null domain
     - Unknown domain

For details, see Configure Authentication Sources.
Multi-Domain Authentication

When the RADIUS Plugin (the CounterACT RADIUS server) must interoperate with multiple user directory domains, perform the following configuration tasks in the plugin's Authentication Sources tab:

- Add organizational domains as authentication sources; the available domains are configured in the User Directory Plugin.
- Each entry's Domains column is populated with the local authentication source(s) (Microsoft Active Directory) as configured in the User Directory Plugin.
- (Optional) In one of the entry's Domains column, set the local authentication source to be the Default Source. Doing so instructs the CounterACT RADIUS server to attempt authentication against this source for RADIUS access requests that contain an unknown domain.
- (Optional) In one of the entry's Domains column, set the local authentication source to be the Null Domain handler. Doing so instructs the CounterACT RADIUS server to attempt authentication against this source for RADIUS access requests that do not contain a domain.

For details, see Configure Authentication Sources.

Pre-Admission Authorization in a Multi-Domain Environment

This section provides an example of the pre-admission authorization rules that a Forescout user might configure when the RADIUS Plugin (the CounterACT RADIUS server) operates in a multi-domain environment. For details, see Configure Pre-Admission Authorization.

In this example, two Authentication Sources are defined in Forescout:

- The source named FSD contains the following domains:
  - forescout.com
  - alias1
  - child2
- The source named PM_DC contains the following domains:
  - Pm.lab.forescout.com
  - Eddie
  - NULL Domain
The following authorization rules are defined:

- Assign to VLAN 35 (authorization) the authenticated endpoint of users who are members of the PM group in authentication source FSD.
• Assign to VLAN 36 (authorization) the authenticated endpoint of users who are members of the PM group in authentication source PM_DC.

![Add Pre Admission Authorization Rule](image1)

• Authenticate the endpoints of users with no domain against domain PM_DC and assign the authenticated endpoints to VLAN 40 (authorization).

The regular expression ^[^\@\\]*$ is used to evaluate the User-Name attribute. This ensures that user-Name does not contain the @ (ampersand) character and does not contain the \ (backslash) character.

![Add Pre-Admission Criterion](image2)
The result of applying these rules is displayed in the Pre-Admission Authorization tab.

CounterACT RADIUS Server as a Proxy

When the RADIUS Plugin (the CounterACT RADIUS server) functions as a proxy to an external RADIUS server, perform the following configuration tasks in the plugin’s Authentication Sources tab:

- Add the external RADIUS server as the authentication source; the available external RADIUS servers are configured in the User Directory Plugin.
If you want the CounterACT RADIUS server to proxy all RADIUS access requests to the external RADIUS server authentication source, set the external RADIUS server to be the **Default Source** and the **Null Domain** handler.

Endpoint authorization provided by pre-admission authorization rule or by Forescout 8.1 policies (the RADIUS Authorize action) always replaces an external RADIUS server-provided endpoint authorization.

### Centralized Web Authentication

Centralized web authentication is used to accomplish redirection of guest endpoints for the purposes of managing these guests, who have requested access to your organization’s network (guests, whose network access is approved, can browse the network and possibly use other network resources). Forescout centralized web authentication combines the use of MAC authentication, provided by the RADIUS Plugin, and Forescout 8.1 policy actions to authenticate endpoints.

Forescout centralized web authentication delivers enhanced Forescout guest management responsiveness. This enhanced Forescout guest management responsiveness is provided by the RADIUS Plugin.

> As of RADIUS Plugin version 4.2.0 (previously the 802.1X Plugin), IP-MAC visibility is provided only by the plugin.

Deploy Forescout centralized web authentication by performing the following tasks:

- Enable MAC Address Bypass
- Configure Pre-Admission Authorization Rule
- Centralized Web Authentication Policy Template

### Enable MAC Address Bypass

In the MAR, enable the **Accept MAB authentication for endpoints not defined in this repository** option. Selecting this option instructs the RADIUS Plugin to use MAC address bypass (MAB) to authenticate MAC addresses, which are received in RADIUS requests that are not listed in the MAR. For details, see Configure MAC Access Bypass.

