ForeScout

ForeScout CounterACT®

Authentication Module: RADIUS Plugin

Configuration Guide

Version 4.3

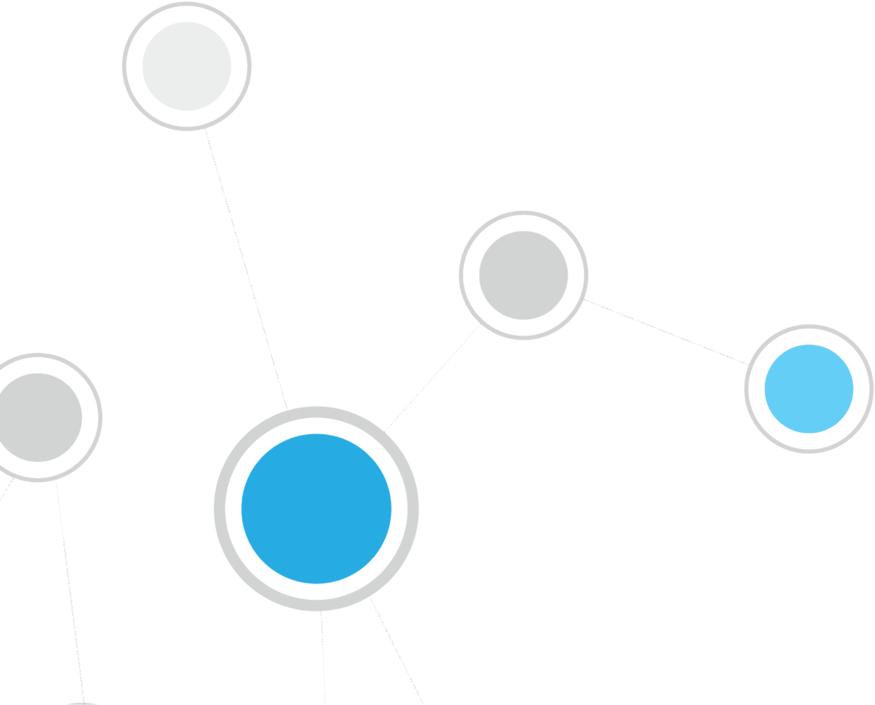


Table of Contents

Overview

This section provides an overview of the following topics:

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

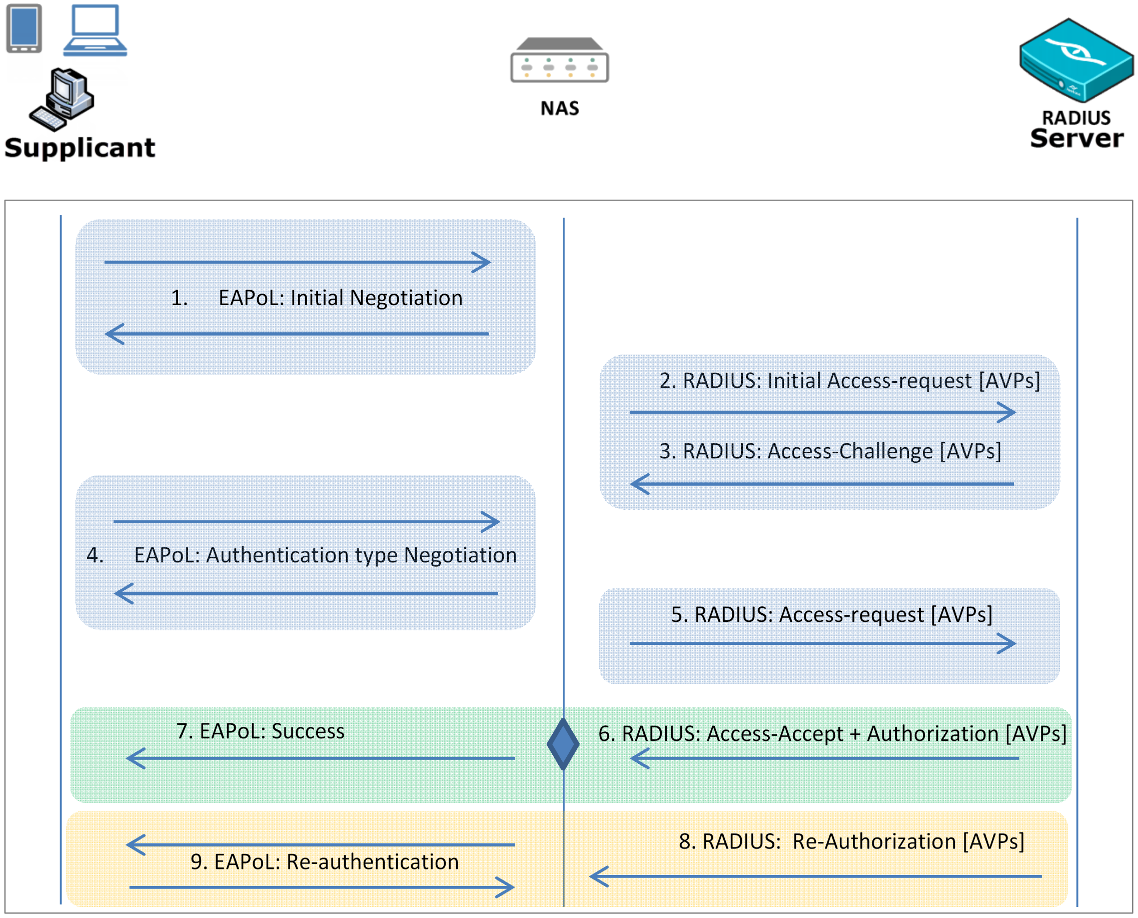
Understanding the 802.1X Protocol

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. The organization's security requirements require these endpoints to undergo authentication and be evaluated as authenticated, as follows:
  - 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), located 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

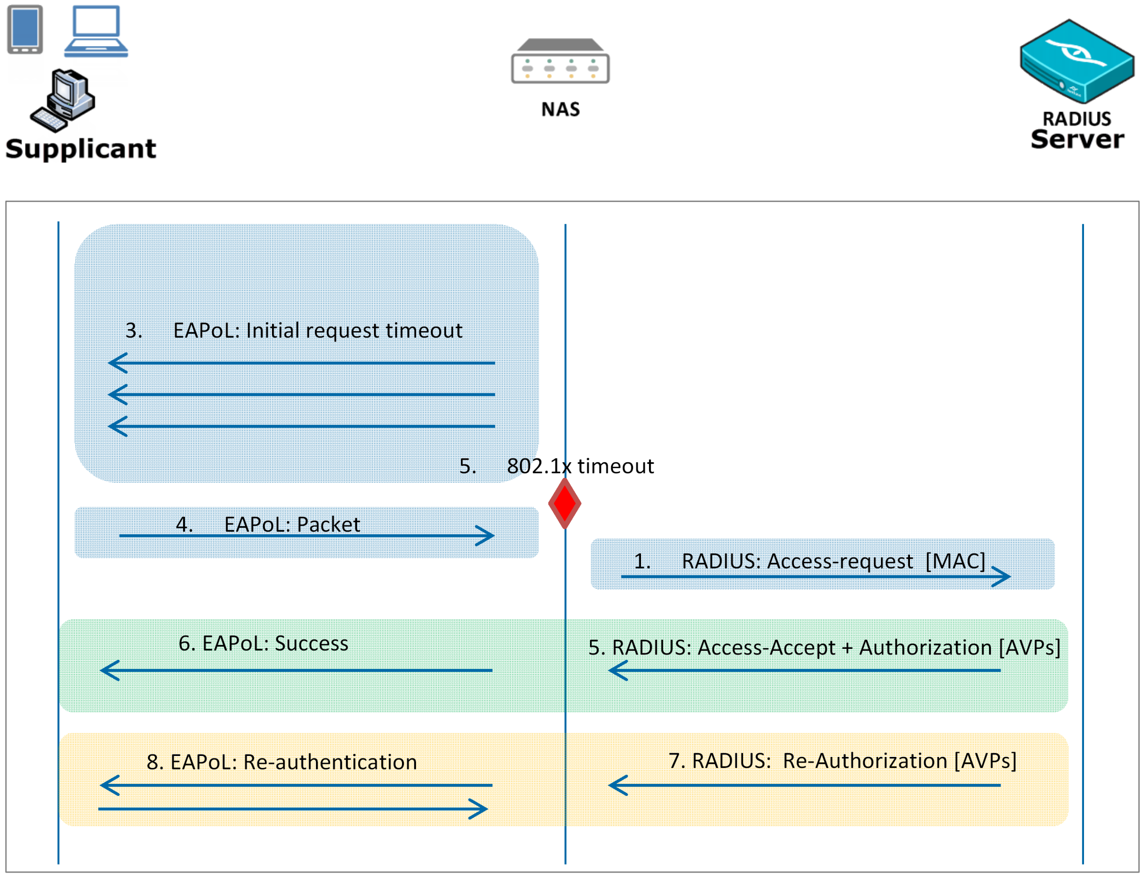
The following diagram provides a high-level view of the 802.1X processing sequence for endpoints having a supplicant:


Supplicant
NAS
RADIUS Server
1. EAPoL: Initial Negotiation
2. RADIUS: Initial Access-request [AVPs]
3. RADIUS: Access-Challenge [AVPs]
4. EAPoL: Authentication type Negotiation
5. RADIUS: Access-request [AVPs]
6. RADIUS: Access-Accept + Authorization [AVPs]
7. EAPoL: Success
8. RADIUS: Re-Authorization [AVPs]
9. EAPoL: Re-authentication

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:


Supplicant
NAS
RADIUS Server
3. EAPoL: Initial request timeout
5. 802.1x timeout
4. EAPoL: Packet
1. RADIUS: Access-request [MAC]
6. EAPoL: Success
5. RADIUS: Access-Accept + Authorization [AVPs]
8. EAPoL: Re-authentication
7. RADIUS: Re-Authorization [AVPs]

About the CounterACT RADIUS Plugin

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

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

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

The RADIUS Plugin enables 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.

IPv6 Support

The RADIUS Plugin provides IPv6 support for purposes of performing endpoint authentication, authorization and guest centralized web authentication (CWA). The plugin handles the IPv6 addresses of NAS devices (switches, WLAN devices), Microsoft domain controllers and external RADIUS servers with which it must interface. For information about overall CounterACT IPv6-related support, refer to the *CounterACT 8.0 Release Notes*. See Additional CounterACT Documentation for information on how to access this document.

About This Document

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

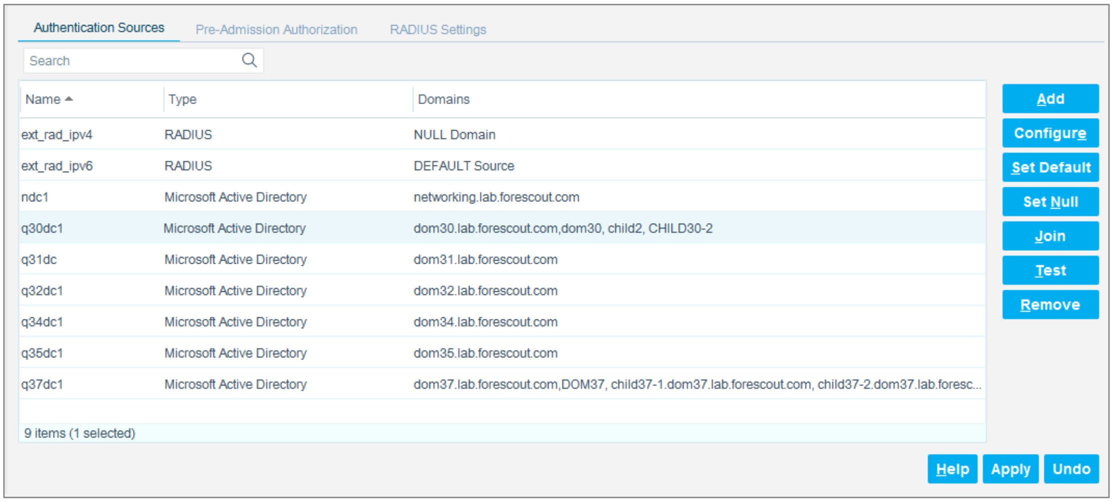
RADIUS Plugin Components

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

- Authentication Sources
- Pre-Admission Authorization
- 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.

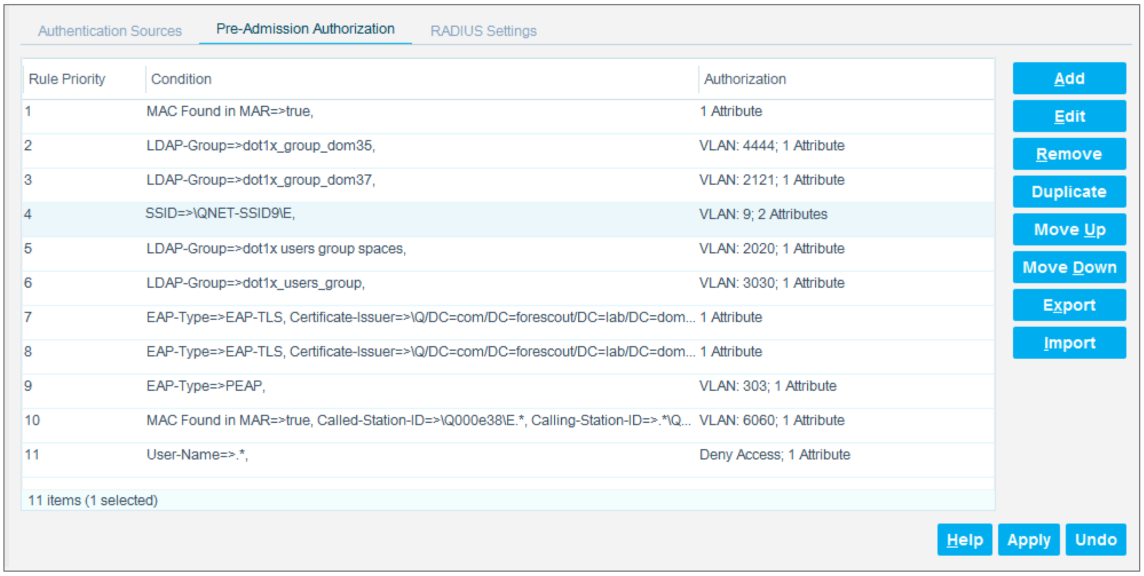


Name ▲	Type	Domains
ext_rad_ipv4	RADIUS	NULL Domain
ext_rad_ipv6	RADIUS	DEFAULT Source
ndc1	Microsoft Active Directory	networking.lab.forescout.com
q30dc1	Microsoft Active Directory	dom30.lab.forescout.com,dom30, child2, CHILD30-2
q31dc	Microsoft Active Directory	dom31.lab.forescout.com
q32dc1	Microsoft Active Directory	dom32.lab.forescout.com
q34dc1	Microsoft Active Directory	dom34.lab.forescout.com
q35dc1	Microsoft Active Directory	dom35.lab.forescout.com
q37dc1	Microsoft Active Directory	dom37.lab.forescout.com,DOM37, child37-1.dom37.lab.forescout.com, child37-2.dom37.lab.foresc...

