CounterACT® 802.1X Plugin
Configuration Guide
Version 4.2.0
### Table of Contents

**Overview** ................................................................. 4
  - Understanding the 802.1X Protocol ................................................. 4
  - About the CounterACT 802.1X Plugin .................................................. 6
    - About This Document ........................................................................ 7
  - 802.1X Plugin Components ................................................................. 7
    - Authentication Sources ...................................................................... 7
    - Pre-Admission Authorization ................................................................. 7
    - Server Certificate ............................................................................. 8
    - RADIUS Settings ............................................................................. 9
    - MAC Address Repository ................................................................. 9

**Supported Authentication Types** ....................................... 10

**CounterACT Requirements** .............................................. 10

**Install the Plugin** ........................................................... 11

**How to Proceed** ............................................................. 12
  - Environment Readiness ................................................................. 12
  - Network Device Readiness ............................................................... 13
  - Endpoint Readiness ........................................................................ 22
  - User Directory Readiness ................................................................. 26
  - Plugin Configuration ......................................................................... 28
    - Configure Authentication Sources ................................................... 29
    - Configure Pre-Admission Authorization ........................................... 32
    - Configure Server Certificates .......................................................... 37
    - Configure RADIUS Settings ............................................................. 46
    - Per Appliance 802.1X Configuration ............................................... 49
    - Configure MAC Access Bypass ......................................................... 50
  - Testing and Troubleshooting ............................................................ 55
    - Test the Plugin .............................................................................. 55
    - Troubleshooting Policy Templates .................................................... 57
    - Technical Support .......................................................................... 63

**Plugin Properties and Custom Policies** ............................. 63
  - Properties for Use in Policy Conditions ............................................ 63
    - Advanced ...................................................................................... 64
    - Authentication Decision ................................................................. 64
    - Authentication Details ...................................................................... 65
    - Authentication Events ....................................................................... 66
    - Authorization .................................................................................. 66
    - Client Certificate ........................................................................... 66
    - MAR .............................................................................................. 67
    - NAS Device ................................................................................... 67
    - Windows 7 Supplicant ....................................................................... 67
Create Custom Policies........................................................................................................... 68

Actions.................................................................................................................................. 69
  802.1X Authorize Action.......................................................................................................... 69
  802.1X Update MAR Action.................................................................................................... 71

Use Cases.................................................................................................................................. 74
  Categorize Endpoint Authorizations ..................................................................................... 75
  Monitor Successful Authentications and Apply Authorizations .......................................... 79
  Corporate Wired and Wireless Authentication ......................................................................... 85
    Single Domain ....................................................................................................................... 85
    Multi-Domain ....................................................................................................................... 86
  CounterACT RADIUS Server as a Proxy ................................................................................. 89
  Centralized Web Authentication ............................................................................................. 89
    Enable MAC Address Bypass ............................................................................................... 90
    Configure Pre-Admission Authorization Rule ....................................................................... 90
    Centralized Web Authentication Policy Template .............................................................. 92
  EDU-ROAM ............................................................................................................................ 98
  MAC Address Bypass ............................................................................................................. 103

Advanced Topics ..................................................................................................................... 104
  Authentication-Authorization Processing Flow .................................................................... 105
  Re-Authentication Methods .................................................................................................. 106
  Plugin Redundancy and Failover ............................................................................................ 107
  Common Troubleshooting Issues ............................................................................................ 108
    CounterACT Machine Fails to Join Domain ....................................................................... 108

Appendix .................................................................................................................................... 109
  Configure Endpoint Supplicant .............................................................................................. 109
    Supplicant on Windows 7/Windows XP Endpoints ............................................................ 109
    Supplicant on MAC Endpoints ............................................................................................ 112

Additional CounterACT Documentation .................................................................................... 113
  Documentation Portal ........................................................................................................... 113
  Customer Support Portal ....................................................................................................... 113
  CounterACT Console Online Help Tools .............................................................................. 114
Overview

This section provides an overview of the following topics:

- Understanding the 802.1X Protocol
- About the CounterACT 802.1X Plugin
- 802.1X Plugin Components

Understanding 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 a network, whether wired and wireless. The 802.1X authentication process consists of the following participating entities:

- **Client**: The user or client endpoint attempting to access an organization's network and is required, by the organization security requirements, to undergo authentication and be evaluated as authenticated:
  - Endpoints having a *supplicant*, embedded software that handles the endpoint's side of the 802.1X authentication sequence, can be authenticated based on any of the following:
    > User credentials or certificate
    > Device credentials or certificate
  - Endpoints not having a *supplicant*, for example printers, are authenticated solely based on their MAC address, which is termed 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), situated between the client and the authentication server, to which the client connects in its attempt to gain network access. Both wireless access points and switches are authenticator examples.
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 not having a supplicant undergo MAB authentication. Since in such a scenario there is no supplicant response, phase 1 times out. Then, the RADIUS server evaluates the source client, based on the endpoint MAC address.
Endpoints without Supplicant: Processing Sequence

The following diagram provides a high-level view of the 802.1X processing sequence for endpoints not having a supplicant:

![Diagram showing the processing sequence for endpoints without a supplicant]

About the CounterACT 802.1X Plugin

The CounterACT 802.1X 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 802.1X Plugin enables CounterACT 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 CounterACT to provide authentication and authorization instructions to NAS devices, to integrate with user directory servers and to employ powerful CounterACT 802.1X policies to detect, authenticate and control network endpoints and associated user activity.
About This Document

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

802.1X Plugin Components

This section provides high-level description of the 802.1 X Plugin components that require configuration in order for the plugin to effectively operate. Plugin components are:

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

Authentication Sources

Use the Authentication Sources tab to select the RADIUS servers and the User Directories that handle the validation of credentials provided during endpoint authentication. All of the authentication sources are configured in the User Directory Plugin.

Pre-Admission Authorization

Use the Pre-Admission Authorization tab to define the set of prioritized rules that the CounterACT RADIUS server uses to evaluate endpoints for authorization treatment, after their authentication by the applicable RADIUS server (a selected Authentication Source). These rules are evaluated in the order of their designated priority against authenticated endpoints. For endpoints matching a rule's condition, the CounterACT RADIUS server applies the defined authorization treatment to the endpoint in the ACCEPT message it sends to the NAS device.
Server Certificate

Use the **Server Certificate** tab to define the following:

- The CounterACT RADIUS server certificate configuration
- The parameters for generating a Certificate Signing Request (CSR) file
RADIUS Settings

Use the **RADIUS Settings** tab to configure settings that are relevant when the CounterACT RADIUS server functions as the authenticating RADIUS server. Regardless of whether the CounterACT RADIUS server functions the authenticating RADIUS server or not, it _always handles_ the **authorization** of authenticated endpoints.

![RADIUS Settings Tab](image)

MAC Address Repository

Maintain the repository of MAC addresses of endpoints that do not have a functioning 802.1X supplicant and are being permitted to be authenticated by the CounterACT RADIUS Server using MAC address bypass (MAB).

Optionally, per MAC address entry in this repository, define an authorization that is imposed on the MAB-authenticated endpoint by the CounterACT RADIUS Server.
Supported Authentication Types

The 802.1X Plugin supports use of 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-MSCHAPv2</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>
</tbody>
</table>

For the supported RADIUS access request delimiters, see section Determining the Authentication Source to Query.

CounterACT Requirements

- CounterACT version 7.0.0:
  - Hotfix 1.7.1 or above
  - Install Service Pack 3.0.0 or above for the plugin to provide its full support of CounterACT centralized web authentication. For details, see Centralized Web Authentication, Configure Pre-Admission Authorization Rule.

It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.

- CounterACT Switch Plugin 8.5.7 or above
- CounterACT Wireless Plugin 1.3.2 or above
- CounterACT User Directory 5.4.3 or above
Install the Plugin

This section describes how to install the 802.1X Plugin. It is recommended to deploy the plugin on all Appliances. To accomplish this plugin deployment, install the plugin on the Enterprise Manager; the Enterprise Manager then automatically installs/upgrades the plugin in all Appliances under its control.

To install the plugin:
1. Take one of the following actions to acquire the plugin:
   a. If this is a beta release of the plugin version, acquire the plugin .fpi file from your ForeScout representative or contact beta@forescout.com.
   b. Otherwise, navigate to the Customer Support, Base Plugins page and download the plugin .fpi file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select Options from the Tools menu.
5. Select Install. The Open dialog box opens.
6. Browse to and select the saved plugin .fpi file.
7. Select Install
8. An installation or upgrade information dialog box and a license agreement dialog box open. Accept the license agreement to proceed with the installation.
9. The following dialog box opens:

![Dialog Box Image]

10. The installation screen provides instructions for working with certificates. See [Configure Server Certificates](#) for details.

11. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

12. Select **Start**.

### How to Proceed

This section presents information about the following topics:

- **Environment Readiness**
- **Plugin Configuration**
- **Testing and Troubleshooting**

### Environment Readiness

In order to work with the 802.1X solution, you need to configure a variety of components. This section provides an overview of the components you will be working with.

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 scenario(s) you want to address using the 802.1X Plugin, see [Use Cases](#).
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 CounterACT

NAS devices (switches, WLAN devices) must be managed by the appropriate CounterACT plugin, this being either the Switch Plugin or the Wireless Plugin. Per managed NAS device, make sure that each CounterACT plugin is configured with the necessary RADIUS secret.