### Configure Pre-Admission Authorization Rule

In the Pre-Admission Authorization tab, add a rule containing the following rule condition that the CounterACT RADIUS server uses to evaluate authenticated endpoints for a match:

- Criterion name (endpoint attribute): **SSID**
- Criterion value (attribute value): `<Guest SSID Name>`

In the Pre-Admission Authorization tab, assign this rule **Rule Priority 1**. For details, see Configure Pre-Admission Authorization.
In addition, define the following *rule authorization* (attribute-value pair assignments) that the CounterACT RADIUS server imposes on authenticated endpoints found to match the *rule condition*:

- Aruba Attribute-Value Pair for Rule Authorization
- Cisco Attribute-Value Pairs for Rule Authorization
- HPE Attribute-Value Pairs for Rule Authorization
- Meraki Attribute-Value Pair for Rule Authorization
- Meraki Management Configuration

### Aruba Attribute-Value Pair for Rule Authorization

The following table presents the Aruba attribute-value (A-V) pair to use in defining the rule authorization.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba</td>
<td>Aruba-User-Role</td>
<td>Enter the user role name defined in the wireless controller.</td>
</tr>
</tbody>
</table>

### Cisco Attribute-Value Pairs for Rule Authorization

The following table presents the Cisco attribute-value (A-V) pairs to use in defining the rule authorization. As necessary, modify these A-V pairs to use the A-V pairs of other supported vendors.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>1st: Cisco-AVPair</td>
<td>url-redirect-acl= Enter the ACL name that is configured on the WLAN device.</td>
</tr>
<tr>
<td></td>
<td>2nd: Cisco-AVPair</td>
<td>url-redirect= http://${appliance_address}/captiveredirect/a?t=${client_token} During expression evaluation, {appliance_address} is dynamically replaced with the FQDN of the CounterACT Appliance. This dynamic replacement requires that the Attempt to redirect using DNS name option be enabled on the Appliance (Options &gt; NAC &gt; HTTP Redirection &gt; HTTP Redirection Settings).</td>
</tr>
</tbody>
</table>

### HPE Attribute-Value Pairs for Rule Authorization

The following table presents the HPE attribute-value (A-V) pair to use in defining the rule authorization.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE</td>
<td>HPE-User-Role</td>
<td>Enter the user role name defined in the wireless controller.</td>
</tr>
</tbody>
</table>
### Meraki Attribute-Value Pair for Rule Authorization

The following table presents the Meraki attribute-value (A-V) pair to use in defining the rule authorization. Modify these A-V pairs to use the A-V pairs of other supported vendors, as required.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meraki</td>
<td>Cisco-AVPair</td>
<td>url-redirect= http://${appliance_address}/captiveredirect/a?t=${client_token}</td>
</tr>
</tbody>
</table>

During expression evaluation, \{appliance_address\} is dynamically replaced with the FQDN of the CounterACT Appliance. This dynamic replacement requires that the option **Apply to redirect using DNS name** is enabled on the Appliance (Options > NAC > HTTP Redirection > HTTP Redirection Settings).

### Meraki Management Configuration

When configuring CWA on the Meraki management platform, make sure that the following guidelines are addressed:

- Make sure that the CoA re-authentication method is enabled.
- When the managing Appliance is not the authenticating Appliance, define the managing Appliance’s IP address in the **Walled Garden** field. Doing so enables the configured network device to communicate with the managing Appliance, in addition to communicating with the authenticating Appliance.
  - By default, the network device is allowed to communicate with the configured, authenticating RADIUS servers.
  - By default, the network device is allowed to communicate with the DNS and DHCP servers.

For the definition of the terms managing Appliance and authenticating Appliance, see **Plugin Redundancy and Failover**.

### Centralized Web Authentication Policy Template

Use the Centralized Web Authentication template to generate a policy to accomplish the following objective:

- Manage guest/corporate users network access lifecycle

It is recommended to tailor the policy you create, using the Centralized Web Authentication template to address your organization’s unique guest redirection/authentication needs.