9 items (1 selected)

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.

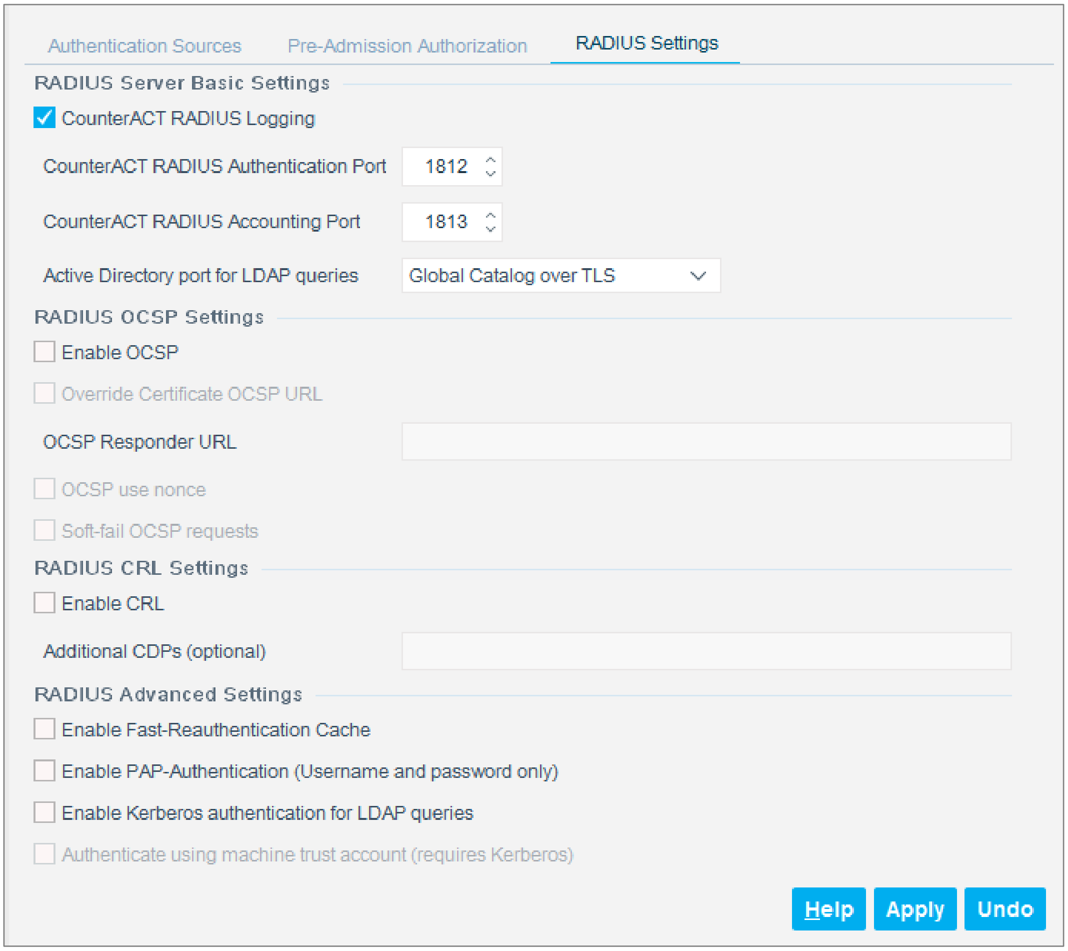


Rule Priority	Condition	Authorization
1	MAC Found in MAR=>true,	1 Attribute
2	LDAP-Group=>dot1x_group_dom35,	VLAN: 4444; 1 Attribute
3	LDAP-Group=>dot1x_group_dom37,	VLAN: 2121; 1 Attribute
4	SSID=>\QNET-SSID9\E,	VLAN: 9; 2 Attributes
5	LDAP-Group=>dot1x users group spaces,	VLAN: 2020; 1 Attribute
6	LDAP-Group=>dot1x_users_group,	VLAN: 3030; 1 Attribute
7	EAP-Type=>EAP-TLS, Certificate-Issuer=>\Q/DC=com/DC=forescout/DC=lab/DC=dom...	1 Attribute
8	EAP-Type=>EAP-TLS, Certificate-Issuer=>\Q/DC=com/DC=forescout/DC=lab/DC=dom...	1 Attribute
9	EAP-Type=>PEAP,	VLAN: 303; 1 Attribute
10	MAC Found in MAR=>true, Called-Station-ID=>\Q000e38\E.*, Calling-Station-ID=>.*\Q...	VLAN: 6060; 1 Attribute
11	User-Name=>.*,	Deny Access; 1 Attribute

11 items (1 selected)

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 as the authenticating RADIUS server or not, it ***always handles*** the ***authorization*** of authenticated endpoints.



RADIUS Server Basic Settings

☑ CounterACT RADIUS Logging

CounterACT RADIUS Authentication Port: 1812

CounterACT RADIUS Accounting Port: 1813

Active Directory port for LDAP queries: Global Catalog over TLS

RADIUS OCSP Settings

☐ Enable OCSP

☐ Override Certificate OCSP URL

OCSP Responder URL:

☐ OCSP use nonce

☐ Soft-fail OCSP requests

RADIUS CRL Settings

☐ Enable CRL

Additional CDPs (optional):

RADIUS Advanced Settings

☐ Enable Fast-Reauthentication Cache

☐ Enable PAP-Authentication (Username and password only)

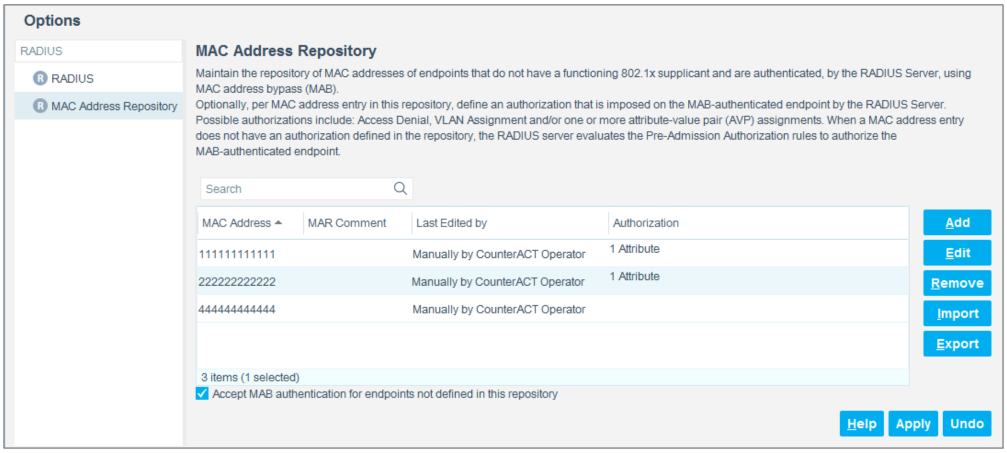
☐ Enable Kerberos authentication for LDAP queries

☐ Authenticate using machine trust account (requires Kerberos)

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.



MAC Address Repository

Maintain the repository of MAC addresses of endpoints that do not have a functioning 802.1x supplicant and are authenticated, by the 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 RADIUS Server. Possible authorizations include: Access Denial, 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 RADIUS server evaluates the Pre-Admission Authorization rules to authorize the MAB-authenticated endpoint.

MAC Address	MAR Comment	Last Edited by	Authorization
111111111111		Manually by CounterACT Operator	1 Attribute
222222222222		Manually by CounterACT Operator	1 Attribute
444444444444		Manually by CounterACT Operator	

3 items (1 selected)

☑ Accept MAB authentication for endpoints not defined in this repository

Supported Authentication Protocols

The RADIUS Plugin supports use of the following authentication protocols:

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

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

CounterACT Requirements

The section describes CounterACT requirements for this release.

- CounterACT version 8.0
- Network Module version 1.0 with the following components running:
  - Switch Plugin - for wired network RADIUS-based deployment
  - Wireless Plugin - for wireless network RADIUS-based deployment
- Authentication Module version 1.0 with the User Directory Plugin running - for authentication-authorization against Microsoft Active Directory and external RADIUS.
- An active Maintenance Contract for CounterACT devices is required

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 RADIUS Plugin, see Use Cases.

This section presents the following topics:

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

Certificate Readiness

Certificate management in CounterACT is accomplished using the Console certificates interface (**Options** > **Certificates**). Certificates serve either one of the following functions:

- System Certificate
- Trusted Certificate

You have the following flexibility when defining and provisioning certificates:

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

System Certificate

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

🗎 *When you generate the certificate signing request (CSR), remember that you are generating the CSR for the RADIUS Plugin (the CounterACT RADIUS server) and you must designate the certificate's use to be either for all Appliances or for a specific Appliance.*

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

Trusted Certificate

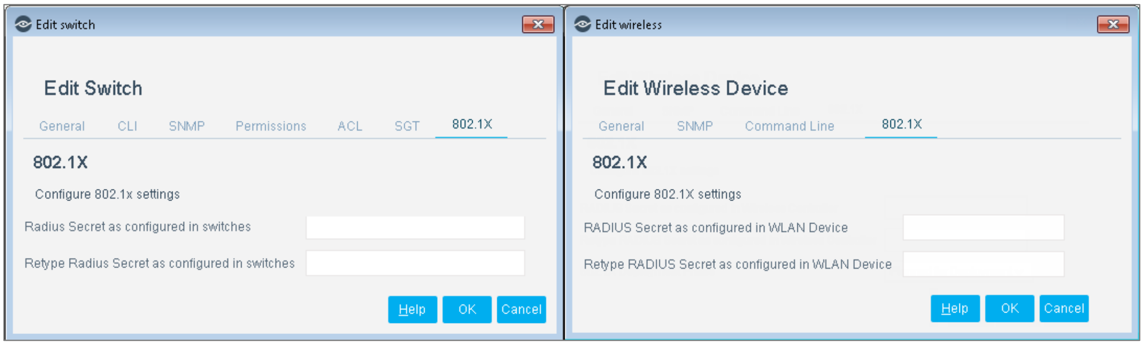
Use the certificate interface (**Options** > **Certificates > Trusted Certificates**) to configure certificate authority trust chains that are used by the RADIUS Plugin to authenticate external network endpoints.

Network Device Readiness

Configure NAS devices:

- To perform RADIUS-based network authentication
- With the necessary RADIUS secret to allow for successful endpoint authentication processing to occur with 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 plugin-managed NAS device, make sure that each CounterACT plugin is configured with the necessary RADIUS secret.


Edit switch
Edit Switch
General
CLI
SNMP
Permissions
ACL
SGT
802.1X
802.1X
Configure 802.1x settings
Radius Secret as configured in switches
Retype Radius Secret as configured in switches
Help
OK
Cancel
Edit wireless
Edit Wireless Device
General
SNMP
Command Line
802.1X
802.1X
Configure 802.1X settings
RADIUS Secret as configured in WLAN Device
Retype RADIUS Secret as configured in WLAN Device
Help
OK
Cancel

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 CounterACT Administration 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:

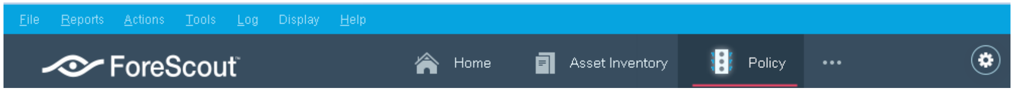
- Verify that the Switch Plugin is configured to manage the switch, including:
  - CLI is selected for use and CLI credentials are configured
  - The selected MAC read/write method includes CLI
  - The **cdm** configuration flag is activated

Run the Template

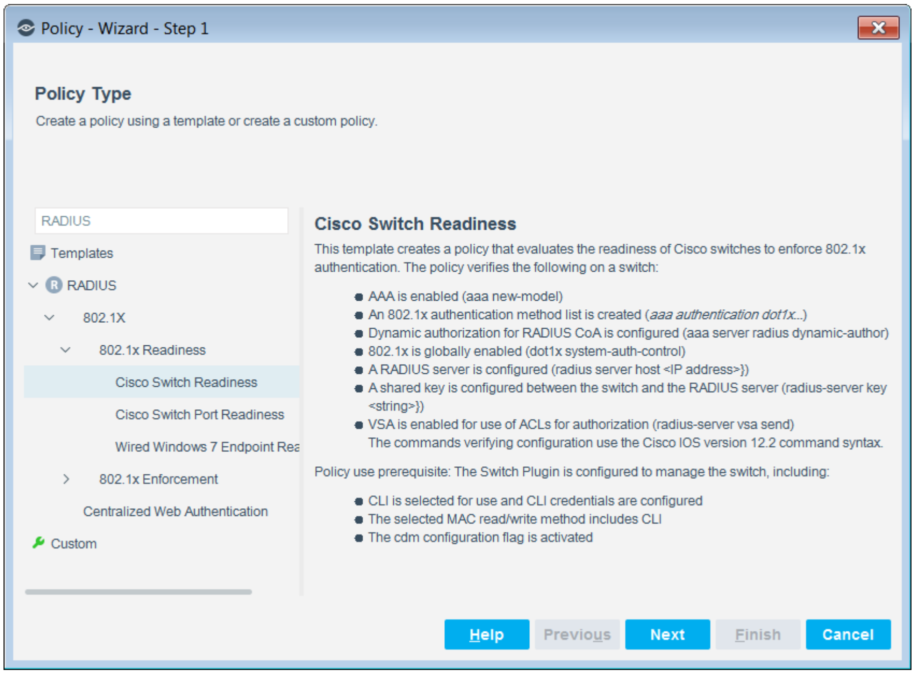
This section describes how to create a policy based on the template.

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 **RADIUS** > **802.1X** > **802.1X Readiness** and then select **Cisco Switch Readiness**.



Policy Type

Create a policy using a template or create a custom policy.

Cisco Switch Readiness

This template creates a policy that evaluates the readiness of Cisco switches to enforce 802.1x authentication. The policy verifies the following on a switch:

- AAA is enabled (aaa new-model)
- An 802.1x authentication method list is created (*aaa authentication dot1x..*)
- Dynamic authorization for RADIUS CoA is configured (aaa server radius dynamic-author)
- 802.1x is globally enabled (dot1x system-auth-control)
- A RADIUS server is configured (radius server host <IP address>})
- A shared key is configured between the switch and the RADIUS server (radius-server key <string>})
- VSA is enabled for use of ACLs for authorization (radius-server vsa send)
  The commands verifying configuration use the Cisco IOS version 12.2 command syntax.