Network Device Readiness Policy Templates

It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Guide.

Cisco Switch Readiness Template

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

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

Run the Template

This section describes how to create a policy based on the template.
To run the template:

1. Select the **Policy** tab from the Console.

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

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

4. Select **Next**. The Name page opens.

*Name the Policy*

The Name page lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.
1. 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 will be 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.

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

**Define which Endpoints are Inspected - Policy Scope**

The Scope Page and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.
1. Specify the scope of the policy. The following options are available:
   - **All IPs**: Include all addresses in the Internal Network range.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK to close IP Address Range dialog box, and select **Segments** from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Select this option to include endpoints for which the IP address is not known.

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

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

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

**Cisco Switch Readiness Main Rule**

CounterACT-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 and 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>
</table>
| **1. AAA Not Enabled**                            | Verifies if any one of the following is true on the switch:  
  |       • aaa new-model is not configured            |                                                                                                                                          |
  |       • no aaa new-model is configured             | When the switch configuration matches any one of these conditions, the switch is **not ready** for 802.1X authentication.               |
| **2. 802.1X Authentication Method List Not Created** | Verifies if the following is true on the switch:  
  |       • aaa authentication dot1x... is not configured | When the switch configuration matches this condition, the switch is **not ready** for 802.1X authentication.               |
| **3. Dot1X Not Globally Enabled**                  | Verifies if the following is true on the switch:  
  |       • dot1x system-auth-control is not configured | When the switch configuration matches this condition, the switch is **not ready** for 802.1X authentication.               |
| **4. RADIUS Server Not Configured**                | Verifies if the following is true on the switch:  
  |       • radius-server host <IP address> is not configured | When the switch configuration matches this condition, the switch is **not ready** for 802.1X authentication.               |
| **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.

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

Run the Template

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

**To run the template:**

1. Select the Policy tab from the Console.


3. In the navigation tree, select **802.1X > 802.1X Readiness** and then select **Cisco Switch Port Readiness**.
4. Select **Next**. The Name page opens.

**Name the Policy**

The Name page lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

1. 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 will be 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.

2. Select **Next**. The Scope page and the IP Address Range dialog box open.

**Define which Endpoints are Inspected - Policy Scope**
The Scope Page and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.

1. Specify the scope of the policy. The following options are available:
   - **All IPs**: Include all addresses in the Internal Network range.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close IP Address Range dialog box, and select **Segments** from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Select this option to include endpoints for which the IP address is not known.

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

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

3. 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 CounterACT-managed switches that meet the following criteria match the main rule of this policy:

- 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.

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>- <code>dot1x pae authenticator</code> 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>
<tr>
<td>2. 802.1X Authentication on the Port Not Enabled</td>
<td>Verifies if the following is true for the switch port:</td>
</tr>
<tr>
<td></td>
<td>- <code>authentication port-control auto</code> 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>
<tr>
<td>Sub-Rule Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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.

**Endpoint Readiness Policy Templates**

It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Guide.

*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.

**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 CounterACT Asset Classification policy)
- Verify that endpoints are classified in the *Corporate Hosts* group (can be accomplished by running the CounterACT Corporate/Guest Control policy)
- Verify that the CounterACT HPS Inspection Engine Plugin, version 9.5.5 or above, manages the endpoints

**Run the Template**

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

**To run the template:**

1. Select the **Policy** tab from the Console.
2. Select **Add**. The Policy Wizard opens.

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

4. Select **Next**. The Name page opens.

**Name the Policy**

The Name page lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.
1. 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 will be 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.

2. Select **Next**. The Scope page and the IP Address Range dialog box open.

**Define which Endpoints are Inspected - Policy Scope**

The Scope Page and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.

1. Specify the scope of the policy. The following options are available:
   - **All IPs**: Include all addresses in the Internal Network range.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close IP Address Range dialog box, and select **Segments** from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Select this option to include endpoints for which the IP address is not known.

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

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

3. Select **Finish**. The policy is created.
Wired Windows 7 Endpoint Readiness Main Rule

CounterACT-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 either remotely managed (Windows Manageable Domain property) or 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>
<tbody>
<tr>
<td>1. Wired AutoConfig Service Not Running</td>
<td>Verifies if the following is true on the endpoint:</td>
</tr>
<tr>
<td></td>
<td><strong>Wired AutoConfig</strong> service is not running</td>
</tr>
<tr>
<td></td>
<td>When this condition is true, the endpoint is not ready for 802.1X authentication.</td>
</tr>
<tr>
<td>2. 802.1X Authentication Not Enabled</td>
<td>Verifies if the following is true for the supplicant installed on the endpoint:</td>
</tr>
<tr>
<td></td>
<td><strong>Enable IEEE 802.1X authentication</strong> configuration is not enabled</td>
</tr>
<tr>
<td></td>
<td>When this condition is true, the endpoint is not ready for 802.1X authentication.</td>
</tr>
</tbody>
</table>
### Sub-Rule Name | Description
--- | ---
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 of these 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 802.1X Plugin of the configured user directories. The following topics are described:

- **User Directory Plugin: General Pane**
- **User Directory Plugin: Settings Pane**
- **Authenticating Using Microsoft Active Directory: Other Issues**
- **Using an External RADIUS Server**

#### User Directory Plugin: General Pane
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 802.1X 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.


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 802.1X Plugin automatically selects a user directory (Microsoft Active Directory) server FQDN. Take note of the following:

   a. The 802.1X 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 CounterACT machine to the domain.

2. However, if the **DNS Detection** option is not enabled, the 802.1X 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 CounterACT machine to the domain.

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

4. For the CounterACT RADIUS server to authenticate using Microsoft Active Directory, the CounterACT device must be bound to (join) the domain. When the 802.1X 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 Settings pane > Directory section > **Administrator** field, for that domain.

5. In the Active Directory server, sufficient privileges for the **user**, defined in the Settings pane > Directory section > **Administrator** field, 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 802.1X Plugin Authentication Sources tab, verify that the following information is defined in the User Directory Plugin:
   a. Additional Domain Aliases: In the Settings pane > Additional Domain Aliases section > **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.

   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 of the Additional Domain Aliases section. For example, the **Domain** field contains the entry `glbl.mycompany.com`, there is no need to also enter `glbl` in the **Specify** field.

**Authenticating Using Microsoft Active Directory: Other Issues**

1. To avoid difficulties when a CounterACT machine attempts to join a domain, it is recommended that the CounterACT machine hostname is a maximum length of 15 characters. Reference: [https://support.microsoft.com/en-gb/kb/909264](https://support.microsoft.com/en-gb/kb/909264)
2. 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 on using an external RADIUS server as an authentication source for the 802.1X 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.

Plugin Configuration

This section describes how to configure the various plugin components in order for the 802.1X 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 Server Certificates
- Configure RADIUS Settings
- 802.1X Authorize Action
- Per Appliance 802.1X Configuration
- Configure MAC Access Bypass

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

To configure the plugin:

1. In the Console, select Tools > Options > Plugins. The Plugins pane opens.
2. In the Plugins pane, select the 802.1X entry from the table listing.
3. Select **Configure**. The 802.1X pane opens in the Options window and displays the Authentication Sources tab.

### Configure Authentication Sources

Use the **Authentication Sources** tab to define the servers that the plugin uses to accomplish the 802.1X authentication of endpoints.

Supported authentication sources:

- Microsoft Active Directory
- External RADIUS Server

### To add new authentication sources:

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

2. In the dialog, select one or more than one entry; it is valid to select RADIUS servers, Microsoft Active Directory servers or a combination of both types.
3. Select **OK**. The Authentication Sources tab opens containing the added authentication sources.

The Authentication Sources tab presents the user directories and external RADIUS servers that are selected to function as the authentication sources that the CounterACT RADIUS server queries, when executing the 802.1X authentication of endpoints. User directories and external RADIUS servers that are available to be added as authentication sources are configured in the User Directory Plugin. For details about the necessary User Directory Plugin configurations, see *User Directory Readiness*.

Per selected authentication source, the tab presents the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name   | Name of the authentication source as configured in the User Directory Plugin. Authentication Sources that are not configured for plugin use have the information *(Source NOT in USE)* displayed immediately after their name. Configure an authentication source for plugin use by performing any of the following:  
• Define a domain for the source  
• Set the source as the **DEFAULT Source**  
• Set the source to handle **NULL Domains** |
<p>| Type   | The server type of the authentication source as configured in the User Directory Plugin. For 802.1X Plugin purposes, the supported types are <strong>Microsoft Active Directory</strong> and <strong>RADIUS</strong>. |</p>
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains</td>
<td>Lists the domains, as supplied in 802.1X authentication requests, which the authentication source is assigned to handle.</td>
</tr>
<tr>
<td></td>
<td>- For Microsoft Active Directory source:</td>
</tr>
<tr>
<td></td>
<td>- The information appearing in this column comes from the domain and additional domain aliases that are configured for the authentication source in the User Directory Plugin.</td>
</tr>
<tr>
<td></td>
<td>- In the 802.1X Plugin, this information is view-only. Select View.</td>
</tr>
<tr>
<td></td>
<td>- For RADIUS server source:</td>
</tr>
<tr>
<td></td>
<td>- Domain information is manually configured for the authentication source. Select a RADIUS authentication source entry and select Edit. The Edit Radius Proxy Condition dialog opens.</td>
</tr>
<tr>
<td></td>
<td>- In the Domain field of the dialog, enter a domain NetBIOS name, as it would appear in the RADIUS access request, and select +Add. Repeat this step to add multiple domain names.</td>
</tr>
</tbody>
</table>

The Authentication Sources tab provides the following options for defining an entry's domain handling:

- **Set Default**: Select this button to designate the authentication source as the default authentication source. See Determining the Authentication Source to Query.
- **Set Null**: Select this button to designate the authentication source as the null domain handler. See Determining the Authentication Source to Query.