### Prerequisites

Before you run a policy based on this template, make sure to perform the following tasks:

- **Enable MAC Address Bypass**
- **Configure Pre-Admission Authorization Rule**
Create a Centralized Web Authentication Policy

This section describes how to create a policy based on the Centralized Web Authentication template.

To create a policy:

1. In the Console, select the Policy tab.


3. In the navigation tree, select RADIUS and then select Centralized Web Authentication.

4. Select Next.
5. Define a unique name for the policy you are creating based on this template and enter a description.
   - Use a name that clearly reflects what the policy does. Use a descriptive name that identifies what your policy verifies and what actions are taken.
   - Ensure that the name identifies whether the policy criterion must be met or not met.
   - Make policy names unique. Avoid policies with similar, generic names.

   *Policy names appear in the Policy Manager, the Views pane, Reports and in other features. Precise names make working with policies and reports more efficient.*

6. Select **Next**. The Scope pane and the IP Address Range dialog box open.

7. Use the IP Address Range dialog box to define which endpoints are inspected.

   The following options are available:
   - **All IPs**: Include all IP addresses in the Internal Network.
− **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box and select **Segments** from the Scope pane.

− **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

You can filter the range by including only policy groups and/or excluding devices or users that should be ignored when using a policy.

> When defining the policy scope, a best practice is to select the **Unknown IP addresses** option in the IP Address Range dialog box. This option lets you detect and handle endpoints based on their MAC address when an IP address is not yet available to Forescout 8.1.

8. In the Scope pane, select **Add** to re-open the IP Address Range dialog box and specify an additional IP address option.

9. Select **Next**. The Main Rule pane opens.

10. Select **Next**. The Sub-Rules pane opens and lists the default sub-rules of the policy generated by the template. Sub-rules can be modified at this point if required. For details, see [Centralized Web Authentication Sub-Rules](#). In addition, define the following **rule authorization** (attribute-value pair assignments) that the CounterACT RADIUS server imposes on authenticated endpoints found to match the **rule condition**Select **Finish**. The policy is created.

**Centralized Web Authentication Main Rule**

Forescout 8.1-detected endpoints that meet the following criterion match the main rule of this policy:

- Endpoint is attached to a WLAN device SSID containing the value `<SSID Name>`
1. In the Condition pane of the Main Rule pane, select the criterion **802.1X Endpoint SSID - Contains <Enter Your SSID>**.

2. Select Edit. The Condition window opens and displays the fields for configuring the selected condition **802.1X Endpoint SSID**.

3. Replace the text **<Enter Your SSID>** with the name of the SSID to which endpoints attach when initiating access to your organization’s network.

**Centralized Web Authentication Sub-Rules**

Sub-rules of this policy are used to further evaluate those endpoints matching the policy main rule. By default, each policy sub-rule includes an enabled action to be applied on matching endpoints.
Endpoints matching the policy main rule are inspected against each sub-rule in the order listed, as follows:

<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **1. Signed In as Corporate User** | Endpoints matching this sub-rule meet all of the following conditions:  
  - Within the last `<configurable number of>` days, the HTTP Login action accepted the user's login to the organization's network and authenticated the endpoint as an organization member  
  - The most recent authorization imposed on the endpoint by the CounterACT RADIUS server was **NOT** redirection of the endpoint to Forescout captive portal for handling.  
Forescout applies the RADIUS Authorize action on endpoints matching this sub-rule. For details, see **Actions**. |
| **2. Signed In as Guest** | Endpoints matching this sub-rule meet all of the following conditions:  
  - Within the last `<configurable number of>` days, the HTTP Login action accepted the user's login to the organization's network and authenticated the endpoint as a guest  
  - The most recent authorization imposed on the endpoint by the CounterACT RADIUS server was **NOT** redirection of the endpoint to Forescout captive portal for handling.  
Forescout applies the RADIUS Authorize action on endpoints matching this sub-rule. For details, see **Actions**. |
3. Signed In - Pending Authorization

Endpoints matching this sub-rule meet the following condition:

- Within the last <configurable number of> days, the HTTP Login action accepted the user's login to the organization's network and authenticated the endpoint as a member of the corporate organization or as a guest.