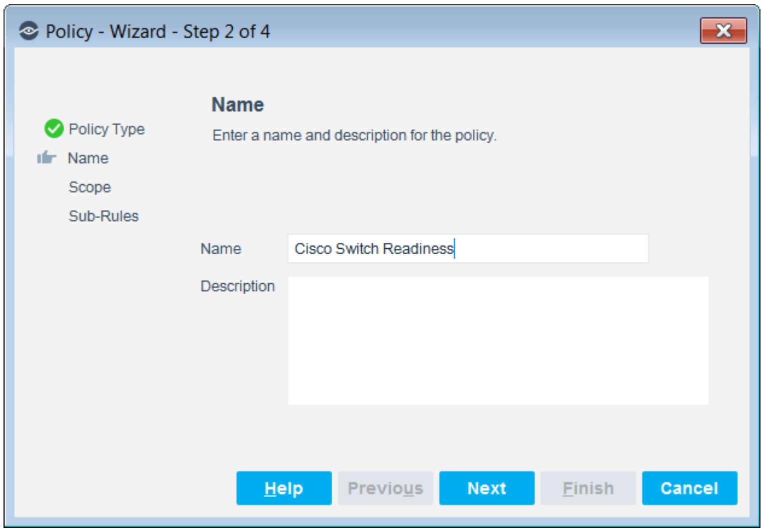
Policy use prerequisite: The Switch Plugin is configured to manage the switch, including:

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

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, Reports and in other features. Precise names make working with policies and reports more efficient.



Policy - Wizard - Step 2 of 4

Name

Enter a name and description for the policy.

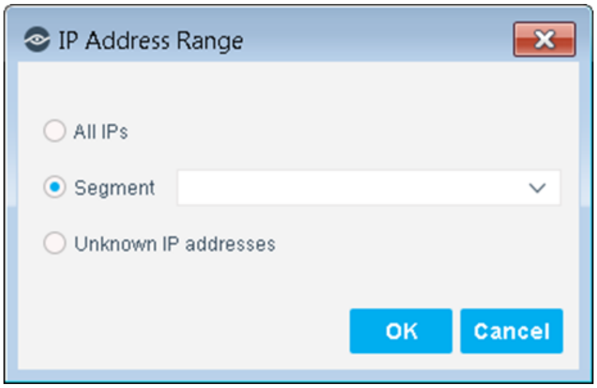
Name: Cisco Switch Readiness

Description:

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

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



IP Address Range

○ All IPs

● Segment

○ Unknown IP addresses

Define Policy Scope

The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close this dialog box, and select **Segments** from the Scope page.

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

You can filter the range by including only certain 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.

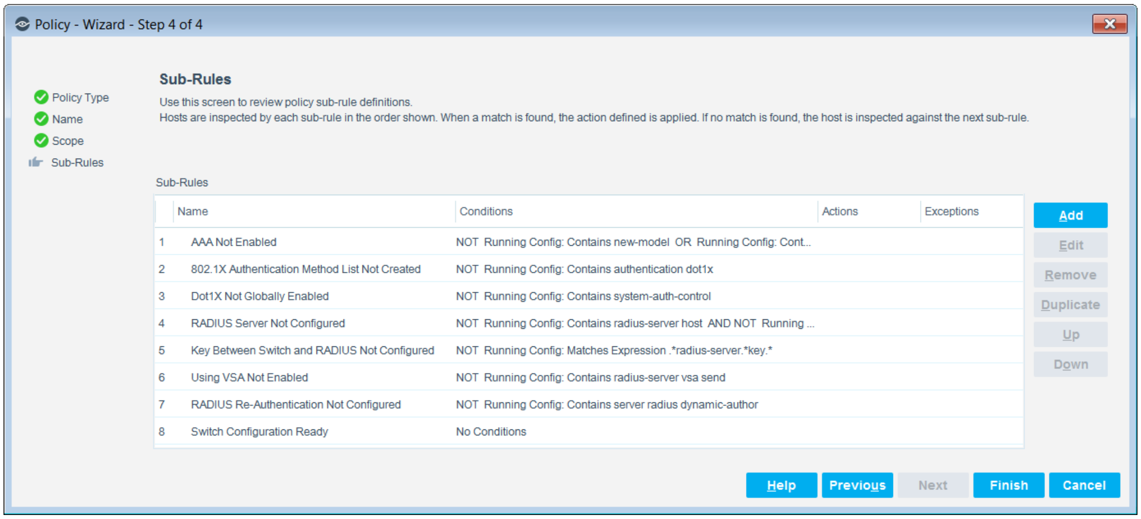
Cisco Switch Readiness Main Rule

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.



Policy - Wizard - Step 4 of 4

Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	AAA Not Enabled	NOT Running Config: Contains new-model OR Running Config: Cont...		
2	802.1X Authentication Method List Not Created	NOT Running Config: Contains authentication dot1x		
3	Dot1X Not Globally Enabled	NOT Running Config: Contains system-auth-control		
4	RADIUS Server Not Configured	NOT Running Config: Contains radius-server host AND NOT Running ...		
5	Key Between Switch and RADIUS Not Configured	NOT Running Config: Matches Expression .*radius-server.*key.*		
6	Using VSA Not Enabled	NOT Running Config: Contains radius-server vsa send		
7	RADIUS Re-Authentication Not Configured	NOT Running Config: Contains server radius dynamic-author		
8	Switch Configuration Ready	No Conditions		

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.*

Sub-Rule Name	Description
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:

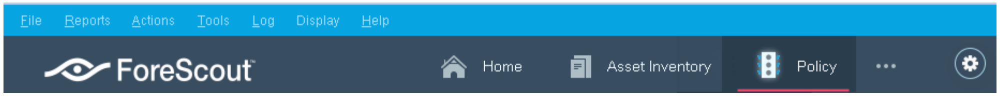
- Verify that the Switch Plugin is configured to manage the switch, including:
  - CLI is selected for use and CLI credentials are configured
  - The selected MAC read/write method includes CLI

Run the Template

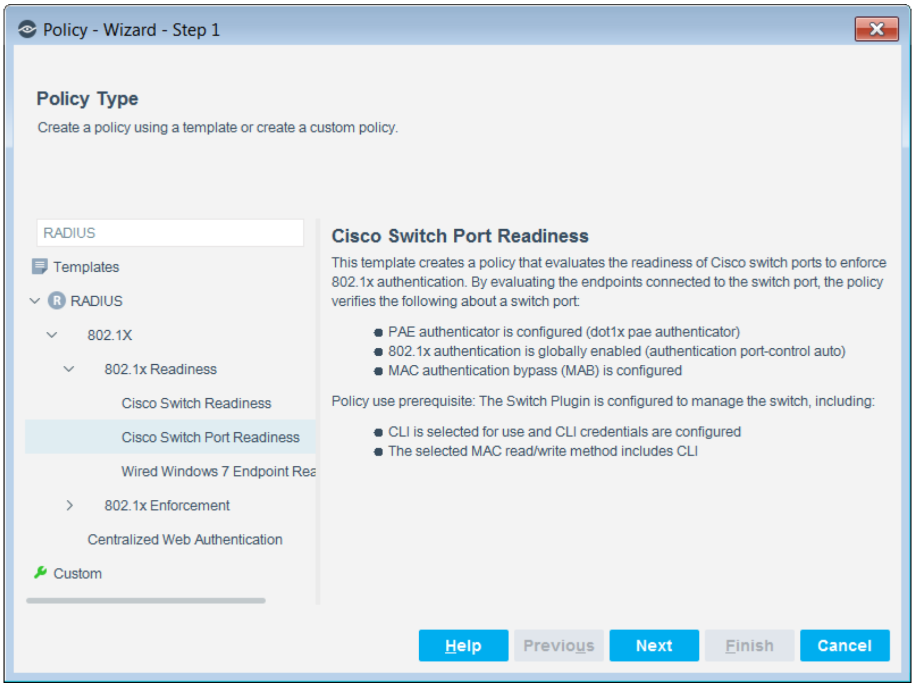
This section describes how to create a policy based on the template.

To run the template:

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



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



Policy Type

Create a policy using a template or create a custom policy.

RADIUS

Cisco Switch Port Readiness

This template creates a policy that evaluates the readiness of Cisco switch ports to enforce 802.1x authentication. By evaluating the endpoints connected to the switch port, the policy verifies the following about a switch port:

- PAE authenticator is configured (dot1x pae authenticator)
- 802.1x authentication is globally enabled (authentication port-control auto)
- MAC authentication bypass (MAB) is configured

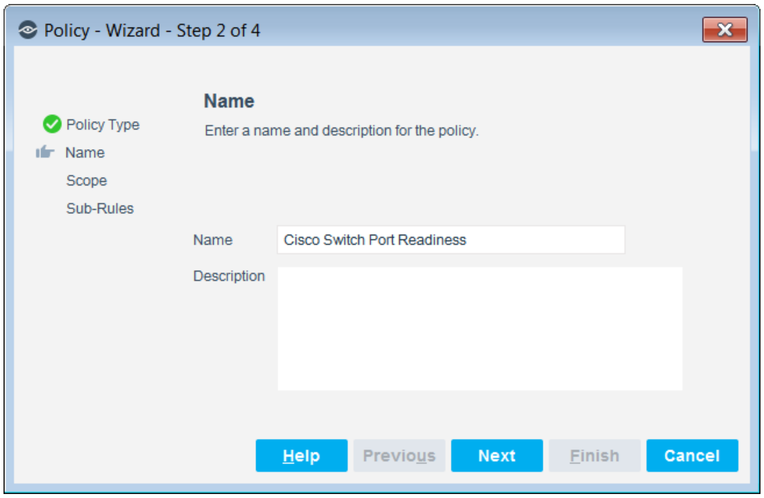
Policy use prerequisite: The Switch Plugin is configured to manage the switch, including:

- CLI is selected for use and CLI credentials are configured
- The selected MAC read/write method includes CLI

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, Reports and in other features. Precise names make working with policies and reports more efficient.



Name

Enter a name and description for the policy.

Name: Cisco Switch Port Readiness

Description:

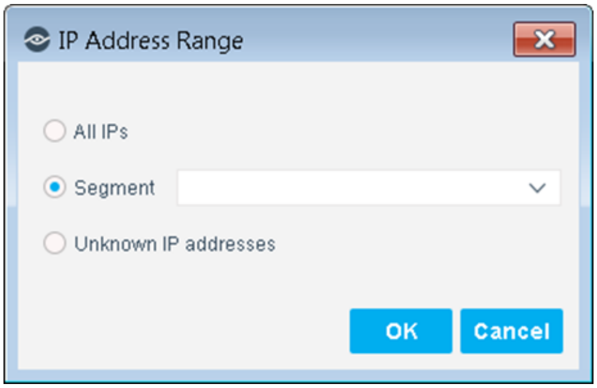
1. Define a unique name for the policy you are creating based on this template and enter a description.
   – Use a name that clearly reflects what the policy does. Use a descriptive name that identifies what your policy verifies and what actions will be taken.

- 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

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



Define Policy Scope

The following options are available:

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

You can filter the range by including only certain 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.

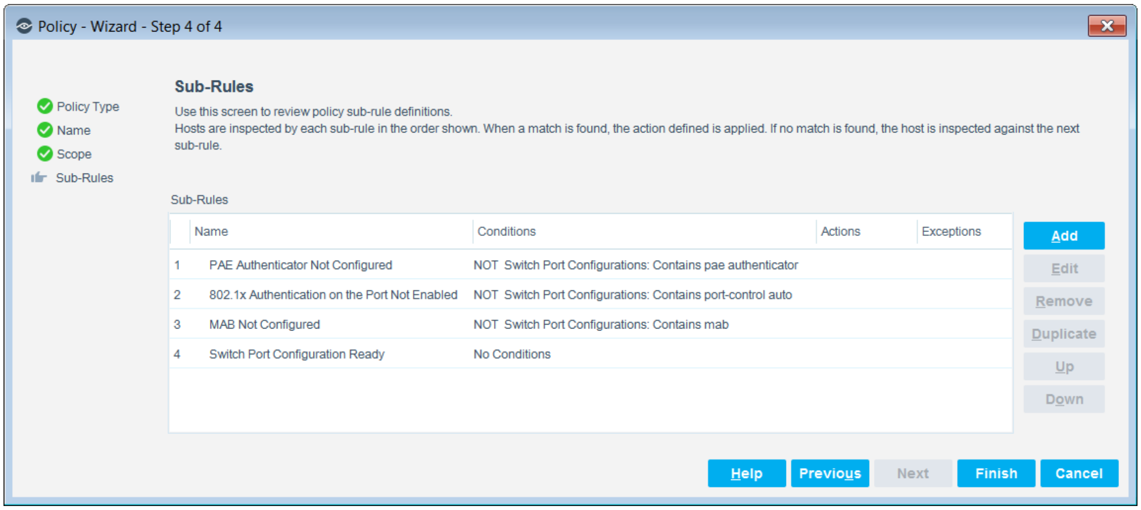
Cisco Switch Port Readiness Main Rule

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.



Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	PAE Authenticator Not Configured	NOT Switch Port Configurations: Contains pae authenticator		
2	802.1x Authentication on the Port Not Enabled	NOT Switch Port Configurations: Contains port-control auto		
3	MAB Not Configured	NOT Switch Port Configurations: Contains mab		
4	Switch Port Configuration Ready	No Conditions		

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:

Sub-Rule Name	Description
1. PAE Authenticator Not Configured	Verifies if the following is true for the switch port: ▪ **`dot1x pae authenticator`** is not configured When this condition is true, the switch port is ***not ready*** for 802.1X authentication.
2. 802.1X Authentication on the Port Not Enabled	Verifies if the following is true for the switch port: ▪ **`authentication port-control auto`** is not configured When this condition is true, the switch port is ***not ready*** for 802.1X authentication.
3. MAB Not Configured	Verifies if the following is true for the switch port: ▪ **`mab`** is not configured When this condition is true, the switch port is ***not ready*** for 802.1X authentication.
4. Switch Port Configuration Ready	When the inspected endpoints connected to the switch port do not match any of the preceding policy sub-rules, the switch port is ***ready*** for 802.1X authentication.

Endpoint Readiness

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

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 CounterACT Administration 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:

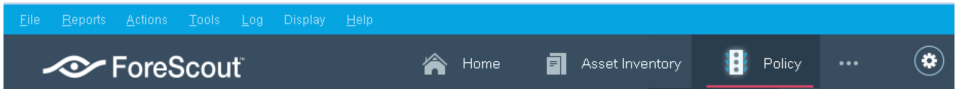
- Verify that endpoints are classified in the *Windows* group (can be accomplished by running the CounterACT Asset Classification policy)
- Verify that endpoints are classified in the *Corporate Hosts* group (can be accomplished by running the CounterACT Corporate/Guest Control policy)
- Verify that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

Run the Template

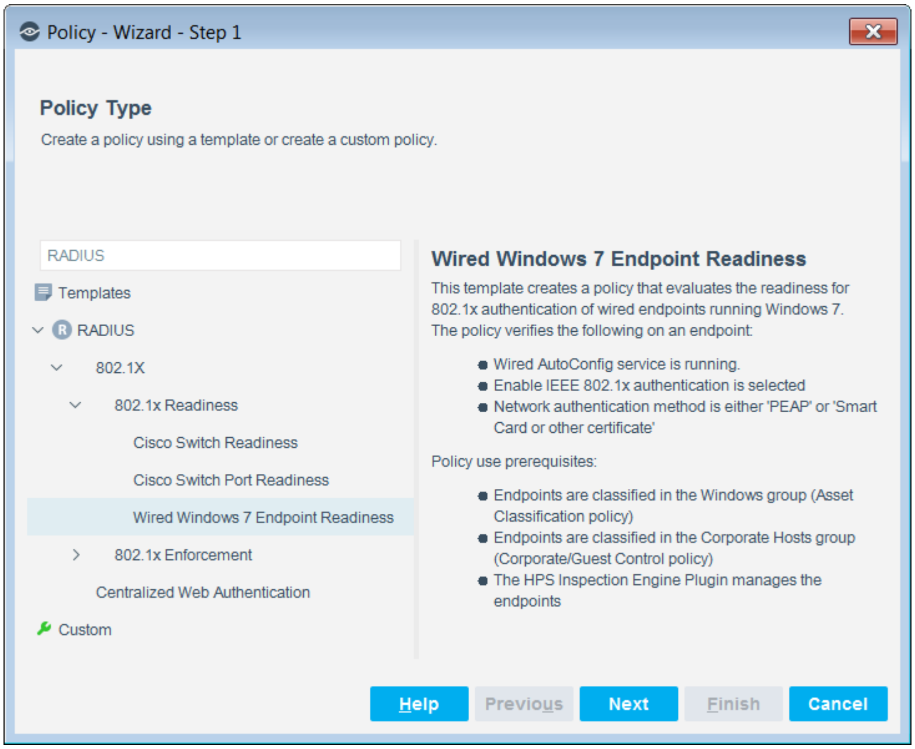
This section describes how to create a policy based on the template.