An authentication source can be assigned any combination of domains, designated the default handler and designated the null domain handler.
Determining 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. First - 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:
   a. domain\user
   b. user@domain

2. Second - 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. Third - 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.

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 their designated priority.

The CounterACT RADIUS server evaluates pre-admission authorization rules when no other CounterACT source - not policy action, not 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. Rule evaluation priority displays in the Rule Priority column of the Pre-Admission Authorization table.
  - When an endpoint is found to match 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; you can edit this rule and modify its detail.

In the CounterACT RADIUS Server’s reply message it send to the NAS device:

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

In the tab, the table displays the current set of defined pre-admission authorization rules.
In the tab, perform any of 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.

- **Move Up** or **Move Down** - use these buttons to modify the priority in which rules are evaluated. Rule evaluation priority displays in the **Rule Priority** column of the Pre-Admission Authorization table.

- **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.

**Rule Configuration**

Each pre-admission authorization rule is composed of 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. In the Condition section, perform any of the following:

- **Add** new rule conditions
- **Edit** rule conditions
- **Remove** rule conditions

After you perform any of the above [Add, Edit, Remove], selecting **OK** in the Pre-Admission Authorization Rule window updates 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 802.1X 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:

- **Called Station ID**
- **Calling Station ID**
- **Certificate Common Name**
- **Certificate Issuer**
- **Certificate Subject**
- **Certificate Subject Alternate Name**
- **Day and Time Restriction** - is compared with the day/time of the received endpoint authentication request.
- **EAP Type**
- **LDAP-Group** - is compared with the 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 Source tab. 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).
- **MAC Found in MAR** - 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).
- **NAS IP Address**
- **NAS Port Type**
- **SSID**
- **User-name**
Column Description

**Criterion Value**
For the selected attribute, define the attribute value that the CounterACT RADIUS server uses to evaluate authenticated endpoints for a match.

Depending on the selected attribute, one of the following methods is used to define the attribute value:

- 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:
  - This field is case sensitive.
  - To escape any special character except the backslash, prefix the special character with four (4) consecutive backslashes. For example, `.engineering` must be provided in the field as `\\\\.engineering`.
  - To escape a backslash special character, enter a total of eight (8) consecutive backslashes. For example, `finance\\eastern` must be provided in the field as `finance\\\\\\\\eastern`.
  - 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.
- Select from a table the day(s) of the week and/or hour(s) of the day to evaluate and/or not evaluate.
- Choose from a menu of available values.
- Select between evaluation instruction buttons [Meets this criterion, Does not meet this criterion].
- In an Expression field, enter any combination of alphanumeric and special characters.

**Rule Authorization**
For an authenticated endpoint found to match 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deny Access</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>VLAN</strong></td>
<td>Define the VLAN to which the NAS device must assign the authenticated endpoint. Enter either the VLAN ID or the VLAN name. This field accepts alphanumeric characters.</td>
</tr>
</tbody>
</table>
### Configure Server Certificates

By default, the CounterACT RADIUS server contains a self-signed certificate that is presented during initial TLS negotiation. A certificate signed by an external certificate authority can be installed on the CounterACT RADIUS server instead of the self-signed certificate. This allows endpoints to validate the authenticity of the CounterACT RADIUS server using a trusted certificate authority (CA). ForeScout recommends that endpoint supplicants are configured to validate the RADIUS server.
Server certificate configuration is accomplished in the Server Certificate tab of the 802.1XPane.

Two options are available for working with certificates:

- **Use a Self-Signed Certificate**
- **Use Certificate Issued by an External Certificate Authority**

By default, the plugin uses the SHA-512 algorithm, an AES-256 encryption and a 2048 bit certificate key, as follows:

- For the self-signed certificate
- When signing the CSR used to generate the RADIUS server certificate

**Use a Self-Signed Certificate**

Use certificates internally generated during the plugin installation. This is a server certificate signed by the root certificate authority (CA) residing in the CounterACT RADIUS server that is self-signed.

**To configure CounterACT to work with an internally generated certificate:**

1. Select the **Use self-signed certificate** checkbox. This option is selected by default.
Use Certificate Issued by an External Certificate Authority

Use of a server certificate that is issued by an external certificate authority (CA), other than the root CA residing in the CounterACT RADIUS server, allows for the following:

- The same external CA to issue a client certificate to the authenticating endpoint
- The authenticating endpoint to validate the RADIUS server using its CA store

When working with an external CA to issue a server certificate, the CA’s certificate must be installed on the Appliances. The following certificate installation options are available when working with an external CA:

- Global Appliance Certificate Setup
- Per Appliance Setup

By default, the server certificate installed on the Enterprise Manager, along with its CA certificates, are distributed to and used by all the Appliances. However, if required, a separate and unique server certificate can be installed on individual Appliances.

An example in which Appliances require their own individual server certificate: An organization deploys multiple wireless networks. One wireless network is dedicated to serving corporate-issued endpoints and a second wireless network is dedicated to serving guest or BYOD devices. Corporate-issued endpoints trust a certain organizational certificate authority and are authenticated by Appliances with an installed server certificate that is signed by this particular certificate authority. Guest and BYOD devices trust an alternate certificate authority and are authenticated by an Appliance with an installed server certificate that is signed by the alternate certificate authority.

Global Appliance Certificate Setup

This section describes how to set up all Appliances to work with the Enterprise Manager external certificate. This means that the server certificate from the Enterprise Manager is propagated to and used by all the Appliances, unless an Appliance-specific certificate setup is defined.

To propagate the Enterprises Manager certificate on all Appliances:

1. Select the Default tab.
2. In the Server Certificate tab, clear the Use self-signed certificate checkbox. This option is selected by default.
3. In the Server Certificate tab, clear the Use local server certificate checkbox. This option is cleared by default.

When the Use local server certificate checkbox is selected in the Default tab, all Appliances, which do not have a per-Appliance configuration to override this option selection, use their own local server certificate (a separate and unique installed server certificate). Therefore, when propagating the Enterprise Manager server certificate on either all or some Appliances, make sure that the Use local server certificate checkbox is cleared in the Default tab.
4. Follow the directions specified in Install Certificates.

Per Appliance Setup

This section describes how to set up individual Appliances with their own separate and unique server certificate that is issued by an external CA.

**To define an Appliance with a separate and unique certificate:**

1. Create a tab for the Appliance. See Create and Apply Multiple Configurations.

2. In the Server Certificate tab of the Appliance, clear the Use self-signed certificate checkbox. This option is selected by default.

3. In the Server Certificate tab of the Appliance, select the Use local server certificate checkbox. The Appliance is instructed to use its local server certificate.

   - If the Use local server certificate checkbox is cleared in an Appliance tab, that Appliance uses the Enterprise Manager server certificate.
4. Follow the directions specified in Install Certificates.

Install Certificates

Perform the following when using an external certificate authority (CA) to issue certificates for the CounterACT RADIUS server and/or endpoint supplicants:

1. Install the Organizational CA Root Certificate on CounterACT
2. Add Intermediate CA Certificates (Optional)
3. Generate a CSR for the RADIUS Server Certificate
4. Issue and Install the Server Certificate
5. Verify Required Certificates for Client

After performing these steps, test the plugin to verify these procedures were completed successfully. See Test the Plugin for details.

- Installed certificates are preserved during plugin upgrade. There is no need to regenerate or install certificates after a plugin upgrade.

1. Install the Organizational CA Root Certificate on CounterACT

This section describes how to install the organizational CA root certificate to the certificate path of the bundled RADIUS server on each Appliance. This is required so CounterACT will trust the organizational CA.

This trust is required when:

- CounterACT validates the server certificate before installing it.
- CounterACT validates endpoint certificates signed by the same CA.
To install the organizational CA root certificate:

1. Log in to the CounterACT device.
   Copy the root certificate file to the following location on the CounterACT device:
   
   `/tmp/<root_fname>`

2. Run the following command:
   
   `fstool dot1x cert install_root /tmp/<root_fname>`
   
   The certificate is installed.

3. Repeat steps 1-2, as necessary, to install multiple (different) CA root certificates.

   - *On a Windows-Based CA, you should export the certificate file:*
     
     `C:/> certutil -ca.cert <CCC>`

   - *This CA certificate should be deployed on endpoints so that they can validate the server certificate.*

   - *If intermediate CA certificates are part of the server certificate’s trust chain they should be added as described in 2. Add Intermediate CA Certificates (Optional).*

2. Add Intermediate CA Certificates (Optional)

   Additional CA certificates can be added to the RADIUS CA trusted store. This is required when:

   - The RADIUS server needs to validate endpoint certificates signed by a root CA different than the one installed in 1. Install the Organizational CA Root Certificate on CounterACT, or in addition to the root CA as part of a chain. This is usually relevant during EAP-TLS.
   