The matching endpoint has authenticated, but the CounterACT RADIUS server has not imposed any authorization on it.

Forescout 8.1 applies the RADIUS Authorize action on endpoints matching this sub-rule. For details, see Actions.

4. Obsolete Log In

Endpoints matching this sub-rule meet the following condition:

- The most recent authorization imposed on the endpoint by the CounterACT RADIUS server was NOT redirection of the endpoint to Forescout captive portal for handling.

Matching endpoints are no longer logged in to the organization's network as a member of the corporate organization or as a guest. These endpoints must undergo centralized web authentication.

Forescout 8.1 applies the RADIUS Authorize action on endpoints matching this sub-rule to redirect these users to the Forescout captive portal. For details, see Actions. By default, the policy template generates a policy that uses Cisco A-V pairs. As necessary, modify these A-V pairs to use the A-V pairs of other supported vendors.

5. Pending Log In

Endpoints matching this sub-rule did not match any of the preceding sub-rules.

Forescout 8.1 applies the HTTP Login action on endpoints matching this sub-rule following their redirection to allow these users to log in again to the organization's network.

For more information about the HTTP Login action, refer to the User Directory Plugin Configuration Guide. See Additional Forescout Documentation for information on how to access this guide.

Edu-Roam

Edu-Roam (education roaming) is a world-wide roaming access service developed for the international research and education community. The service allows students, researchers, and staff from participating institutions and cities to obtain Internet connectivity across town, campus, and when visiting other participating institutions.
When the CounterACT RADIUS server must proxy to an external RADIUS server in support of an Edu-Roam deployment, use the following RADIUS Plugin configuration guidelines:

**Authentication Sources**

In the Authentication Sources tab, select and configure the relevant entries as follows:

- Set the RADIUS server, designated to serve Edu-Roam endpoint authentication, to be the **Default Source**. All RADIUS access requests with an implicit unknown domain are handled by this authentication source.

- All other authentication sources’ **Domains** column is populated with the local authentication source(s) (Microsoft Active Directory) as configured in the User Directory Plugin.
  - (Optional) Set one of these other authentication sources to be the **NULL Domain** handler.

For details about authentication source domain assignments, see Configure Authentication Sources.

**Pre-Admission Authorization**

In the Pre-Admission Authorization tab, define the following pre-admission authorization rules:

- Authorize roaming users, on **SSID edu-roam**, to access the organization’s network.
  
  For example, only during specific hours, from 8 a.m. - 7 p.m. Monday - Friday, and assign these endpoints to **VLAN 10**.
• Authorize local users, on **SSID edu-roam**, to access the organization's network.
  For example, 24 per day/7 days a week and assign these endpoints to **VLAN 1**.
• *(Optional)* Authorize all other users with **Deny Access**.

The CounterACT RADIUS server *always* handles the authorization of endpoints.

**Edu-Roam Endpoint Authorization**
Local Endpoint Authorization
Pre-Audit Authorization Tab Rule Display

MAC Address Bypass

To allow endpoint network authentication using only a MAC address, see Configure MAC Access Bypass. MAC address bypass (MAB) authentication is typically used to authenticate network devices such as printers. You can define the authorization that the CounterACT RADIUS server imposes on the endpoint following its authentication. Possible authorizations include:

- Deny access only
- VLAN assignment only
- VLAN assignment and one or more attribute-value pair (AVP) assignments
- One or more attribute-value pair (AVP) assignments.

For details about defining authorization options, see Rule Authorization.

In the RADIUS Plugin, implement endpoint MAB authentication using any of the following configurations:

- Local Mode
- Proxy Mode

Local Mode

Configure entries in the MAC Address Repository (MAR). These are the identified endpoints that you permit to authenticate using MAB.
Proxy Mode

In the Authentication Sources tab, configure an external RADIUS server entry with the domain assignments **NULL Domain** and **DEFAULT Source**. The CounterACT RADIUS server then queries this source to accomplish endpoint authentications. For details about authentication source domain assignments, see Configure Authentication Sources.