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 **RADIUS** > **802.1X** > **802.1X Readiness** and then select **Wired Windows 7 Endpoint Readiness**.



Policy - Wizard - Step 1

Policy Type

Create a policy using a template or create a custom policy.

RADIUS
Templates
RADIUS
802.1X
802.1x Readiness
Cisco Switch Readiness
Cisco Switch Port Readiness
Wired Windows 7 Endpoint Readiness
802.1x Enforcement
Centralized Web Authentication
Custom

Wired Windows 7 Endpoint Readiness

This template creates a policy that evaluates the readiness for 802.1x authentication of wired endpoints running Windows 7. The policy verifies the following on an endpoint:

- Wired AutoConfig service is running.
- Enable IEEE 802.1x authentication is selected
- Network authentication method is either 'PEAP' or 'Smart Card or other certificate'

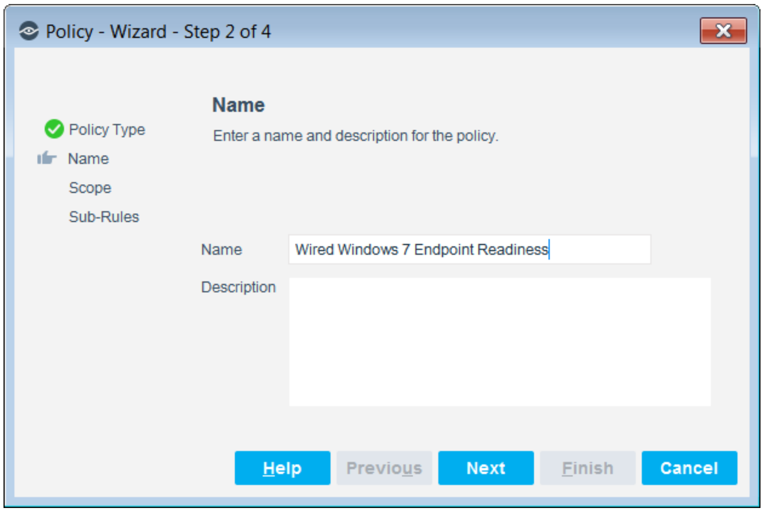
Policy use prerequisites:

- Endpoints are classified in the Windows group (Asset Classification policy)
- Endpoints are classified in the Corporate Hosts group (Corporate/Guest Control policy)
- The HPS Inspection Engine Plugin manages the endpoints

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, Reports and in other features. Precise names make working with policies and reports more efficient.



Policy - Wizard - Step 2 of 4

Name

Enter a name and description for the policy.

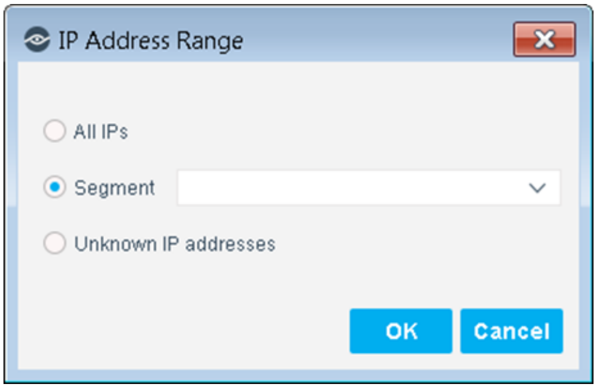
Name: Wired Windows 7 Endpoint Readiness

Description:

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

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



IP Address Range

○ All IPs

● Segment

○ Unknown IP addresses

Define Policy Scope

The following options are available:

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

You can filter the range by including only certain 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

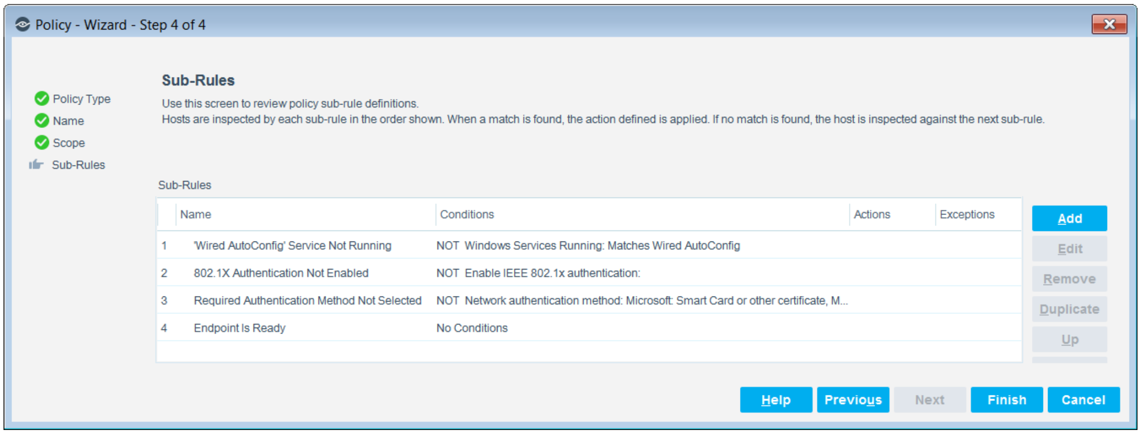
CounterACT-detected endpoints that meet the following criteria match the main rule of this policy:

- 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.



Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	'Wired AutoConfig' Service Not Running	NOT Windows Services Running: Matches Wired AutoConfig		
2	802.1X Authentication Not Enabled	NOT Enable IEEE 802.1x authentication:		
3	Required Authentication Method Not Selected	NOT Network authentication method: Microsoft: Smart Card or other certificate, M...		
4	Endpoint Is Ready	No Conditions		

Wired Windows 7 endpoints are inspected against each sub-rule in the order listed and verify the following about an endpoint configuration:

Sub-Rule Name	Description
1. Wired AutoConfig Service Not Running	Verifies if the following is true on the endpoint: ▪ **`Wired AutoConfig`** service is not running When this condition is true, the endpoint is ***not ready*** for 802.1X authentication.
2. 802.1X Authentication Not Enabled	Verifies if the following is true for the supplicant installed on the endpoint: ▪ **`Enable IEEE 802.1X authentication`** configuration is not enabled When this condition is true, the endpoint is ***not ready*** for 802.1X authentication.
3. Required Authentication Method Not Selected	Verifies if both of the following are true for the supplicant installed on the endpoint: ▪ Network authentication method is not **PEAP** ▪ Network authentication method is not **`Smart Card or other certificate`** When both 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 RADIUS 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 RADIUS Plugin to join the machine to the domain.
   - This best practice is also applicable when adding a user directory replica and configuring its **Name** field in the Replicas pane of the User Directory Plugin.

   See User Directory Plugin: Settings Pane, bullet 2.
2. Make sure that both the **Use as directory** option and the **Use for authentication** option are enabled.

User Directory Plugin: Settings Pane

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

1. If the **DNS Detection** option is enabled, then the RADIUS Plugin automatically selects a user directory (Microsoft Active Directory) server FQDN. Take note of the following:
   - **a.** The RADIUS Plugin queries domain to obtain the domain server FQDN list; the plugin uses the domain configured in the **Domain** field in the Directory section of the User Directory Plugin Settings pane.
   - **b.** A domain controller FQDN is chosen based on quickest responder.
   - **c.** The plugin uses the selected FQDN to join the CounterACT machine to the domain.
2. However, if the **DNS Detection** option is not enabled, the RADIUS Plugin statically builds a domain server FQDN list by concatenating the Main/replicas configured **Name** field with its configured **Domain** field. Take note of the following:
   - **a.** A domain controller FQDN is chosen based on quickest responder.
   - **b.** The plugin uses the selected FQDN to join the 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 RADIUS Plugin is started or when its configuration is saved, the CounterACT device joins the relevant domain using the user credentials that are defined in the 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
6. When 802.1X authentication by an Appliance uses multiple user directories, then for each selected, authenticating user directory defined in the RADIUS Plugin Authentication Sources tab, verify that the following information is defined in the User Directory Plugin:
   a. Additional Domain Aliases: In the 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

- 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. Refer to https://support.microsoft.com/en-gb/kb/909264
- Network Time Protocol (NTP) configuration of CounterACT devices [Enterprise Manager, Appliances] must be aligned with the domain to successfully obtain a Kerberos ticket.

Using an External RADIUS Server

If you plan on using an external RADIUS server as an authentication source for the RADIUS Plugin, configure (**Add**) the server in the User Directory Plugin.

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

Plugin Configuration

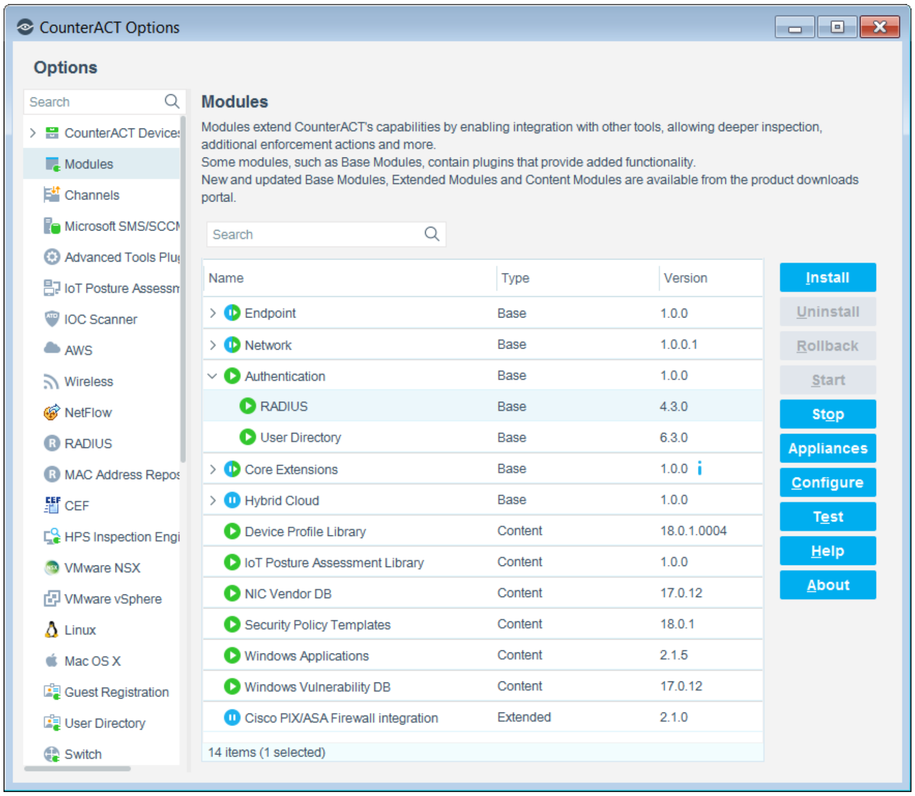
This section describes how to configure the various plugin components in order for the RADIUS Plugin to provide authentication and authorization of the endpoints attempting to access your organization's network. This section presents the following topics:

- Configure Authentication Sources
- Configure Pre-Admission Authorization
- Configure RADIUS Settings
- RADIUS 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** > **Modules**. The Modules pane opens.
2. In the Modules pane, select the **Authentication** module. The plugins, which are installed as part of the CounterACT Authentication Module, display beneath the Authentication entry.
3. In the Modules pane, select the **RADIUS** entry from the table listing.



Modules

Modules extend CounterACT's capabilities by enabling integration with other tools, allowing deeper inspection, additional enforcement actions and more.
Some modules, such as Base Modules, contain plugins that provide added functionality.
New and updated Base Modules, Extended Modules and Content Modules are available from the product downloads portal.

Name	Type	Version
Endpoint	Base	1.0.0
Network	Base	1.0.0.1
Authentication	Base	1.0.0
RADIUS	Base	4.3.0
User Directory	Base	6.3.0
Core Extensions	Base	1.0.0
Hybrid Cloud	Base	1.0.0
Device Profile Library	Content	18.0.1.0004
IoT Posture Assessment Library	Content	1.0.0
NIC Vendor DB	Content	17.0.12
Security Policy Templates	Content	18.0.1
Windows Applications	Content	2.1.5
Windows Vulnerability DB	Content	17.0.12
Cisco PIX/ASA Firewall integration	Extended	2.1.0

14 items (1 selected)

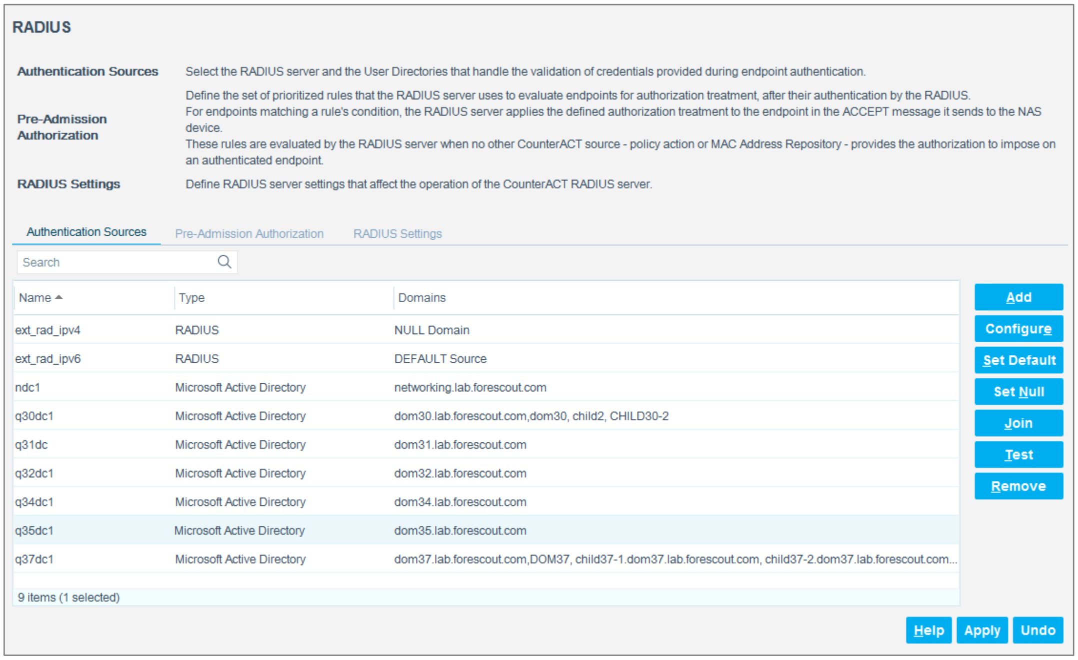
4. Select **Configure**. The RADIUS pane opens in the Options window and displays the Authentication Sources tab.