   - When the server certificate trust chain includes more than the one installed in 1. Install the Organizational CA Root Certificate on CounterACT.

To add certificates:

1. Copy the CA certificate file to the CounterACT device.

2. From the CounterACT device command line, run the following command:
   
   `fstool dot1x cert add_root <cert_file_full_path>`
   
   The certificate is added.

3. Repeat steps 1-2, as necessary, to install multiple (different) intermediate CA certificates.

4. Restart the plugin.
3. Generate a CSR for the RADIUS Server Certificate

Perform the following in order to set up your system to ensure that the CounterACT RADIUS server authenticity is validated by the endpoint:

- Define Certificate Signing Request Details
- Generate and Sign the Certificate Signing Request

**Define Certificate Signing Request Details**

This section describes how to generate Certificate Signing Request (CSR) details.

**To define CSR details:**

1. In the CounterACT Console, select **Options** from the **Tools** menu.
2. Navigate to the 802.1X folder and select the **Server Certificate** tab.

3. Clear the **Use self-signed certificate** checkbox. This option is selected by default.
4. Enter the request details. All fields are mandatory.
   - CA Host OS
   - Private Key Password
   - Subject server name
   - Subject email
   - Organizational Name
   - Country name
   - State or Province Name
   - Locality Name

5. Select **Apply**.

**Generate and Sign the Certificate Signing Request**

This section describes how to generate the certificate signing request (CSR).

**To generate the CSR:**

1. Log in to the Enterprise Manager. If you are generating a dedicated certificate for a specific Appliance, log in to the relevant Appliance

2. Run the following command: `fstool dot1x cert server_csr`

3. The request file is generated and saved to the following location on the CounterACT device:
   
   `/etc/raddb/certs.production/server.csr`

4. A prompt appears with instructions for proceeding. The presented instructional text varies depending on the operating system selected in the **CA Host OS** field of the Server Certificate tab.

   ```plaintext
   • Generating a 2048 bit RSA private key
     ....+++............+++  
   • writing new private key to
     '/etc/raddb/certs.production/server.key'  
   • Certificate Signing Request for RADIUS server of rama-eml-70 is in
     /etc/raddb/certs.production/server.csr; next, please:
   •   => Copy the request file to CA host, and sign the request there
   To sign the csr (Windows-based Certification Authority):
     • ---------------------------------------------------------------
     • 1) On CA host's 'cmd' prompt, submit the csr by typing:
     •   C:\> certreq -submit server.csr
         (select the appropriate CA in the window pop-up)
   ```
2) In CA application>'Pending requests', right-click the <ID> request and choose 'All Tasks > Issue'
3) In CA application>'Issued certificates', double-click the <ID> request, and goto in the 'details' tab
4) There, make sure the 'Extended Key Usage' is present and has the value of '1.3.6.1.5.5.7.3.1'
5) Also in 'details' tab, click 'Copy to file' and save as either 'DER' or 'Base64' encoding.

---

To install the signed certificate:
<= Copy the certificate file <SSS> back here (to /tmp), and do 'fstool dot1x cert install_server /tmp/<SSS>'
===================================

Regenerating the Certificate Signing Request

Use the following procedure to regenerate a CSR.

To regenerate the CSR:

1. Log in to the Enterprise Manager.
2. Run the following command and follow the on-screen instructions:
   
   `fstool dot1x cert server_csr force`
3. The request file is generated and saved to the following location on the Enterprise Manager:
   `/etc/raddb/certs.production/server.csr`

4. Issue and Install the Server Certificate

This section describes how to issue and install the server certificate, which is used by the CounterACT RADIUS server. Carrying out this process requires that you have access to the CA server, to the CounterACT Enterprise Manager and the Appliance, if a dedicated certificate on the Appliance is needed.

On the CA Server:

1. Copy the request file `server.csr` to the CA host, and sign the request on the host. This results in a signed certificate.
2. Verify that you sign the request with the same CA whose certificate you installed previously on the CounterACT server. See 1. Install the Organizational CA Root Certificate on CounterACT.
3. Verify that the certificate's details match the certificate request details, specifically, that extensions are copied from the request to the certificate.

After you receive a signed certificate from your CA, install it on the CounterACT device.

On the CounterACT device:

1. Copy the signed certificate to the following location on the CounterACT device:

   `<CounterACT device>:/tmp`
2. Log in to the CounterACT device and run the following command:
   `fstool dot1x cert install_server /tmp/<server_fname>`
   The following prompt appears:
   `/tmp/server_signed.pem: OK`
   The signed certificate is installed.

3. Verify the installation of the server certificate by running the following command:
   `fstool dot1x cert verify_server`
   The command verifies the following information:
   – That the installed CA certificate issued the server certificate
   – That the server certificate contains the required extensions
   – That the server certificate public key matches the installed private key

4. After completing the certificate installation, restart the plugin and then perform the plugin test (installation of the server certificate is also verified as part of the plugin test).

5. Verify Required Certificates for Client

Verify the installation of all certificates required by the CounterACT RADIUS server to validate the client certificate of an authenticating endpoint.

To verify certificate installation:

1. Copy one of the client certificates to the Enterprise Manager and run the following command:
   `fstool dot1x cert verify_client <cert_file_full_path>`
   An error message appears if the required certificate is not installed.

Configure RADIUS Settings

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

The tab provides the following setting categories:

- RADIUS Server Basic Settings
- RADIUS OCSP 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>Enable/disable running the CounterACT RADIUS server in debug mode. When enabled, CounterACT captures and logs RADIUS traffic processing detail. This option is enabled by default. <strong>Disable this option when plugin configuration is complete, to avoid performance degradation.</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** | The LDAP port that the CounterACT RADIUS server uses to query domains. The available menu options from which to select are as follows:  
  - **Global Catalog** - using port 3268.  
  - **Global Catalog over TLS** - using port 3269. This is the default and *recommended* method.  
  - **Standard LDAP** - using port 389.  
  - **Standard LDAP over TLS** - using port 636.  
  - **User Directory plugin port per AD** - Per domain, as configured in User Directory Plugin |
### RADIUS OCSP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable OCSP                   | By default, this option is not selected. Selecting the Enable OCSP option instructs the CounterACT RADIUS server to look for an OCSP responder URL in the client certificate and verify 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). Upon selecting the Enable OCSP option, the following options become available for selection:  
  - Override Certificate OCSP URL  
  - OCSP Use Nonce  
  - Ignore OCSP Responder Errors |
| Override Certificate OCSP URL | By default, this option is not selected. Selecting the Override Certificate OCSP URL option instructs the CounterACT RADIUS server to ignore the certificate's OCSP URL and, instead, use the URL that is defined in the OCSP Responder URL field to obtain the revocation status of the certificate. Upon selecting the Override Certificate OCSP URL option, the OCSP Responder URL field is enabled for input. |
| OCSP Responder URL            | 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. |
| OCSP Use Nonce                | By default, this option is selected. For security reasons, it is recommended to use nonce in the OCSP query; clearing this checkbox should only be done in the event that the nonce setting is either not supported by or cannot be enabled on the OCSP server. |
| Ignore OCSP Responder Errors  | By default, this option is not selected. When Ignore OCSP Responder Errors is selected, certificate validation does not fail in instances where the OCSP responder is either unspecified or unreachable.  
  
  **Use this option with caution. Use of this option might enable clients, possessing a revoked certificate, to authenticate and connect if the OCSP responder is unavailable.** |

### RADIUS Advanced Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Fast-Reauthentication Cache | Provides the ability to reconnect to wireless access points by using cached session keys. Having this ability allows for:  
  - Quick roaming between wireless access points |
Per Appliance 802.1X Configuration

In the 802.1X Pane of the Console, accomplish any of the following plugin configurations:

- Define, in the Default tab, an 802.1X Plugin configuration [Authentication Source, Pre-Admission Authorizations, Server Certificate and RADIUS Settings]. By default, this 802.1X Plugin configuration is designated to apply to all CounterACT devices that are not designated with a unique 802.1X Plugin configuration.

- Define additional, unique 802.1X 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 802.1X 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 CounterACT device:

1. Select the plus-sign tab [Default +]. The Select CounterACT devices to configure dialog box opens and lists all your CounterACT devices [Enterprise Manager, Appliance1 - Appliance_n].

2. Select a device and select OK. A tab for the selected Appliance appears. This tab contains the full complement of 802.1X Plugin configuration tabs [Authentication Source, Pre-Admission Authorizations, Server Certificate and RADIUS Settings].

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

1. Select the Plus-sign tab [Default +]. The Select CounterACT devices to configure dialog box opens and lists all your CounterACT devices [Enterprise Manager, Appliance1 - Appliance_n].

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 802.1X Plugin configuration tabs [Authentication Source, Pre-Admission Authorizations, Server Certificate and RADIUS Settings].

**To edit settings of a unique 802.1X configuration:**

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

2. On the tab itself, select the relevant edit icon or delete icon to update the scope of the configuration. If you delete the configuration, the settings of the 802.1X Plugin configuration defined in the **Default** tab are re-applied to the affected CounterACT device(s).

**Configure MAC Access Bypass**

Maintain the repository of MAC addresses of endpoints, which do not have a functioning 802.1X supplicant, and are being permitted to be authenticated by the CounterACT RADIUS Server using MAC address bypass (MAB).