The CounterACT RADIUS server **always** handles the authorization of **endpoints that require MAB authentication**. Make sure that your Pre-Admission Authorization rules are well defined, such that these endpoints are not denied access by default. For the authorization processing logic, see Authentication-Authorization Processing Flow.

Network Device Administration

The RADIUS Plugin supports the need to perform authentication and initial authorization on the administrators of an organization's network devices, based on both RADIUS and Active Directory. The administrator, in this use case, already has access to the organization's network; what they need is to be able to log in to a network device and to execute shell commands on that device.
To accomplish this:

- In the organization’s network device, configure:
  - The IP address of the CounterACT device as the RADIUS server
  - The pre-shared key of the CounterACT RADIUS server
- In the User Directory Plugin, configure the Active Directory server to be queried about user group membership (LDAP-Group)
- In the RADIUS Plugin:
  - In the RADIUS Settings tab, select **Enable PAP-Authentication**.
    - **PAP authentication is not secure and, therefore, must be explicitly selected for use.**
  - In the Authentication Sources tab, add the Active Directory server as an authentication source and configure test credentials and join credentials. Join the applicable AD domain and run the plugin test.
  - In the Pre-Admission Authorization tab, add the following pre-admission rule:
    - Rule Condition that evaluates the **Authentication-Type** attribute for a match on the value **PAP**.
    - Rule Authorization that uses the attribute template: **Cisco-Network Device Administration**. This template contains the **Service-Type** attribute with the value **NAS-Prompt-User** and the **Cisco-AV Pair** attribute with the value `shell:priv-lv=#`. Replace the pound sign (#) with a valid privilege level value that allows user execution of shell commands on the network device, which are authorized for that privilege level.

Generate a Forescout 8.1 policy log and view policy processing activity that specifically dealt with PAP Authentication.

**To generate a policy log and view PAP Authentication activities:**

1. In the Console toolbar, select **Log > Policy Log**. The Policy Log dialog box opens.
2. In the dialog box, define a time scope, a host scope, and the number of records you want the log to display.
3. Select **OK**. The Policy Log window opens, displaying the generated results.
4. Using the **Filter** options/fields, re-generate filtered log results that display PAP authentication activities.
5. Double-click a log entry to view its details.
UserPrincipalName does not match sAMAccountName

There are cases where the userPrincipalName (UPN), a logon name for a user based on the Internet-standard RFC 822, and the sAMAccountName (SAM), a logon name used to support clients and servers for pre-Windows 2000 environments, may be in use but do not match.

For cases where users log on using the UPN account and the UPN account name is not the same as the SAM, the Forescout administrator should set dot1x set_property config.upn.doesntmatch.sam to 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.

To allow user log on when UserPrincipalName does not match sAMAccountName, complete the following steps:

1. Log in to the CLI on the Appliance.
2. Run the following commands:
   a. fstool dot1x set_property config.upn.doesntmatch.sam true.
   b. fstool dot1x restart

Advanced Topics

This section presents information about the following advanced topics:

- Authentication-Authorization Processing Flow
- Re-Authentication Methods
- Plugin Redundancy and Failover
- Common Troubleshooting Issues
Authentication-Authorization Processing Flow

The following diagram presents the CounterACT RADIUS server processing flow when performing endpoint authentication and authorization:

When the CounterACT RADIUS server must impose authorization on managed, authenticated endpoints, it uses the authorization provided from the following hierarchy of Forescout sources:

1. Policy action authorization – If available, first preference.
   
   **Exception**: When an endpoint attempts its initial admission to an organization’s network (Forescout 8.1 has not yet detected the endpoint), the CounterACT RADIUS server always imposes the matching **pre-admission authorization rule** on the endpoint.

2. MAR authorization – If available, second preference.
3. Pre-admission authorization rule – Third preference. The CounterACT RADIUS server evaluates pre-admission authorization rules when no other Forescout source (not policy action, no MAC Address Repository) provides the authorization to impose on an authenticated endpoint, including when an endpoint attempts its initial admission to an organization’s network (Forescout 8.1 has not yet detected the endpoint).