Configure Authentication Sources

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

Supported authentication sources:

- Microsoft Active Directory Server
- External RADIUS Server



RADIUS

Authentication Sources Select the RADIUS server and the User Directories that handle the validation of credentials provided during endpoint authentication.

Pre-Admission Authorization Define the set of prioritized rules that the RADIUS server uses to evaluate endpoints for authorization treatment, after their authentication by the RADIUS. For endpoints matching a rule's condition, the RADIUS server applies the defined authorization treatment to the endpoint in the ACCEPT message it sends to the NAS device. These rules are evaluated by the RADIUS server when no other CounterACT source - policy action or MAC Address Repository - provides the authorization to impose on an authenticated endpoint.

RADIUS Settings Define RADIUS server settings that affect the operation of the CounterACT RADIUS server.

Name ▲	Type	Domains
ext_rad_ipv4	RADIUS	NULL Domain
ext_rad_ipv6	RADIUS	DEFAULT Source
ndc1	Microsoft Active Directory	networking.lab.forescout.com
q30dc1	Microsoft Active Directory	dom30.lab.forescout.com,dom30, child2, CHILD30-2
q31dc	Microsoft Active Directory	dom31.lab.forescout.com
q32dc1	Microsoft Active Directory	dom32.lab.forescout.com
q34dc1	Microsoft Active Directory	dom34.lab.forescout.com
q35dc1	Microsoft Active Directory	dom35.lab.forescout.com
q37dc1	Microsoft Active Directory	dom37.lab.forescout.com,DOM37, child37-1.dom37.lab.forescout.com, child37-2.dom37.lab.forescout.com...

9 items (1 selected)

To add new authentication sources:

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

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

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 displays the added authentication sources.

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

Column	Description
Name	Name of the authentication source as configured in the User Directory Plugin. Authentication sources that the CounterACT RADIUS server cannot use (query) display the text ***(Source NOT in USE)*** immediately after their name. For an explanation, see the **Domains** column description.
Type	The server type of the authentication source as configured in the User Directory Plugin. For CounterACT RADIUS server purposes, the supported types are *Microsoft Active Directory* and *RADIUS* (external RADIUS server).
Domains	Lists the domains that the authentication source is assigned to handle; these are domains that could be supplied in 802.1X authentication requests. ▪ For authentication sources of type *Microsoft Active Directory*: The information appearing in this column comes from the domain and additional domain aliases that are configured in the User Directory Plugin for these authentication sources. Column information is view-only. ▪ For authentication sources of type *RADIUS*: Domain assignment must be manually configured for these authentication sources. For configuration detail, see the **Configure** button in Tab Buttons for Authentication Sources. Authentication sources must fulfill at least one of the following criteria, in order for the CounterACT RADIUS server to be able to use (query) them: ▪ The source has an assigned domain ▪ The source is designated as the *DEFAULT Source*. See the **Set Default** button in Tab Buttons for Authentication Sources. ▪ The source is designated to handle the *NULL Domain*. See the **Set NULL** button in Tab Buttons for Authentication Sources.

Tab Buttons for Authentication Sources

The tab provides the following buttons for dealing with authentication sources:

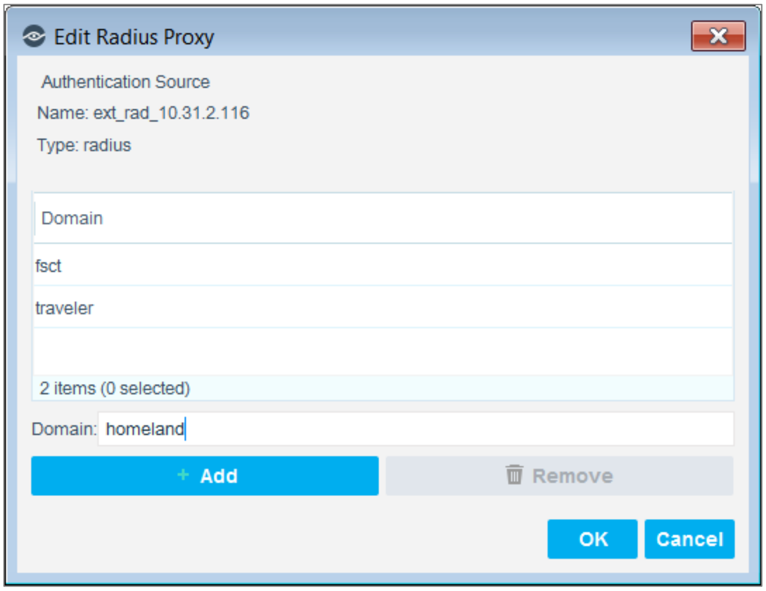
- **Add** - select to open the Add Authentication Sources dialog. In the dialog, select one or more than one entry to add as an authentication source in the Authentication Sources tab; it is valid to select *RADIUS* servers, *Microsoft Active Directory* servers or a combination of both types.
- **Configure** - for a selected authentication source, select this button to open the following dialog:
  - For a *Microsoft Active Directory* authentication source, the **Configure Active Directory** dialog opens:

    > The dialog lists the domain and additional domain aliases that are configured in the User Directory Plugin for the source. This information is view-only.

    > Saved Test Credentials pane - select an entry in the Domain listing located above this pane. Then, in the pane, enter credentials that the plugin uses to access and test the functionality of that authentication source.

- For a *RADIUS* authentication source, the **Edit Radius Proxy** dialog opens:

  > In the **Domain** field of the dialog, enter a domain NetBIOS name, as it would appear in the RADIUS *access request*, and select **+Add**. As necessary, repeat this step to enter additional domain NetBIOS names, as a *RADIUS* authentication source can be assigned to handle multiple domains.



Authentication Source

Name: ext_rad_10.31.2.116

Type: radius

Domain
fsct
traveler

2 items (0 selected)

Domain: homeland

- Designate a selected authentication source for special domain handling responsibility, as follows:
  - **Set Default** - selecting this button designates the authentication source as the default authentication source; the text *DEFAULT Source* displays in its **Domains** column. At any given time, only one authentication source can be designated as the default authentication source.
  - **Set Null** - selecting this button designates the authentication source as the null domain handler; the text *NULL Domain* displays in its **Domains** column*.* At any given time, only one authentication source can be designated as the null domain handler.

  An authentication source can be assigned multiple domains and/or can be designated the default authentication source and/or can be designated the null domain handler. See Determining the Authentication Source to Query.

- **Join** - enabled only for a selected *Microsoft Active Directory* authentication source. Select this button to open the **Join Domain: Provide Credentials** dialog. Use this dialog to accomplish the following:
  - Provide administrator credentials that the plugin uses to join CounterACT device(s) to the Active Directory domain.
  - Select **Join** to launch a plugin attempt to join CounterACT devices to the Active Directory domain, using the provided credentials.

  For further information, see Join CounterACT Devices to Active Directory Domain.

Test - select this button to run a plugin test of the functionality of a selected authentication source. For further information, see Test Authentication Source Functionality.

- **Remove** - select an authentication source and then select **Remove**. The authentication source is removed from display in the Authentication Sources tab.

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

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.

Join CounterACT Devices to Active Directory Domains

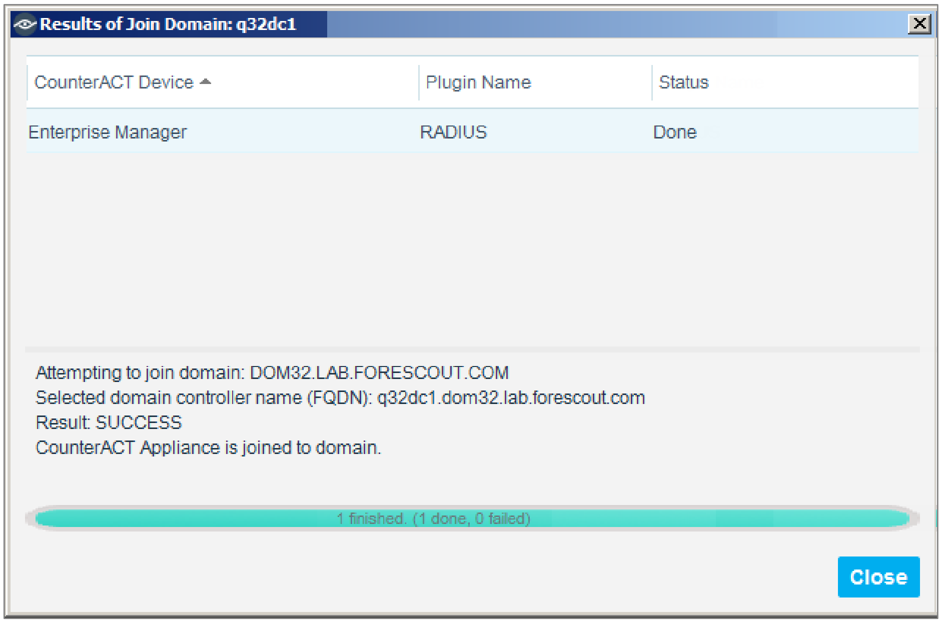
In order for the CounterACT RADIUS server to query a *Microsoft Active Directory* authentication source, the RADIUS Plugin must first join all CounterACT devices to each of the authentication source's assigned domains. The credentials (administrator level) that the plugin uses for the join must already be configured via the **Join Domain: Provide Credentials** dialog. To access this dialog and initiate a plugin join attempt, see the Join button description.

After providing the credentials and confirming, the **Join Domain: Confirmation** window opens and presents the following information:

> **Join the following CounterACT device(s) to domain:** *<active directory domain>*
>
> – *<CounterACT device-1>*
>
> – .
>
> – .
>
> – *<CounterACT device-n>*
>
> **Continue?**

Upon selecting **Yes** to proceed with the join, the **Results of Join Domain:** *<active directory domain>* window opens and presents the following information:

> **Attempting to join domain:** *<active directory domain>*
>
> **Selected domain controller name (FQDN):** *<domain controller FQDN>*
>
> **Result:** *<result>*
>
> – If the join is successful, the following information displays:
>
> **Result: SUCCESS**
>
> **CounterACT Appliance is joined to domain.**
>
> – If the join is not successful, the following information displays:
>
> **Result: FAILURE**
>
> **CounterACT Appliance is not joined to domain.**
>
> **CAUSE:** *<error message>*


Results of Join Domain: q32dc1
1 finished. (1 done, 0 failed)
Close

CounterACT Device	Plugin Name	Status
Enterprise Manager	RADIUS	Done

Attempting to join domain: DOM32.LAB.FORESCOUT.COM
Selected domain controller name (FQDN): q32dc1.dom32.lab.forescout.com
Result: SUCCESS
CounterACT Appliance is joined to domain.

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

ForeScout recommends performing the *join* at step **d** of the authentication source configuration flow, as follows:

a. Add a *Microsoft Active Directory* authentication source

b. Configure the source's test credentials

c. Repeat steps a through b as necessary for multiple authentication sources

d. Initiate plugin join attempt per authentication source

e. Run plugin test of the authentication source functionality per source

f. After performing the above, select **Apply** to save the modified plugin configuration.

Test Authentication Source Functionality

For a selected authentication source, initiate a plugin test of the source's functionality using the Test button in the Authentication Sources tab. After selecting **Test**, the **Test Authentication Source: Confirmation** window opens and presents the following information:

- For a *Microsoft Active Directory* authentication source:

  Test functionality of Active Directory <*NetBIOS name*> **with the following CounterACT device(s):**

- For a *RADIUS* authentication source:

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

- The CounterACT devices to be tested with the selected authentication source:

  – <*CounterACT device-1*>

  – .

  – .

  – <*CounterACT device-n*>

  Continue?

When selecting **Yes** to proceed with the test, the **Results of Test Authentication Source:** window opens.

Testing with Microsoft Active Directory Server

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

Testing functionality of authentication source <*NetBIOS name*> **of type Active Directory**

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

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

CounterACT Appliance is joined to domain

Testing authentication using configured test credentials for joined Appliance

Authentication test: <*result*>

- If the test is successful, the <*result*> displayed is:

  SUCCEEDED

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

  FAILED

The test does not proceed and an applicable error message displays, when any one of the following conditions are true:

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

Testing with RADIUS Server

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

Testing functionality of authentication source <*RADIUS server name*> **of type RADIUS**

Testing external server RADIUS service status on port <*port #*>: <*result*>

- If the test is successful, the <*result*> displayed is:

  SUCCESS

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

  FAILURE

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

Testing external server connectivity status (ping): <*result*>

- If the test is successful, the <*result*> displayed is:

  SUCCESS

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

  FAILURE

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

Configure Pre-Admission Authorization

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

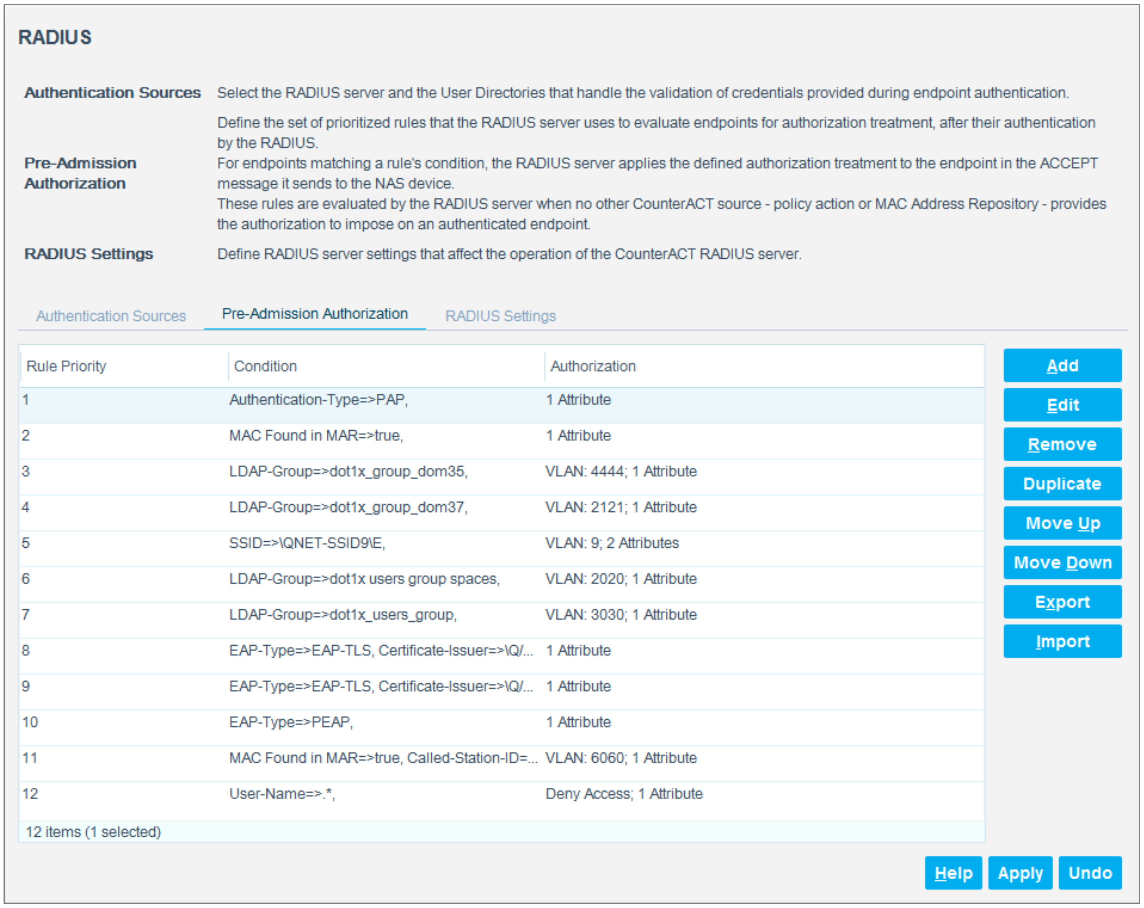
The CounterACT RADIUS server evaluates pre-admission authorization rules when no other CounterACT source - not policy action, not MAC Address Repository - provides the authorization to impose on an authenticated endpoint; for example, prior to an endpoint being admitted to an organization's network. 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 sends to the NAS device:

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

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



RADIUS

Authentication Sources	Select the RADIUS server and the User Directories that handle the validation of credentials provided during endpoint authentication.
Pre-Admission Authorization	Define the set of prioritized rules that the RADIUS server uses to evaluate endpoints for authorization treatment, after their authentication by the RADIUS. For endpoints matching a rule's condition, the RADIUS server applies the defined authorization treatment to the endpoint in the ACCEPT message it sends to the NAS device. These rules are evaluated by the RADIUS server when no other CounterACT source - policy action or MAC Address Repository - provides the authorization to impose on an authenticated endpoint.
RADIUS Settings	Define RADIUS server settings that affect the operation of the CounterACT RADIUS server.

Rule Priority	Condition	Authorization
1	Authentication-Type=>PAP,	1 Attribute
2	MAC Found in MAR=>true,	1 Attribute
3	LDAP-Group=>dot1x_group_dom35,	VLAN: 4444; 1 Attribute
4	LDAP-Group=>dot1x_group_dom37,	VLAN: 2121; 1 Attribute
5	SSID=>\QNET-SSID9\E,	VLAN: 9; 2 Attributes
6	LDAP-Group=>dot1x users group spaces,	VLAN: 2020; 1 Attribute
7	LDAP-Group=>dot1x_users_group,	VLAN: 3030; 1 Attribute
8	EAP-Type=>EAP-TLS, Certificate-Issuer=>\Q/...	1 Attribute
9	EAP-Type=>EAP-TLS, Certificate-Issuer=>\Q/...	1 Attribute
10	EAP-Type=>PEAP,	1 Attribute
11	MAC Found in MAR=>true, Called-Station-ID=...	VLAN: 6060; 1 Attribute
12	User-Name=>.*,	Deny Access; 1 Attribute

12 items (1 selected)

In the tab, perform any of the following actions:

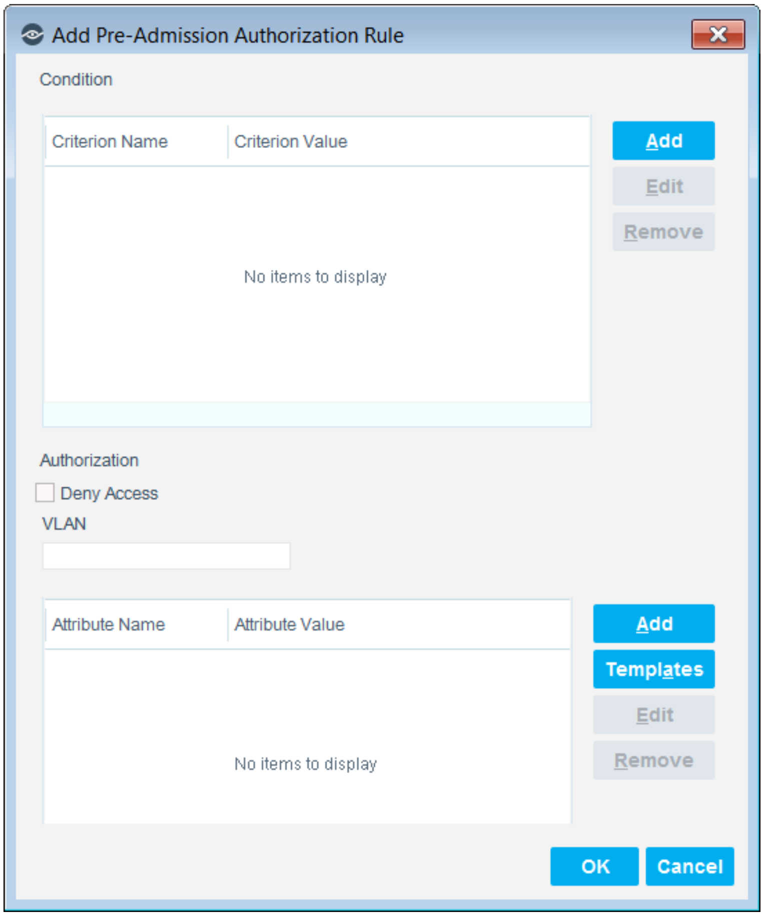
- **Add** new pre-admission authorization rules. Select **Add**. The Add Pre-Admission Authorization Rule window opens. Define rule details [Condition, Authorization]. Selecting **OK** adds the rule to the top of the list of entries in the Pre-Admission Authorization table.
- **Edit** rules. Select a 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. The Condition section provides the following buttons for rule condition configuration:

- **Add** - select this button to add a new rule condition
- **Edit** - select this button to edit an existing rule condition
- **Remove** - select this button to remove one or more existing 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:

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

Column	Description
	The attributes available for configuration are: ▪ **Authentication-Type** ▪ **Called-Station-ID** ▪ **Calling-Station-ID** ▪ **Certificate-Common-Name** ▪ **Certificate-Issuer** ▪ **Certificate-Subject** ▪ **Certificate-Subject-Alternate-Name** ▪ **Day and Time Restriction** - is compared with the day/time of the received endpoint authentication request. ▪ **EAP-Type** ▪ **LDAP-Group** - is compared with the user LDAP groups defined in the Microsoft Active Directory server of the domain in the User-name. By default, the plugin uses TLS to perform a secure LDAP query to the Active Directory server. Valid servers are configured in the **Authenticating User Directories** table of the **Authentication Sources** tab. In order for the plugin to perform this comparison, the CA certificate of the Microsoft Active Directory server must be defined as a ***trusted certificate*** in the Console certificate interface. Refer to the *CounterACT Certificate Interface Configuration Guide* for instructions. See Additional CounterACT Documentation for information on how to access this guide. The following are examples of valid text to enter in this field: - Straightforward text, as in *Students_Eng* or *Hospital_Admin* - Text containing the use of the wildcard character, as in *Hospital** (any user in a group beginning with *Hospital* is matched) or as in **Admin* (any user in a group ending with *Admin* is matched). ▪ **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 to be authenticated using MAC address bypass (MAB). ▪ **MAR Comment** - free text. Use this attribute to assign a tag to endpoints that are listed in the MAC Address Repository, to later support their appropriate authorization, based on the assigned MAR comment. ▪ **NAS-IP-Address** -IPv4 address of the switch or the WiFi AP/Controller ▪ **NAS-IPv6-Address** -IPv6 address of the switch or the WiFi AP/Controller ▪ **NAS-Port-Type** ▪ **SSID** ▪ **Tunneled-Method** - the authentication method used in a protected EAP (PEAP) tunnel ▪ **Tunneled-User-Name** - the user name used for the

Column	Description
	inner authentication phase of both Protected EAP-MSCHAPv2 and Protected EAP-TLS authentication processes. Usually both inner and outer user names are the same. However, when the supplicant's **Identity Privacy** field is configured, then the inner user-name (the Tunneled User Name) is the supplicant's true user name. ▪ **User-Name**
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:

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

- **VLAN**: Define the VLAN to which the NAS device must assign the authenticated endpoint. Enter either the VLAN ID or the VLAN name. This field accepts alphanumeric characters.
- **Attribute-Value Pair**: Attribute-value pair (AVP) assignments are imposed on the connection that the NAS device maintains for the authenticated endpoint. Multiple AVPs can be defined.

The Authorization section provides the following buttons for AVP configuration:

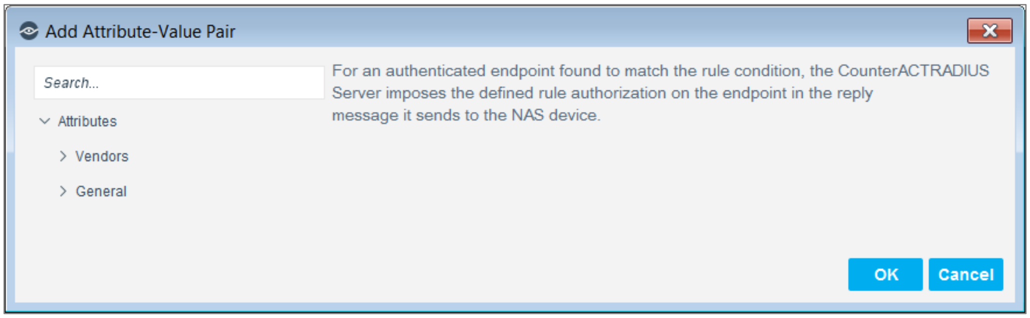
- **Add** - select this button to add new AVPs. For details, see Adding/Editing Attribute-Value Pairs.
- **Templates** - select this button to add new AVPs that are provided by one of several, different templates; each template provides AVP(s) that address a specific authorization use case. For details, see Attribute-Value Templates.
- **Edit** - select this button to edit an existing AVP
- **Remove** - select this button to remove one or more existing AVPs

After you perform any of the above [**Add**, **Templates**, **Edit**, **Remove**], selecting **OK** in the Pre-Admission Authorization Rule window updates the rule in the Pre-Admission Authorization tab. Select **Apply** to save the modified plugin configuration.

After endpoint admission to the network, additional or updated post-connect authorizations can be applied to such endpoints via CounterACT policy using the *RADIUS Authorize* action. For information about defining the *RADIUS Authorize* action, see Actions.

Adding/Editing Attribute-Value Pairs

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



For an authenticated endpoint found to match the rule condition, the CounterACTRADIUS Server imposes the defined rule authorization on the endpoint in the reply message it sends to the NAS device.

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

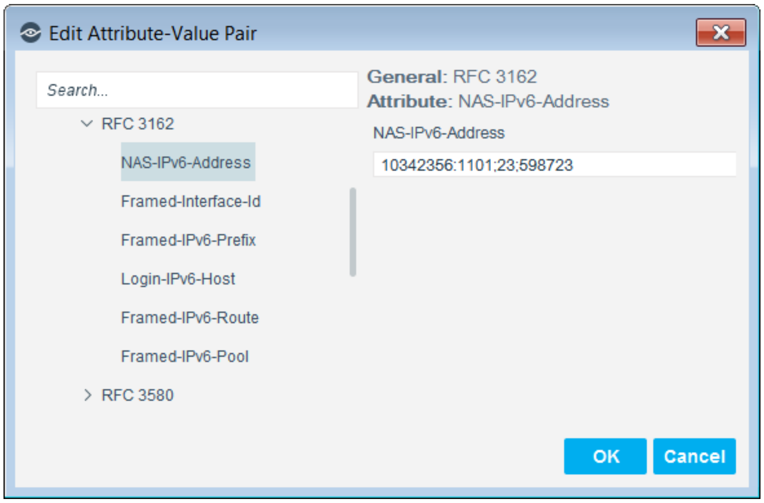
- **Vendors** - open this group to display a wealth of vendor-specific attribute groups. Opening any of these groups displays vendor-specific attributes that are available to select for value assignment.
- **General** - open this group to display primarily RFC-specific attribute groups. Opening any of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

Also, you can locate attributes using the dialog box's **Search** field.

After assigning the necessary value(s) for a selected attribute, select **OK**. The AVP you added is listed in the Authorization section of the Add Pre-Admission Authorization Rule window.

When a configured AVP, listed in the Authorization section, is selected for **Edit**, the Edit Attribute-Value Pair dialog box opens, as follows:

- On left side of the dialog box, the **Attributes** option is open to the attribute you selected for edit
- The right side of the dialog box displays the selected attribute and its paired value field/drop-down menu



Edit Attribute-Value Pair

Search...

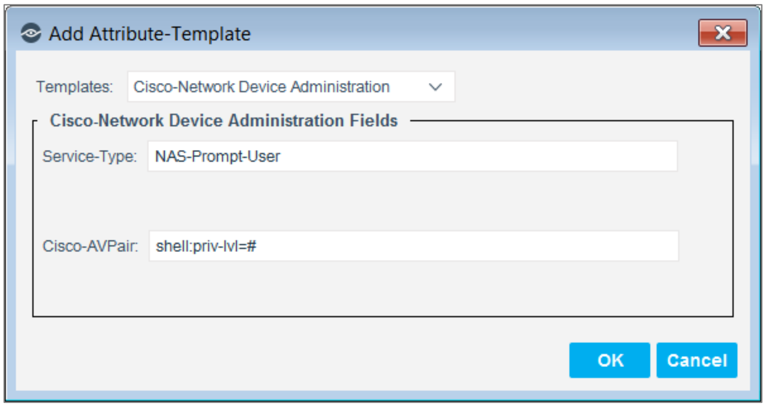
RFC 3162
NAS-IPv6-Address
Framed-Interface-Id
Framed-IPv6-Prefix
Login-IPv6-Host
Framed-IPv6-Route
Framed-IPv6-Pool
RFC 3580

General: RFC 3162
Attribute: NAS-IPv6-Address

NAS-IPv6-Address: 10342356:1101:23:598723

Attribute-Value Templates

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



Add Attribute-Template

Templates: Cisco-Network Device Administration

Cisco-Network Device Administration Fields

Service-Type: NAS-Prompt-User

Cisco-AVPair: shell:priv-lvl=#

From the **Templates** dropdown, select any one of the following available templates:

- **Cisco-ACL (ingress)** - provides two Cisco AVPs that impose access control list (ACL) authorization on each authenticated endpoint found to match the associated rule condition endpoint.
- **Cisco-Guest** - provides two Cisco AVPs that require you to assign them their necessary values. The authorization treatment provided by these AVPs is required for the RADIUS Plugin to deliver enhanced CounterACT guest management in the CounterACT centralized web authentication solution. For details, see the use case Centralized Web Authentication.
- **Cisco-Network Device Administration** - provides two AVPs, a RADIUS one and a Cisco one. The Cisco attribute requires you to assign it the necessary value. The authorization treatment provided by these AVPs is required for the RADIUS Plugin to perform authentication and initial authorization on the administrators of an organization's network devices. For details, see the use case Network Device Administration.
- **Meraki-Guest** - provides one Cisco AVP that requires you to assign it the necessary values. The authorization treatment provided by this AVP is required for the RADIUS Plugin to deliver enhanced CounterACT guest management in the CounterACT centralized web authentication solution. For details, see the use case Centralized Web Authentication.