For **endpoints that are listed in the MAC Address Repository (MAR)**, the CounterACT RADIUS server handles the MAB authentication of these endpoints. For **endpoints that require MAB authentication and are not listed in the MAR**, authentication is done 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, such 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 defined, pre-admission authorization rules, the NAS device determines the
authorization to impose on the endpoint. For information about pre-admission authorization rules, 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, 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 either add or edit the MAR entry. Possible methods are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manually by CounterACT Operator</strong>: CounterACT 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 Last Edited by method, Automatically Learned, displays in existing MAR entries until these entries are either 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>
<tr>
<td></td>
<td>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 defined, pre-admission authorization rules, the NAS device determines the authorization to impose on the endpoint.</td>
</tr>
</tbody>
</table>

In the MAR, enable/disable the option Accept MAB authentication for endpoints not defined in this repository. 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 with entries:

- Automatically Based on Policy Discoveries
- Manual Entries
- Import and Export MAR Entries
Automatically Based on Policy Discoveries

Create a policy that adds detected endpoints to the MAR or edits existing MAR entries.

1. Create a new policy or edit an existing policy.
2. Navigate to the policy action Manage > 802.1X Update MAR action.

   The action allows you to designate updates to MAR entries to be applied in either 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 both existing MAR entries and to new MAR entries

   For information about defining the 802.1X Update MAR action, see Actions.

Manual Entries

Manually add entries to the MAR.

1. Select Options from the Console 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. The Add MAR Entry dialog box opens.
4. In the Endpoint MAC Address field, provide the MAC address of an endpoint which authenticates by MAB.
5. The Last Edited By field is read-only and automatically populated by the plugin. 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 about defining authorization options, see the table provided in Rule Authorization.

8. Select OK.

Import and Export MAR Entries

You can both import MAR entries into and export MAR entries from the MAC Address Repository. Exporting MAR entries to a .csv file does not add any MAR entries.

To import MAR entries from a .csv file, select Import from the MAC Address Repository toolbar.
To export MAR entries to a .csv file, use any of the following methods:

- 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 of use.

- Right-click any MAR entry and select **Export Table** from the displayed dropdown menu.

Use the following 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>MAC Address</td>
<td>dot1x_mac</td>
<td>Required field column</td>
</tr>
<tr>
<td></td>
<td>Enter a MAC address. Information displays in MAR.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dot1x_auth_method</td>
<td>Required field column</td>
</tr>
<tr>
<td></td>
<td>Enter the text <strong>bypass</strong>. Information does not display in MAR.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By definition, all MAR entries authenticate using MAC authentication bypass (MAB).</td>
<td></td>
</tr>
<tr>
<td>Authorization</td>
<td>dot1x_target_access</td>
<td>Optional field column</td>
</tr>
<tr>
<td></td>
<td>Keep field entry blank.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>After successfully importing the .csv file into the MAR, add MAR entry authorizations, by doing either one of the following activities:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&gt; In the Console, manually add required MAR entry authorizations. See Manual Entries.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&gt; Contact ForeScout Customer Support for assistance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information displays in MAR.</td>
<td></td>
</tr>
</tbody>
</table>
### MAR Entry Field

<table>
<thead>
<tr>
<th>Field</th>
<th>CSV File Column Name</th>
<th>CSV File Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x_enforce_access</td>
<td>Keep field entry blank.</td>
<td></td>
</tr>
<tr>
<td>dot1x_last_assigned_access</td>
<td>Keep field entry blank.</td>
<td></td>
</tr>
<tr>
<td>Last Edited By</td>
<td>dot1x_approved_by</td>
<td>Required field column</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter the phrase <code>by_import</code>. Information displays in MAR.</td>
</tr>
<tr>
<td>MAR Comment</td>
<td>dot1x_mar_comment</td>
<td>Optional field column</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter any descriptive text. Information displays in MAR.</td>
</tr>
</tbody>
</table>

Sample `.csv` file for MAR import:

```
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dot1x_mac</td>
<td>dot1x_enh_pass_method</td>
<td>dot1x_target_access</td>
<td>dot1x_enforce_access</td>
<td>dot1x_last_assigned_access</td>
<td>dot1x_approved_by dot1x_mar_comment</td>
</tr>
<tr>
<td>2</td>
<td>0000FFFF000000000000000000000000</td>
<td>bypass</td>
<td>Message-a reply message</td>
<td>by_admin</td>
<td>comment</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1-254/255/3/1</td>
<td>bypass</td>
<td>reject-deny</td>
<td>by_admin</td>
<td>comment</td>
<td></td>
</tr>
</tbody>
</table>
```

### 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 perform any of the above actions, select **Apply** to save the modified MAC Address Repository.

### Testing and Troubleshooting

The section describes the test of the 802.1X Plugin and the plugin-provided 802.1X troubleshooting policy templates.

- **Test the Plugin**
- **Troubleshooting Policy Templates**

### Test the Plugin

The plugin test verifies the essential plugin operation required for a working authentication scenario. You can test a single CounterACT device or simultaneously test several CounterACT devices [Appliances, the Enterprise Manager]. Each authentication source [Microsoft Active Directory server, external RADIUS server] that is configured in the **Authentication Sources** tab is included in the plugin configuration test.

It is recommended to test the plugin configuration after initial configuration and after installing certificates.
For the CounterACT RADIUS server to authenticate using Microsoft Active Directory, the CounterACT device must be bound to (join) the domain. When the 802.1X Plugin is started or when its configuration is saved, the CounterACT device joins the relevant domain using the credentials that are defined in the User Directory Plugin. In order to verify that the CounterACT device successfully joined the domain, run the plugin configuration test.

**To run the test:**

1. Select the Plugins folder from the Options pane.
2. Select **802.1X** from the Plugins pane.
3. Select **Test**. The test is run and the Plugin Test window displays test results.

### Test Results

The following table describes the purpose of each test step performed when running the test of the plugin:

<table>
<thead>
<tr>
<th>Test Step</th>
<th>Sub-Step</th>
<th>Detail</th>
</tr>
</thead>
</table>
| 1. Test Configuration | 1.1: Test user directory with domain `<x>` and Domain Controller `<y>` | }
<table>
<thead>
<tr>
<th>Test Step</th>
<th>Sub-Step</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2: Test user directory with domain</td>
<td><strong>1.2.1</strong> Test kinit – verify ability to obtain a Kerberos ticket (internal component required to connect to Active Directory).&lt;br&gt;<strong>1.2.2</strong> Verify winbindd started – verify winbindd is properly running (required to bind and join to a domain). See Common Troubleshooting Issues for more information.</td>
<td></td>
</tr>
<tr>
<td>1.3: Test bundled FreeRADIUS daemon – verify that it is successfully running</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Test 802.1X Operability per Domain</td>
<td><strong>2.1:</strong> Test authentication in domain&lt;br&gt;<strong>2.2:</strong> Domain : Test authentication in domain</td>
<td><strong>2.2.1</strong> Test trust with domain controller - initial trust verification against the configured domain(s).&lt;br&gt;<strong>2.2.2</strong> Test authenticating Admin user (wbinfo) - Authentication verification with admin user configured in the User Directory plugin (winindd).&lt;br&gt;<strong>2.2.3</strong> Test authenticating Admin user (ntlm_auth) - Authentication verification with admin user credentials configured in User Directory plugin (ntlm_auth).&lt;br&gt;<strong>2.2.4</strong> Test authenticating Admin user (wbinfo) - Authentication verification with test user credentials configured in User Directory plugin test tab.</td>
</tr>
<tr>
<td>3. Test Certificates</td>
<td>Verifies server certificate is installed and valid. Make sure server certificate tab is properly configured and Root certificate is properly installed.</td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting Policy Templates**

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

- **Troubleshoot Rejected Authentications Policy Template**

It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Guide.

**Troubleshoot Rejected Authentications Policy Template**

You might want to identify the causes of rejected authentications. Use the **Troubleshoot Rejected Authentications** template to generate a policy that categorizes, by cause, rejected 802.1X authentications.
Endpoints are rejected by the RADIUS server due to any of the following reasons:

- Cannot authenticate endpoint identity (invalid credentials, invalid certificate, no MAR entry)
- A failure in the processing or communication of an authentication-related component, for example, the Active Directory server does not respond.
- Authorization denial (after being authenticated). A denial of access has any one of the following CounterACT 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 802.1X 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 CounterACT sources of authorization denial are defined and operating.

**Run the Template**

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

**To run the template:**

1. Select the **Policy** tab from the Console.

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

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

**Name the Policy**

The Name page lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

1. 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 will be 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.

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

3. Select **Next**. The Sub-Rules page 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.

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

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

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

**Troubleshoot Rejected Authentications Main Rule**

CounterACT-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 **NAC** tab > **Detections** pane > **All policies** tab.