When none of the above sources provide the CounterACT RADIUS server with the authorization to impose on an authenticated endpoint, the CounterACT RADIUS server does not include any authorization in its reply to the NAS device. In this case, the NAS device determines the authorization to impose on the endpoint.

Re-Authentication Methods

The RADIUS Plugin employs any of the following re-authentication methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>Protocol</th>
<th>NAS Type</th>
<th>Vendor</th>
<th>Packet Content</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>COA</td>
<td>RADIUS-CoA</td>
<td>General</td>
<td>Cisco</td>
<td>Port=1700, with Cisco VSA=&quot;subscriber:command=reauthenticate&quot;</td>
<td>1</td>
</tr>
<tr>
<td>COA</td>
<td>RADIUS-CoA</td>
<td>Switch</td>
<td>Tellabs</td>
<td>Port = 3799, with Calling-Station-Id and Tellabs-AVPair=&quot;subscriber:command=reauthenticate&quot;</td>
<td>2</td>
</tr>
<tr>
<td>POD General</td>
<td>RADIUS-POD</td>
<td>General</td>
<td>General</td>
<td>Port = 3799 with Accounting SID</td>
<td>2</td>
</tr>
<tr>
<td>POD Cisco</td>
<td>RADIUS-POD</td>
<td>General</td>
<td>Cisco</td>
<td>Port = 3799 with Accounting SID, &quot;Service-Type=Login&quot;</td>
<td>3</td>
</tr>
<tr>
<td>Port Authenticate</td>
<td>SNMP</td>
<td>Switch</td>
<td>General</td>
<td>MIB = &quot;1.0.8802.1.1.1.1.2.1.5&quot; + port index</td>
<td>4</td>
</tr>
<tr>
<td>Aironet De-authentication</td>
<td>SNMP</td>
<td>WLAN Device</td>
<td>Cisco/Aironet</td>
<td>MIB = &quot;1.3.6.1.4.1.1.1417 9.2.1.4.1.22&quot;</td>
<td>5</td>
</tr>
<tr>
<td>Xirrus De-authentication</td>
<td>SNMP</td>
<td>WLAN Device</td>
<td>Xirrus</td>
<td>MIB = &quot;1.3.6.1.4.1.2101 3.1.2.22.2.3.0&quot;</td>
<td>6</td>
</tr>
<tr>
<td>Port Bounce</td>
<td>SNMP</td>
<td>Switch</td>
<td>General</td>
<td>MIB = &quot;1.3.6.1.2.1.2.2.1.7&quot; + port index</td>
<td>7</td>
</tr>
</tbody>
</table>
If you need to customize any of the Packet Content information, contact your Forescout representative.

**Plugin Redundancy and Failover**

This section provides an overview of the internal redundancy mechanism of the RADIUS Plugin. The following diagram presents a standard 802.1X deployment:

Terminology:

- **Authenticating Appliance** – The CounterACT Appliance that initially authenticates the endpoint.
- **Managing Appliance** – The CounterACT Appliance whose assigned IP address scope includes the endpoint IP address.
• **Capable Devices** – The CounterACT RADIUS servers defined on a NAS and which the NAS has previously addressed for authentication.

Each CounterACT RADIUS server maps the NAS devices to which it can send re-authentication requests.

> Managing and authenticating Appliances are capable by definition.

When an Appliance triggers an authorization action, the Forescout infrastructure sends this action to the group of *capable* Appliances per the relevant controller. As with any action, the Forescout infrastructure also sends the authorization action to the Managing appliance, regardless of whether that Appliance is capable or not. Each capable Appliance that receives the authorization action learns it and waits, preparing itself to respond to endpoint authentication requests with the application of this action.

At this point, the managing Appliance manages endpoint re-authentication, as follows:

1. The RADIUS Plugin compiles an internal list of all *capable* CounterACT RADIUS servers.
2. Starting with the authenticating Appliance, the managing Appliance evaluates each capable device to identify the Appliance/CounterACT RADIUS server that issues the re-authentication request.
3. If no capable device is available other than the authenticating Appliance and the authenticating Appliance is out of service, the managing Appliance issues the re-authentication request.
4. When the managing Appliance is out of service, no policy evaluation processing occurs.