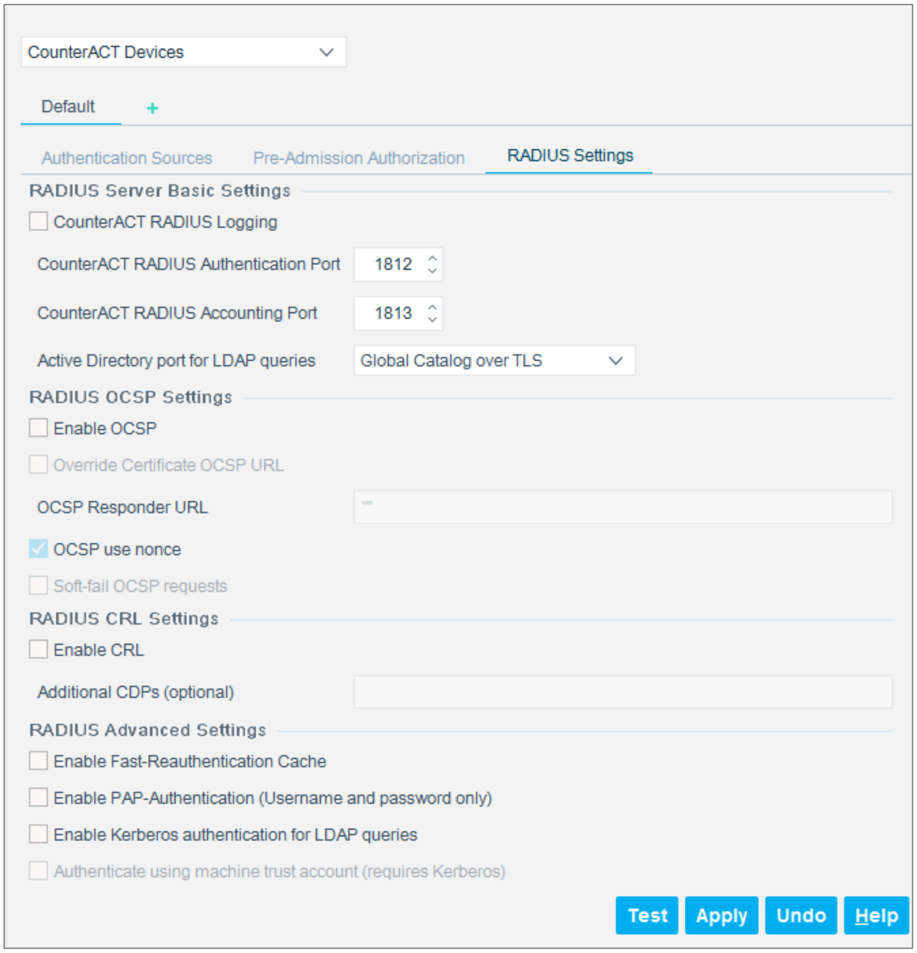
After assigning the necessary value(s) for the template-provided attribute(s), select **OK**. The AVP(s) you added are listed in order in the Authorization section of the Add Pre-Admission Authorization Rule window.

Configure RADIUS Settings

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

The tab provides the following setting categories:

- RADIUS Server Basic Settings
- RADIUS OCSP Settings
- RADIUS CRL Settings
- RADIUS Advanced Settings



RADIUS Server Basic Settings

□ CounterACT RADIUS Logging

CounterACT RADIUS Authentication Port: 1812

CounterACT RADIUS Accounting Port: 1813

Active Directory port for LDAP queries: Global Catalog over TLS

RADIUS OCSP Settings

□ Enable OCSP

□ Override Certificate OCSP URL

OCSP Responder URL: –

☑ OCSP use nonce

□ Soft-fail OCSP requests

RADIUS CRL Settings

□ Enable CRL

Additional CDPs (optional)

RADIUS Advanced Settings

□ Enable Fast-Reauthentication Cache

□ Enable PAP-Authentication (Username and password only)

□ Enable Kerberos authentication for LDAP queries

□ Authenticate using machine trust account (requires Kerberos)

RADIUS Server Basic Settings

Field	Description
CounterACT RADIUS Logging	By default, this option is disabled (not selected). Enable/disable running the CounterACT RADIUS server in debug mode. When enabled, CounterACT captures and logs RADIUS traffic processing detail. Use this option to troubleshoot CounterACT RADIUS server processing issues. ***After using this option, to avoid performance degradation, ForeScout recommends disabling it.***
CounterACT RADIUS Authentication Port	The UDP port for receiving authentication requests from switches and wireless controllers. Default: 1812
CounterACT RADIUS Accounting Port	The UDP port for receiving accounting requests from switches and wireless controllers. Default: 1813

Field	Description
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

Field	Description
Enable OCSP	By default, this option is disabled (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 disabled (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 enabled (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.
Soft-fail OCSP Requests	By default, this option is disabled (not selected). Selecting the **Soft-fail OCSP Requests** option instructs the CounterACT RADIUS server to accept the client certificate even though the CounterACT RADIUS server did not receive an OCSP response about the client certificate's revocation status.

RADIUS CRL Settings

Field	Description
Enable CRL	By default, this option is disabled (not selected). Selecting the **Enable CRL** option instructs the CounterACT RADIUS server to consult the Appliance's Certificate Revocation List (CRL) to verify the revocation status of the client certificate provided by an endpoint supplicant. If the CRL contains an entry for the certificate being verified, then either one of the following statuses are in effect for that certificate: ▪ The issuing certificate authority has permanently *revoked* that certificate ▪ The issuing certificate authority has temporarily *revoked* that certificate CounterACT only supports the use of HTTP to download CRLs. Upon selecting the **Enable CRL** option, the following *optional* field becomes available for data entry: ▪ **Additional CDPs**
Additional CDPs	Additional CRL distribution points (CDPs). (*Optional*) Enter one or more additional URLs from which the CounterACT RADIUS server downloads additional CRLs that it uses to verify the revocation status of the client certificate provided by an endpoint supplicant. Use the comma (,) to separate between multiple URLs. CounterACT only supports the use of HTTP to download CRLs.

RADIUS Advanced Settings

Field	Description
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
Enable PAP-Authentication (Username and password only)	By default, this option is disabled (not selected). Selecting the **Enable PAP-Authentication** option instructs the CounterACT RADIUS server to authenticate endpoints using PAP (password authentication protocol).
Enable Kerberos Authentication for LDAP Queries	Selecting the **Enable Kerberos Authentication for LDAP Queries** option instructs the CounterACT RADIUS server to use Kerberos, version 5, for querying an Active Directory server about user group membership (LDAP-Group). By default, this option is: ▪ Disabled (not selected) when upgrading from a previous Network Module version ▪ Enabled (selected) for a new installation of the Network Module Upon selecting the **Enable Kerberos Authentication for LDAP Queries** option, the following option becomes available for selection: ▪ **Authenticate Using Machine Trust Account**

Field	Description
Authenticate Using Machine Trust Account (requires Kerberos)	Selecting the **Authenticate Using Machine Trust Account** option instructs the CounterACT RADIUS server to use the machine trust account of the CounterACT device, instead of using user directory credentials, in order to access an Active Directory server for purposes of querying the server about user group membership (LDAP-Group). By default, this option is: ▪ Disabled (not selected) when upgrading from a previous Network Module version ▪ Enabled (selected) for a new installation of the Network Module

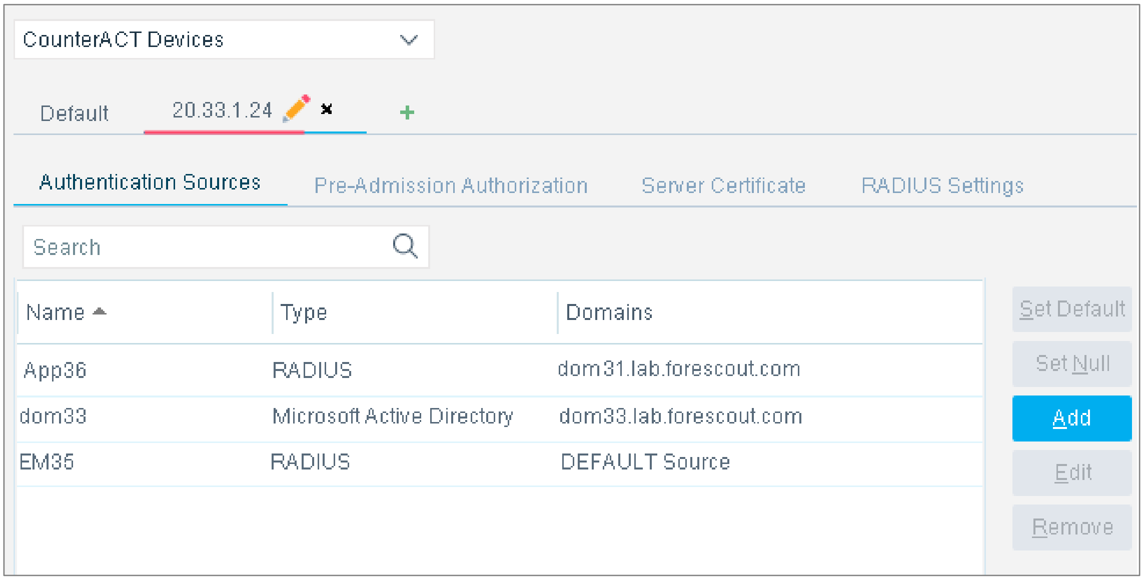
Per Appliance RADIUS Plugin Configuration

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

- Define, in the **Default** tab, a RADIUS Plugin configuration [Authentication Source, Pre-Admission Authorizations, Server Certificate and RADIUS Settings]. By default, this RADIUS Plugin configuration is designated to apply to all CounterACT devices that are not designated with a unique RADIUS Plugin configuration.
- Define additional, unique RADIUS Plugin configurations and designate each additional configuration to apply to either a single CounterACT device or multiple CounterACT devices.

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

- A **Default** configuration
- A configuration for Appliance **20.33.1.24**



Name	Type	Domains
App36	RADIUS	dom31.lab.forescout.com
dom33	Microsoft Active Directory	dom33.lab.forescout.com
EM35	RADIUS	DEFAULT Source

To create a unique 802.1X configuration for a single CounterACT device:

1. Select the plus-sign tab

. The **Select CounterACT devices to configure** dialog box opens and lists all your CounterACT devices [Enterprise Manager, Appliance$_1$ - Appliance$_n$].
2. Select a device and select **OK**. A tab for the selected Appliance appears. This tab contains the full complement of RADIUS Plugin configuration tabs [Authentication Source, Pre-Admission Authorizations, Server Certificate and RADIUS Settings].

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

1. Select the Plus-sign tab

. The **Select CounterACT devices to configure** dialog box opens and lists all your CounterACT devices [Enterprise Manager, Appliance$_1$ - 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 RADIUS Plugin configuration tabs [Authentication Source, Pre-Admission Authorizations, Server Certificate and RADIUS Settings].

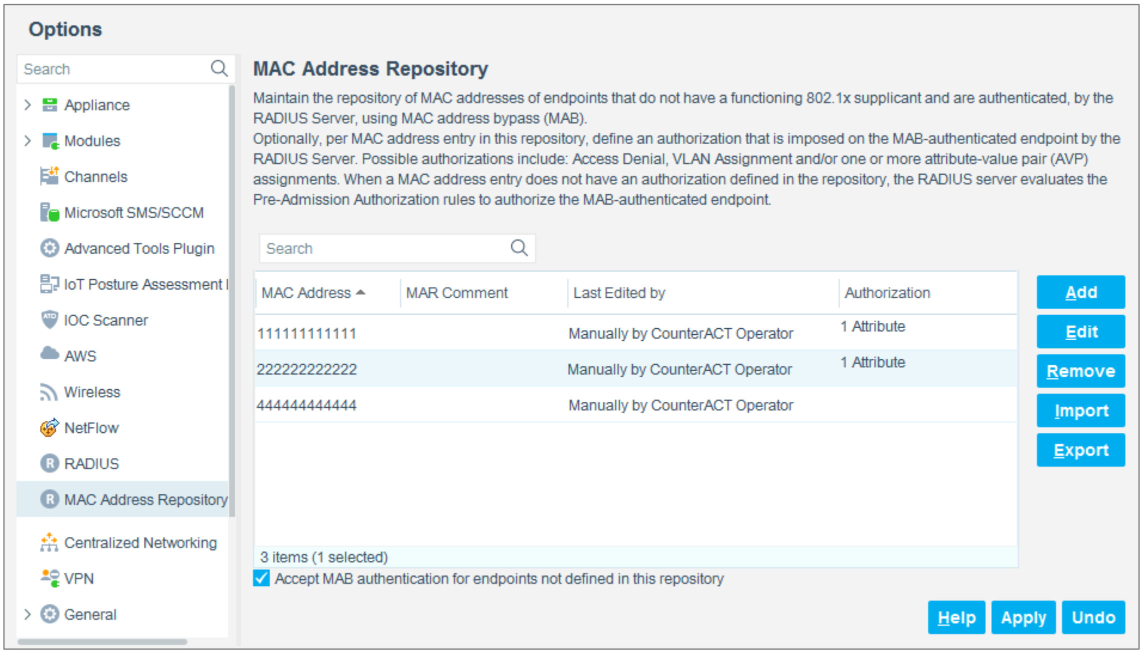
To edit settings of a unique 802.1X configuration:

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 RADIUS 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).



MAC Address Repository

Maintain the repository of MAC addresses of endpoints that do not have a functioning 802.1x supplicant and are authenticated, by the 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 RADIUS Server. Possible authorizations include: Access Denial, 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 RADIUS server evaluates the Pre-Admission Authorization rules to authorize the MAB-authenticated endpoint.

MAC Address ▲	MAR Comment	Last Edited by	Authorization
111111111111		Manually by CounterACT Operator	1 Attribute
222222222222		Manually by CounterACT Operator	1 Attribute
444444444444		Manually by CounterACT Operator	

3 items (1 selected)

☑ Accept MAB authentication for endpoints not defined in this repository

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.

Column	Description
MAC Address	The MAC address of the endpoint, which authenticates using MAB.
MAR Comment	(Optional) Descriptive comment about the endpoint.