**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.
Rejected endpoint authentications are inspected against each sub-rule in the order listed to determine their cause, as follows:

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

<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 on them by the RADIUS server.  
  A denial of access has any one of the following CounterACT sources:  
  - Policy action authorization  
  - MAR authorization  
  - Pre-Admission authorization rule |
| 2. Rejected by External RADIUS Server  | Endpoints matching this sub-rule had their authentication rejected by the external RADIUS server.  
  When CounterACT 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.  
  **CAUSE:** The endpoint MAC address was not listed in the MAC Address Repository (MAR) of the 802.1X Plugin. The MAR is the plugin’s warehouse of endpoints that authenticate using MAB. |
<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Invalid Credentials Supplied</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the RADIUS server.</td>
</tr>
<tr>
<td>CAUSE:</td>
<td>Either computer-supplied or user-supplied credentials did not match the credentials in the Active Directory of the domain.</td>
</tr>
<tr>
<td>5. Domain Controller Detected Error</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the CounterACT RADIUS server.</td>
</tr>
<tr>
<td>CAUSE:</td>
<td>The domain controller did not provide an adequate response to the RADIUS server.</td>
</tr>
<tr>
<td>6. Server Certificate Issuer Not Trusted</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the CounterACT RADIUS server.</td>
</tr>
<tr>
<td>CAUSE:</td>
<td>The endpoint supplicant did not trust the certificate authority that issued the RADIUS server's server certificate.</td>
</tr>
<tr>
<td>7. Client Certificate Issuer Not Trusted</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the CounterACT RADIUS server.</td>
</tr>
<tr>
<td>CAUSE:</td>
<td>The RADIUS server did not trust the certificate authority that issued the endpoint supplicant’s client certificate.</td>
</tr>
<tr>
<td>8. Client Issued TLS Alert</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the CounterACT RADIUS server.</td>
</tr>
<tr>
<td>CAUSE:</td>
<td>The endpoint supplicant stopped the TLS handshake with the RADIUS server. This might indicate that the server certificate is invalid.</td>
</tr>
<tr>
<td>9. Server Issued TLS Alert</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the CounterACT RADIUS server.</td>
</tr>
<tr>
<td>CAUSE:</td>
<td>The RADIUS server stopped the TLS handshake with the endpoint supplicant. This might indicate that the client certificate is invalid.</td>
</tr>
<tr>
<td>10. EAP Negotiation Failure</td>
<td>Endpoints matching this sub-rule had their authentication rejected by the CounterACT RADIUS server.</td>
</tr>
<tr>
<td>CAUSE:</td>
<td>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>
</tbody>
</table>
### 11. Other Rejections
Endpoints matching this sub-rule had their authentication rejected by the CounterACT RADIUS server.

**CAUSE:** The authentication stopped for a reason not matched by any of the preceding sub-rules.

---

**Technical Support**
When the plugin test fails, the test results describe the details of 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.

---

**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**
CounterACT policy conditions and properties let you instruct CounterACT how to detect endpoints authenticating via 802.1X. When adding or editing a policy rule, either 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 property folders supply the 802.1X properties that are available for use in policy conditions:

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

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

### Authentication Decision

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.1X Authenticating Appliance</strong></td>
<td>The IP address of the appliance performing the authentication.</td>
</tr>
<tr>
<td><strong>802.1X Last Authentication State - Computer Credentials</strong></td>
<td>The result of the last authentication attempt made by the endpoint using computer credentials.</td>
</tr>
<tr>
<td>• <strong>RADIUS-Accepted</strong> – The RADIUS server successfully authenticated the endpoint.</td>
<td></td>
</tr>
<tr>
<td>• <strong>RADIUS-Rejected</strong> – The endpoint failed to authenticate with the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td><strong>802.1X Last Authentication State - MAC Based</strong></td>
<td>The result of the last authentication attempt made by the endpoint using its MAC address (MAB).</td>
</tr>
<tr>
<td>• <strong>RADIUS-Accepted</strong> – The RADIUS server successfully authenticated the endpoint.</td>
<td></td>
</tr>
<tr>
<td>• <strong>RADIUS-Rejected</strong> – The endpoint failed to authenticate with the RADIUS server.</td>
<td></td>
</tr>
</tbody>
</table>
### 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 - either Accept or Reject. Note that the final reply might be different, due to any imposed authorization.

### Authentication Details

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| **802.1X Authenticated Entity** | What entity was authenticated:
- **User** – **Authenticated** using user credentials
- **Computer** – **Authenticated** using computer credentials

  *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 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 802.1X Plugin.
| **802.1X EAP Type** | Identifies the selected **EAP Type** in the last authentication.
| **802.1X Host Name** | The **User-Name**, RADIUS attribute (1), used in last authentication request, when computer credentials are used to authenticate.
| **802.1X Requested Domain** | The domain that an endpoint requested to be used for 802.1X authentication.
| **802.1X User Name** | The **User-Name**, RADIUS attribute (1), used in last authentication request.
### Authentication Events

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

### Authorization

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

### Client Certificate

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Client Cert Alternate Subject</td>
<td>Alternate Subject of the Client Certificate.</td>
</tr>
<tr>
<td>802.1X Client Cert commonName</td>
<td>Common-Name of the Client Certificate.</td>
</tr>
<tr>
<td>802.1X Client Cert Expiration</td>
<td>Expiration of the Client Certificate.</td>
</tr>
<tr>
<td>802.1X Client Cert Issuer</td>
<td>Issuer of the Client Certificate.</td>
</tr>
<tr>
<td>802.1X Client Cert Serial</td>
<td>Serial of the Client Certificate.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>802.1X Client Cert Subject</strong></td>
<td>Subject of the Client Certificate.</td>
</tr>
</tbody>
</table>

### MAR

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

### NAS Device

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.1X Called Station ID</strong></td>
<td>The <strong>Called-Station-ID</strong>, RADIUS attribute (30), used on the last authentication request.</td>
</tr>
<tr>
<td><strong>802.1X Endpoint SSID</strong></td>
<td>The <strong>WLAN SSID</strong> used in the 802.1X authentication.</td>
</tr>
<tr>
<td><strong>802.1X NAS IP Address</strong></td>
<td>The <strong>802.1X NAS-IP-Address</strong>, RADIUS attribute (4), as appears in the RADIUS Request (IP of the switch or the WiFi AP/Controller).</td>
</tr>
<tr>
<td><strong>802.1X NAS Port Number</strong></td>
<td>The <strong>NAS-port</strong>, RADIUS attribute (5), as reported in RADIUS Request. This RADIUS attribute contains the port number of the switch, if available. Since wireless access points do not have physical ports, a unique <strong>association ID</strong> 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, then the <strong>NAS-port</strong> attribute contains the association ID, which is a 16 bit, unsigned integer.</td>
</tr>
<tr>
<td><strong>802.1X NAS Port Type</strong></td>
<td>The <strong>NAS-port-type</strong>, RADIUS attribute (61), as appears in RADIUS Request. Supported port types are:</td>
</tr>
<tr>
<td></td>
<td>• Ethernet LAN</td>
</tr>
<tr>
<td></td>
<td>• Wireless LAN</td>
</tr>
</tbody>
</table>

### Windows 7 Supplicant

<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 user to authorize new servers or trusted certification authorities.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</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:  
|                                      | • Quick roaming between wireless access points                              |
| Enable IEEE 802.1X authentication    | Enable IEEE 802.1X authentication.                                          |
| Encryption type                      | Supported encryption types are:                                             |
|                                      | • AES                                                                       |
|                                      | • TKIP                                                                      |
|                                      | • WEP                                                                       |
|                                      | • None                                                                      |
| Fallback to unauthorized network access | Fallback to unauthorized network access.                                   |
| Network authentication method        | Network authentication method.                                              |
| Remember user credentials for this connection for each logon | Remember user credentials for this connection for each log in               |
| Security Type                        | Supported security types are:                                              |
|                                      | • 802.1X                                                                    |
|                                      | • No authentication (Open)                                                  |
|                                      | • Shared                                                                   |
|                                      | • WPA-Enterprise                                                           |
|                                      | • WPA-Personal                                                             |
|                                      | • WPA-2 Enterprise                                                          |
|                                      | • WPA-2 Personal                                                            |
| Use simple certificate selection     | Use simple certificate selection.                                          |
| Validate server certificate          | Validate server certificate.                                               |

Create Custom Policies

It is recommended to tailor the policies you create using the 802.1X policy templates, to address your organization's unique authentication/authorization needs. However, 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 802.1X Plugin is installed. For a description of the available actions, see Actions.

To create a policy:

1. Log in to the CounterACT 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 CounterACT.

![Image of IP Address Range dialog box]

*The Unknown IP addresses option is available with CounterACT version 7.0.0. Refer to CounterACT 7.0.0 Online Help for more information.*

**Actions**

The plugin provides the following actions for application on detected endpoints:

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

**802.1X Authorize Action**

Use the 802.1X Authorize action to define the authorization to be imposed on authenticated endpoints by the CounterACT RADIUS server.
An applied 802.1X Authorize action can be cancelled. When cancelling this action, the 802.1X 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 CounterACT sources:

1. Policy action authorization - if available, first preference to impose
2. MAR authorization - if available, second preference to impose
3. Pre-admission authorization rule - third preference to impose. The CounterACT RADIUS server evaluates pre-admission authorization rules when no other CounterACT source - not policy action, not 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 CounterACT 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.

Policies you create using either the Endpoint Authorization Policy Template or the Centralized Web Authentication Policy Template include sub-rules that apply the 802.1X Authorize action to evaluated endpoints found to match the sub-rule. It is recommended to tailor the authorization defined in each policy sub-rule 802.1X Authorize action, to address your organization's unique authorization needs.