**Common Troubleshooting Issues**

This section describes how to troubleshoot the following common plugin issues that are associated with a Forescout machine failing to join a domain:

- User Directory Plugin Incorrectly Configured
- Winbindd Dead

**Forescout Machine Fails to Join Domain**

**User Directory Plugin Incorrectly Configured**

Review User Directory Readiness.

**Winbindd Dead**

If Winbindd is not running or is not running properly, do the following:

- Verify that Forescout hostname length is no longer than 15 characters. This is a Microsoft AD constraint.
- Verify the Admin user, which is configured in User Directory Plugin, has the required privileges to bind and join to the domain.
• Check that the NTP service is configured (typically performed during Forescout installation). If not configured, do the following to point to the proper IP address:
  
  a. Log in to the CounterACT device CLI.
  b. Run the following command:
     
     ```bash
     fstool ntp <server ip>
     ```
  
• In User Directory Plugin, check both the alias and child domain configurations. See User Directory Readiness.

In some cases, deployments fail due to improper network-related configuration:

• Verify environment readiness [pre-shared key, NAS configuration, endpoint readiness].

## Appendix

This appendix presents information about the following plugin topics:

- Configure Endpoint Supplicant

### Configure Endpoint Supplicant

This section describes how to configure a supplicant on endpoints running any of the following operating systems:

- Supplicants on Windows 7/Windows XP Endpoints
- Supplicants on MAC Endpoints

### Supplicants on Windows 7/Windows XP Endpoints

This section describes how to configure a supplicant on endpoints running the Windows 7 or the Windows XP operating system.

**To configure the Windows 7/XP endpoint supplicant:**

1. Verify that the WIRED/WLAN-AutoConfig service is automatically started and running on the endpoint.

2. Navigate to View Network Connections. The Local Area Connection Properties dialog box opens to the Networking tab.
3. Right-click and select the properties of the LAN card connected to the switch.
4. Select the **Authentication** tab.
5. Configure the following authentication settings:

a. Select **Enable IEEE 802.1X authentication** to start the supplicant or clear this option to stop the supplicant.

b. From the **Choose a network authentication method** drop-down menu, select **Microsoft: Protected EAP (PEAP)**.

c. When using manually entered credentials, select **Remember my credentials for this connection each time I'm logged on**. When selected, the supplicant caches and then re-uses authenticated credentials. If not selected, the user is prompted to enter their credentials with every re-authentication.

d. If a 802.1X supplicant is connected to a non-802.1X port, select **Fallback to unauthorized network access**.
e. Select Settings.

![Protected EAP Properties dialog box]

6. In the Protected EAP Properties dialog box, configure the following:

   a. To have the client validate RADIUS server authenticity, select the **Validate Server Certificate** option.

   b. In the **Trusted Root Certificate Authorities** pane, select the root certificate of the CA that signed the installed RADIUS server certificate. See **Certificate Readiness**.

   c. Select **Do not prompt user to authorize new servers or trusted certification authorities** to disable the following event prompt:

   When encountering an unknown certificate, the supplicant might present a dialog box that allows the user to trust a certificate from an unknown source manually.

   d. From the **Select Authentication Method** drop-down menu, select the **Secured password (EAP-MSCHAP v2)** method.

   To configure Secured password (EAP-MSCHAP v2) settings, select **Configure**.

   e. To cache TLS session keys and make re-authentications faster, select **Enable fast reconnect**.

7. Select **OK** to return to the Local Area Connection Properties dialog box, and then select **OK** to save your settings.
Supplicants on MAC Endpoints

Supplicants on MAC endpoints are automatically configured when these endpoints attempt to access an 802.1X-restricted network.

Authentication Module Information

The RADIUS Plugin is installed with the Forescout Authentication Module.

The Forescout Authentication Module provides secure network access across wired, wireless, and guest networks through its RADIUS and User Directory Plugins.

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.

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:

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/

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).