To define authorization in the action:

1. If defining the action in a policy, do the following:
   a. In the Console Policy tab, select a policy and select Edit.
   b. Select either 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 802.1X Authorize action. The action's Parameters tab opens.
   e. Continue with step 3.

2. If manually invoking the action on detected endpoints, do the following:
   a. In the Detections pane of the NAC tab, right-click one or more selected endpoint entries.
   b. In the displayed menu, navigate to Restrict and select the 802.1X 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 the table provided in 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.

**Cancelling the 802.1.X Authorization Action**

Cancelling the 802.1X Authorize action removes the authorization applied by the action and allows authorization to be applied as provided from the hierarchy of CounterACT 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 CounterACT 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 either add new entries to the MAC Address Repository (MAR) or edit existing entries in the MAR. As is standard for all CounterACT 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).
The action allows you to designate updates to MAR entries to be applied in either 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 MAR entries and to 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 either add or edit the MAR entry. Possible methods are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Manually by CounterACT Operator:</strong> CounterACT 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>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. 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 defined, 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. If defining the action in a policy, do the following:
   a. In the Console Policy tab, select a policy and select Edit.
   b. Select either 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. If manually invoking the action on detected endpoints, do the following:
   a. In the Detections pane of the NAC tab, 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><strong>Deny Access</strong></td>
<td>For details about defining authorization options, see the table provided in <a href="#">Rule Authorization</a>.</td>
</tr>
<tr>
<td><strong>VLAN</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Attribute-Value Pair</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Apply authorization settings to new entries only</strong></td>
<td>Selecting this option instructs the CounterACT RADIUS server to impose the action's defined authorization only on MAR entries being added. If option is not selected, the action's defined authorization is imposed on both added and existing MAR entries being edited.</td>
</tr>
<tr>
<td><strong>MAR Comment</strong></td>
<td>Descriptive comment about the endpoint.</td>
</tr>
<tr>
<td><strong>Apply comment to new entries only</strong></td>
<td>Selecting this option instructs the plugin to record the specified MAR Comment only in MAR entries being added. If option is not selected, the specified MAR Comment is recorded in both added and existing MAR entries being edited.</td>
</tr>
<tr>
<td><strong>Initiate endpoint re-authentication</strong></td>
<td>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 any of the other defined information/setting updates, defined in the action's Parameters tab. When used in combination with any of the other defined information/setting updates, re-authentication of an endpoint is only initiated following success of the defined, update MAR entry processing.</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.

Use Cases

This section presents information about the following plugin use cases:

- Categorize Endpoint Authorizations
- Monitor Successful Authentications and ApplyAuthorizations
- Corporate Wired and Wireless Authentication
- Centralized Web Authentication
- EDU-ROAM
- MAC Address Bypass
Categorize Endpoint Authorizations

Read this section if you want to:

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

Possible CounterACT 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 CounterACT 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 you create, using the Authorization Source 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 802.1X 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.

Run the Template

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

To run the template:

1. Select the Policy tab from the Console.


3. In the navigation tree, select 802.1X > 802.1X Enforcement and then select Authorization Source.
4. Select Next. The Name page opens.

**Name the Policy**

The Name page lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

1. 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 will be 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.

2. Select **Next**. The Scope page and the IP Address Range dialog box open.

### Define which Endpoints are Inspected - Policy Scope

The Scope Page and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.

1. Specify the scope of the policy. The following options are available:
   - **All IPs**: Include all addresses in the Internal Network range.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close IP Address Range dialog box, and select **Segments** from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Select this option to include endpoints for which the IP address is not known.

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

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

3. Select **Finish**. The policy is created.
Authorization Source Main Rule
CounterACT-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 CounterACT source of endpoint authorization. Authorization is imposed on successfully authenticated endpoints.

By default, policy sub-rules do not include any action to be applied.

Endpoints 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 802.1X Authorize action; application of this action could have been due to either policy evaluation or manually initiated by the CounterACT user.</td>
</tr>
</tbody>
</table>
### Sub-Rule Name | Description
---|---
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 defined, 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 defined, 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 CounterACT 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 802.1X Plugin is running and 802.1X endpoint authentication is operating in the organization's network.

**Run the Template**

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

**To run the template:**

1. Select the **Policy** tab from the Console.
2. Select **Add**. The Policy Wizard opens.
3. In the navigation tree, select **802.1X > 802.1X Enforcement** and then select **Endpoint Authorization**.
4. Select Next. The Name page opens.

Name the Policy

The Name page lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

1. 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 will be 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.

2. Select Next. The Endpoint Authentication Methods page opens.

Categorize Successful Authentications by Endpoint Authentication Method

The Endpoint Authentication Methods page 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.

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

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

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

   - **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 created policy still identifies successful authentications (accepted by the RADIUS server) but does not categorize them according to the method used to authenticate the endpoint.

2. Select Next. The Sub-Rules page opens and lists the default sub-rules of the policy generated by the template. Sub-rules can be modified at this point if required.
3. 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**

CounterACT-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>
</table>
| **1. MAC Bypass** | 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 802.1X Plugin. The MAR is the plugin's warehouse of endpoints that authenticate using MAC address bypass (MAB).

If the **802.1X 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. |
<table>
<thead>
<tr>
<th>Sub-Rule Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Accepted by Computer Certificate</td>
<td>Endpoints matching this sub-rule had their authentication accepted by the RADIUS server given the following conditions:</td>
</tr>
<tr>
<td></td>
<td>- A machine certificate was presented by the endpoint</td>
</tr>
<tr>
<td></td>
<td>- The network authentication method of the endpoint supplicant was <strong>EAP-TLS</strong></td>
</tr>
<tr>
<td></td>
<td>If the <strong>802.1X Authorize</strong> 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>3. Accepted by a Certificate</td>
<td>Endpoints matching this sub-rule had their authentication accepted by the RADIUS server given the following conditions:</td>
</tr>
<tr>
<td></td>
<td>- A client certificate (issued either to the machine or to the user) was presented by the endpoint.</td>
</tr>
<tr>
<td></td>
<td>- The network authentication method of the endpoint supplicant was <strong>EAP-TLS</strong></td>
</tr>
<tr>
<td></td>
<td>If the <strong>802.1X Authorize</strong> 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>4. Accepted by Computer Authentication</td>
<td>Endpoints matching this sub-rule had their authentication accepted by the RADIUS server given the following condition:</td>
</tr>
<tr>
<td></td>
<td>- Either computer-supplied credentials or a machine certificate was used to authenticate the endpoint.</td>
</tr>
<tr>
<td></td>
<td>If the <strong>802.1X Authorize</strong> 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>5. Accepted</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If the <strong>802.1X Authorize</strong> 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>
</tbody>
</table>

The authorization options that can be defined in the **802.1X 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 scenario(s) you want to address using the 802.1X Plugin. For details, see Environment Readiness.

The 802.1X Plugin can be configured to interoperate with any of the following authentication sources:

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

**Single Domain**

When the 802.1X 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:

- Add an organizational domain as the authentication source; the available domains from which to select 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.
- 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 request against this source. RADIUS access request 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

When the 802.1X 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 from which to select 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 those 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 those RADIUS access requests that do not contain a domain.

For details, see [Configure Authentication Sources](#).

**Pre-Admission Authorization in a Multi-Domain Environment**

The following are several examples of pre-admission authorization rules that a CounterACT user might configure, when the 802.1X Plugin (the CounterACT RADIUS server) operates in a multi-domain environment. For details, see [Configure Pre-Admission Authorization](#).
- 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.
- Authenticate the endpoints of users with no domain against domain *PM_DC* and assign the authenticated endpoints to VLAN 40 (authorization).

In the Edit Pre-Admission Criterion window above, use of the regular expression ^[\^&\]\}* in the **Expression** field evaluates the content of the selected attribute **User-Name** to ensure that **User-Name** does not contain the @ (ampersand) character and does not contain the \ (backslash) character.
The resulting **Pre-Admission Authorization** tab display, given the configured pre-admission authorization rule examples:

![CounterACT Devices](image)

### CounterACT RADIUS Server as a Proxy

When the 802.1X 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 from which to select 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 as provided either by pre-admission authorization rule or by CounterACT policy (the 802.1X Authorize action), always replaces an external RADIUS server-provided endpoint authorization.

### Centralized Web Authentication

Centralized web authentication is a method that 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). CounterACT centralized web authentication combines the use of both MAC authentication, provided by the 802.1X Plugin, and CounterACT policy actions to authenticate endpoints.

CounterACT centralized web authentication delivers enhanced CounterACT guest management responsiveness; this enhanced CounterACT guest management responsiveness is entirely provided by the 802.1X Plugin.

As of 802.1X Plugin version 4.2.0, IP-MAC visibility is provided solely by the plugin.
Deploy CounterACT 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 option **Accept MAB authentication for endpoints not defined in this repository**. Selecting this option instructs the 802.1X Plugin to use MAC address bypass (MAB) to authenticate MAC addresses, received in RADIUS requests, that are not listed in the MAR. For detail, 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 detail, see [Configure Pre-Admission Authorization](#).

Also for the rule, define the following rule authorization (attribute-value pair assignments) that the CounterACT RADIUS server imposes on authenticated endpoints found to match the rule condition:

- **Cisco Attribute-Value Pairs for Rule Authorization**
- **Meraki Attribute-Value Pair for Rule Authorization**

#### 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><code>url-redirect-acl=enforce the ACL name that is configured on the WLAN device</code></td>
</tr>
</tbody>
</table>
## Vendor Attribute-Value Pair for Rule Authorization

The following table presents the Meraki attribute-value (A-V) pair 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>Meraki</td>
<td>Cisco-AVPair</td>
<td>url-redirect= http://${appliance_address}/captiveredirect/a?t=${client_token}</td>
</tr>
</tbody>
</table>

- When CounterACT is running Service Pack 3.0.0 or above:
  During expression evaluation, `{appliance_address}` is dynamically replaced with the FQDN of the CounterACT Appliance. This dynamic replacement requires that the option **Attempt to redirect using DNS name** is enabled on the Appliance (Options > NAC > HTTP Redirection > HTTP Redirection Settings).
- When CounterACT is running a Service Pack below 3.0.0:
  During expression evaluation, `{appliance_address}` is dynamically replaced with the IP address of the CounterACT Appliance.

### 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 also the authenticating Appliance, then, in the **Walled Garden** field, define the managing Appliance’s IP address. Doing so enables the configured network device to also 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

Run the Template

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

To run the template:

1. Select the Policy tab from the Console.


3. In the navigation tree, select 802.1X > RADIUS and then select Centralized Web Authentication.
4. Select Next. The Name page opens.

**Name the Policy**

The Name page lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

1. 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 will be 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.

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

**Define which Endpoints are Inspected - Policy Scope**

The Scope page and IP Address Range dialog box let you define the range of endpoints to be inspected for this policy.

![IP Address Range Dialog Box]

When defining the policy scope, a best practice is to select the **Unknown IP addresses** option 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 CounterACT.
1. Specify the scope of the policy. The following *IP address* options are available:
   - **All IPs**: Include all addresses in the Internal Network range.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK to close IP Address Range dialog box, and select **Segments** from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Select this option to include endpoints for which the IP address is not known.

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

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

3. Select **Next**. The Main Rule page opens

**Define SSID for Centralized Web Authentication Main Rule**

CounterACT-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 page, 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.

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

5. Select Finish. The policy is created.

**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>
<tbody>
<tr>
<td><strong>1. Signed In as Corporate User</strong></td>
<td>Endpoints matching this sub-rule meet all of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>▪ Within the last <code>&lt;configurable number of&gt;</code> days, the <code>HTTP Login</code> action accepted the user's log in to the organization's network and authenticated the endpoint as an organization member</td>
</tr>
<tr>
<td></td>
<td>▪ The most recent authorization imposed on the endpoint by the CounterACT RADIUS server was <strong>NOT</strong> redirection of the endpoint to CounterACT captive portal for handling.</td>
</tr>
<tr>
<td></td>
<td>CounterACT applies the <code>802.1X Authorize</code> action on endpoints matching this sub-rule. For detail, see <a href="#">Actions</a>.</td>
</tr>
<tr>
<td><strong>2. Signed In as Guest</strong></td>
<td>Endpoints matching this sub-rule meet all of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>▪ Within the last <code>&lt;configurable number of&gt;</code> days, the <code>HTTP Login</code> action accepted the user's log in to the organization's network and authenticated the endpoint as a guest</td>
</tr>
<tr>
<td></td>
<td>▪ The most recent authorization imposed on the endpoint by the CounterACT RADIUS server was <strong>NOT</strong> redirection of the endpoint to CounterACT captive portal for handling.</td>
</tr>
<tr>
<td></td>
<td>CounterACT applies the <code>802.1X Authorize</code> action on endpoints matching this sub-rule. For detail, see <a href="#">Actions</a>.</td>
</tr>
<tr>
<td>Sub-Rule Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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 log in to the organization's network and authenticated the endpoint as either 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.  
  CounterACT applies the 802.1X Authorize action on endpoints matching this sub-rule. For detail, 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 CounterACT captive portal for handling.  
  Matching endpoints are no longer logged in to the organization's network as either a member of the corporate organization or as a guest. These endpoints must undergo centralized web authentication.  
  CounterACT applies the 802.1X Authorize action on endpoints matching this sub-rule to redirect these users to the CounterACT captive portal. For detail, 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.  
  Following this sub-rule treatment, endpoints, when next evaluated by this policy, will match sub-rule 5. |
| 5. Pending Log In | Endpoints matching this sub-rule did not match any of the preceding sub-rules.  
  CounterACT applies the HTTP Login action on endpoints matching this sub-rule following their re-direction to allow these users to log in again to the organization's network.  
  For detail about the HTTP Login action, reference the User Directory Plugin Configuration 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 802.1X Plugin configuration guidelines:

**Authentication Sources**

In the Authentication Sources tab, choose the relevant entries and configure 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

[Image of Local Endpoint Authorization window]

- SSID
  - Matches: Expression (description)
Pre-Admission Authorization Tab Rule Display
MAC Address Bypass

To allow endpoint network authentication using only their 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 the table provided in Rule Authorization.

In the 802.1X 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.

Advanced Topics

This section presents information about the following advanced topics:

- Authentication-Authorization Processing Flow
- Re-Authentication Methods
- Plugin Redundancy and Failover
- Troubleshooting
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 CounterACT sources:

1. Policy action authorization - if available, first preference to impose
   - **Exception**: When an endpoint attempts its initial admission to an organization's network (CounterACT 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 to impose
3. Pre-admission authorization rule - third preference to impose. The CounterACT RADIUS server evaluates pre-admission authorization rules when no other CounterACT source - not policy action, not 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 (CounterACT has not yet detected the endpoint).

When none of the above CounterACT 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 802.1X 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>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;1.0.8802.1.1.1.1.1.2.1.5&quot; + port index</td>
<td>4</td>
</tr>
<tr>
<td>Aironet De-authentication</td>
<td>SNMP</td>
<td>WLAN</td>
<td>Cisco/Aironet</td>
<td>MIB = &quot;1.3.6.1.4.1.1417 9.2.1.4.1.22&quot;</td>
<td>5</td>
</tr>
<tr>
<td>Xirrus De-authentication</td>
<td>SNMP</td>
<td>WLAN</td>
<td>Xirrus</td>
<td>MIB = &quot;1.3.6.1.4.1.2101 3.1.2.22.3.0&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 to your operational environment, contact your ForeScout representative.*
Plugin Redundancy and Failover

This section provides an overview of the internal redundancy mechanism of the 802.1X 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 that 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 CounterACT infrastructure sends this action to the group of capable Appliances per the relevant controller. As with any action, the CounterACT 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 processing point, the managing Appliance, manages endpoint re-authentication, as follows:

1. The 802.1X 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 will issue the re-authentication request.
3. If no capable device is available other than the authenticating Appliance and the authenticating Appliance is out of service, then 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 approach troubleshooting certain common plugin issues that are associated with a CounterACT machine failing to join a domain. The issues described are:

- User Directory Plugin Incorrectly Configured
- Winbindd Dead

**CounterACT Machine Fails to Join Domain**

**User Directory Plugin Incorrectly Configured**

Review [User Directory Readiness](#).

**Winbindd Dead**

When encountering a situation in which `winbindd` is either not running or not properly running, do the following:

- Verify that CounterACT 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 CounterACT installation). If not configured, run the following `fstool` command `ntp` to point to the proper IP address:
  ```bash
  fstool ntp <server ip>
  ```
- In User Directory Plugin, check both `alias` and `child` domain configuration. See [User Directory Readiness](#).
In many situations, 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:

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

**Supplicant on Windows 7/Windows XP Endpoints**

This section provides an overview about how to configure a supplicant on endpoints running either 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 window opens and displays the Networking tab.
3. In the tab, right-click and select the properties of the LAN card connected to the switch.
4. Select the **Authentication** tab.
5. In the tab, configure the following:
   a. Select the **Enable IEEE 802.1X authentication** option to start the supplicant or clear this option to stop the supplicant.
   b. From the **Choose a network authentication method** drop-down menu, select the **Microsoft: Protected EAP (PEAP)** method.
   c. When using manually entered credentials, select the **Remember my credentials for this connection each time I’m logged on** option. 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. Select the **Fallback to unauthorized network access** option, if a 802.1X supplicant is connected to a non-802.1X port.
   e. In the tab, select **Settings**. The Protected EAP Properties dialog box opens.

![Protected EAP Properties Dialog Box]

6. In the 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 **Install Certificates**.
c. Select the **Do not prompt user to authorize new servers or trusted certification authorities** option to disable the following event prompt: When encountering an unknown certificate, the supplicant might present a dialog box that allows the user to manually trust a certificate from an unknown source.

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 the **Enable fast reconnect** option.

**Supplicant on MAC Endpoints**

Supplicant on MAC endpoints are automatically configured when these endpoints attempt to access an 802.1X-restricted network.
Additional CounterACT Documentation

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

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

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

To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal

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

To access the Customer Support Portal:
2. Select the CounterACT version you want to discover.
**CounterACT Console Online Help Tools**

Access information directly from the CounterACT Console.

**Console Help Buttons**

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

**Console User Manual**

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

**Plugin Help Files**

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

**Documentation Portal**

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

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is another valid written agreement executed by you and ForeScout that governs the ForeScout products and services:

- If you have purchased any ForeScout products or services, your use of such products or services is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-07-23 14:53