Column	Description
Last Edited By	Read-only information. Identifies the method last used to either add or edit the MAR entry. Possible methods are: ▪ ***Manually by CounterACT Operator***: CounterACT user manually added/edited the MAR entry. ▪ ***CounterACT Policy***: The *802.1X Update MAR* action, whether initiated by policy or manually by user, added/edited the MAR entry ▪ ***Imported***: The entry was imported into the MAR. 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.
Authorization	(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. 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.

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.

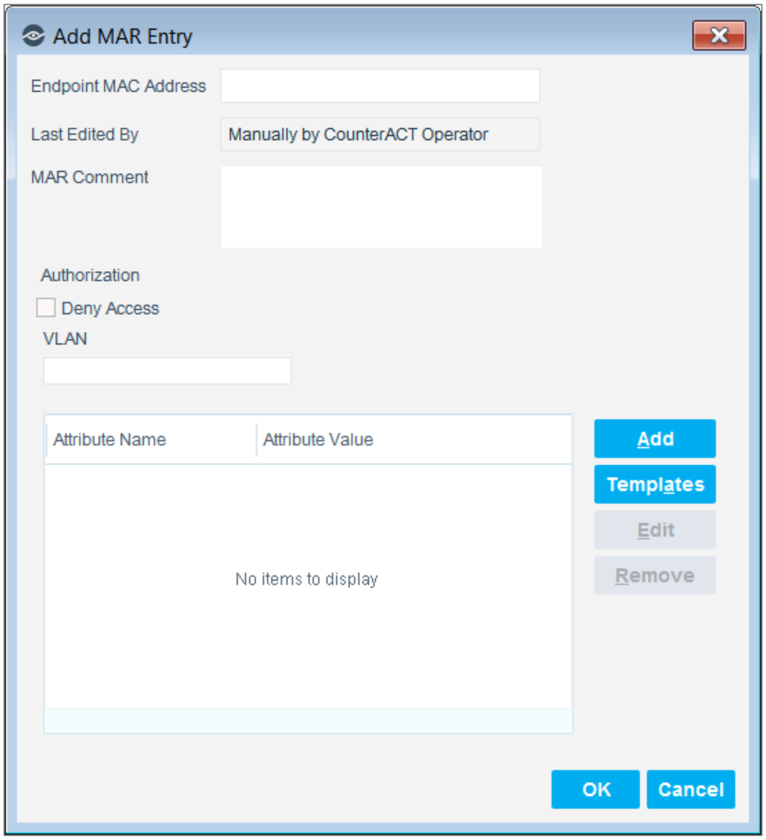
b. Apply the defined information/setting update to both existing MAR entries and to new MAR entries

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.



Add MAR Entry

Endpoint MAC Address

Last Edited By: Manually by CounterACT Operator

MAR Comment

Authorization

□ Deny Access

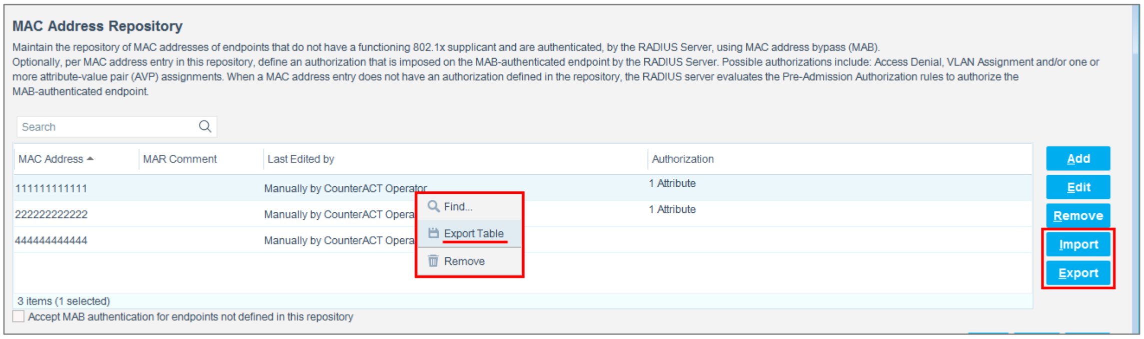
VLAN

Attribute Name	Attribute Value
No items to display	

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 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.



MAC Address Repository

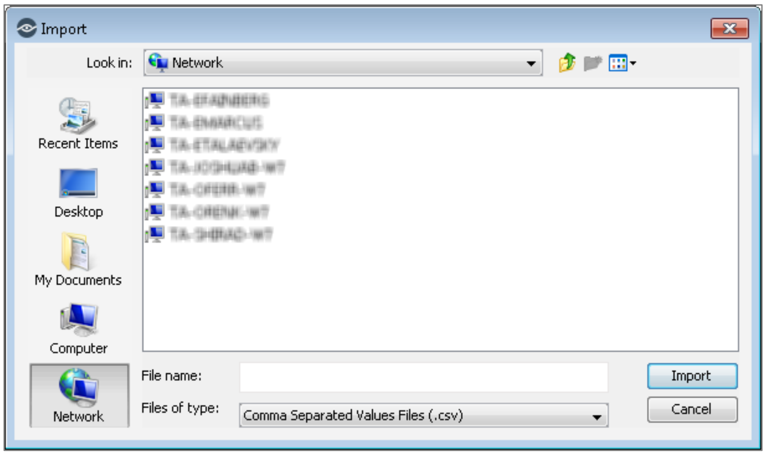
Maintain the repository of MAC addresses of endpoints that do not have a functioning 802.1x supplicant and are authenticated, by the RADIUS Server, using MAC address bypass (MAB).
Optionally, per MAC address entry in this repository, define an authorization that is imposed on the MAB-authenticated endpoint by the RADIUS Server. Possible authorizations include: Access Denial, 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 RADIUS server evaluates the Pre-Admission Authorization rules to authorize the MAB-authenticated endpoint.

MAC Address ▲	MAR Comment	Last Edited by	Authorization
111111111111		Manually by CounterACT Operator	1 Attribute
222222222222		Manually by CounterACT Opera	1 Attribute
444444444444		Manually by CounterACT Opera	

3 items (1 selected)

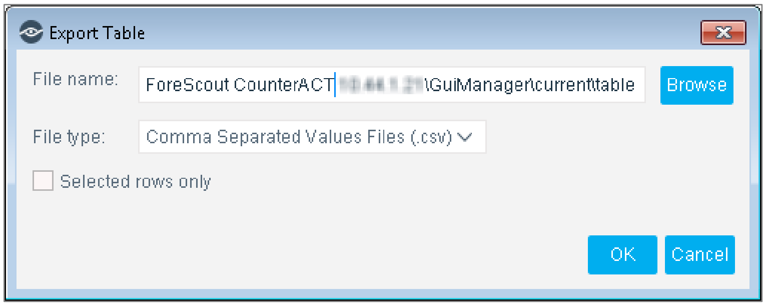
□ Accept MAB authentication for endpoints not defined in this repository

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 to method use.

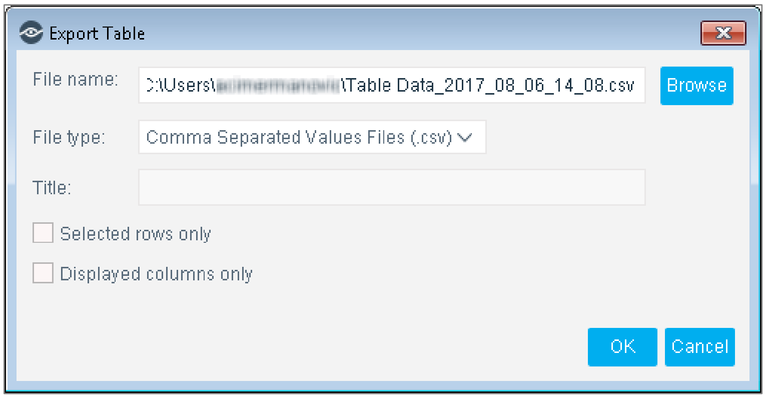


File name: ForeScout CounterACT [redacted]\GuiManager\current\table

File type: Comma Separated Values Files (.csv)

□ Selected rows only

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


Export Table

File name: :\Users\[redacted]\Table Data_2017_08_06_14_08.csv

File type: Comma Separated Values Files (.csv)

Title:

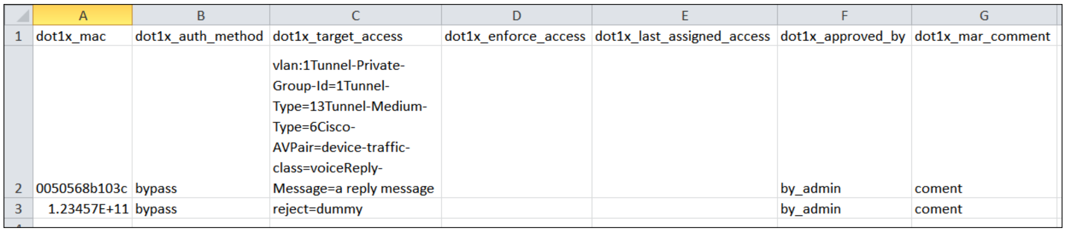
□ Selected rows only

□ Displayed columns only

Use the following guidelines when creating a **.csv** file of MAR entries to import:

MAR Entry Field	CSV File Column Name	CSV File Field Value
MAC Address	**dot1x_mac** Required field column	Enter a MAC address. Information displays in MAR.
	dot1x_auth_method Required field column	Enter the text **bypass**. Information does not display in MAR. By definition, all MAR entries authenticate using MAC authentication bypass (MAB).
Authorization	**dot1x_target_access** Optional field column	▪ Keep field entry blank. ▪ After successfully importing the **.csv** file into the MAR, add MAR entry authorizations, by doing either one of the following activities: **>** In the Console, manually add required MAR entry authorizations. See Manual Entries. **>** Contact ForeScout Customer Support for assistance. Information displays in MAR.
	dot1x_enforce_access	Keep field entry blank.
	dot1x_last_assigned_access	Keep field entry blank.
Last Edited By	**dot1x_approved_by** Required field column	Enter the phrase **by_import**. Information displays in MAR.
MAR Comment	**dot1x_mar_comment** Optional field column	Enter any descriptive text. Information displays in MAR.

Sample **.csv** file for MAR import:



	A	B	C	D	E	F	G
1	dot1x_mac	dot1x_auth_method	dot1x_target_access	dot1x_enforce_access	dot1x_last_assigned_access	dot1x_approved_by	dot1x_mar_comment
2	0050568b103c	bypass	vlan:1Tunnel-Private-Group-Id=1Tunnel-Type=13Tunnel-Medium-Type=6Cisco-AVPair=device-traffic-class=voiceReply-Message=a reply message			by_admin	coment
3	1.23457E+11	bypass	reject=dummy			by_admin	coment

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.

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

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

Testing and Troubleshooting

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

- Test Full Plugin Configuration
- Troubleshooting Policy Templates

Test Full Plugin Configuration

The full test of the plugin configuration accomplishes the following:

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

- The plugin tests the functionality of each authentication source with each relevant CounterACT device. For test details, see Test Authentication Source Functionality.

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

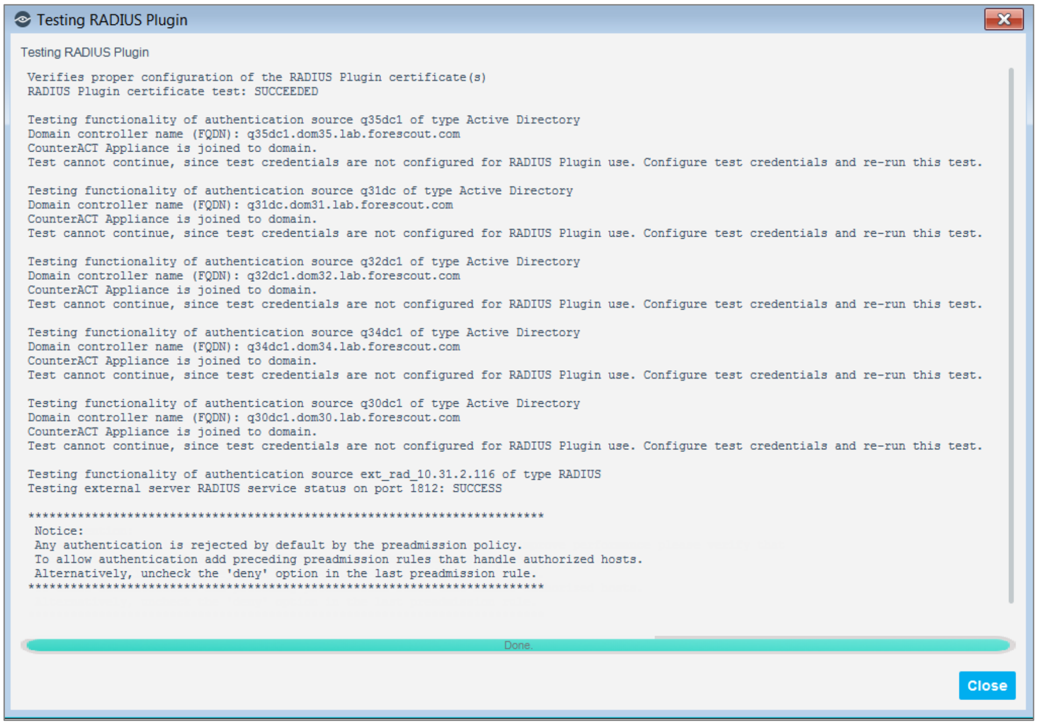
- The plugin joined each CounterACT device to the Active Directory domain(s), using the credentials previously defined using the Join button
- You have defined and provisioned a valid RADIUS server certificate for each CounterACT device

To run the test:

1. In the Console Modules pane, select the **Authentication** module. The plugins, which are installed as part of the CounterACT Authentication Module, display beneath the Authentication entry.
2. In the Modules pane, select the **RADIUS** entry from the table listing.
3. Select **Test**.
4. Select **Yes** to answer the following Console dialog question:

   Do you want to test the following plugins:

   – **RADIUS**
5. The test proceeds and the **Testing RADIUS Plugin** window opens and displays test results.



```
Verifies proper configuration of the RADIUS Plugin certificate(s)
RADIUS Plugin certificate test: SUCCEEDED

Testing functionality of authentication source q35dc1 of type Active Directory
Domain controller name (FQDN): q35dc1.dom35.lab.forescout.com
CounterACT Appliance is joined to domain.
Test cannot continue, since test credentials are not configured for RADIUS Plugin use. Configure test credentials and re-run this test.

Testing functionality of authentication source q31dc of type Active Directory
Domain controller name (FQDN): q31dc.dom31.lab.forescout.com
CounterACT Appliance is joined to domain.
Test cannot continue, since test credentials are not configured for RADIUS Plugin use. Configure test credentials and re-run this test.

Testing functionality of authentication source q32dc1 of type Active Directory
Domain controller name (FQDN): q32dc1.dom32.lab.forescout.com
CounterACT Appliance is joined to domain.
Test cannot continue, since test credentials are not configured for RADIUS Plugin use. Configure test credentials and re-run this test.

Testing functionality of authentication source q34dc1 of type Active Directory
Domain controller name (FQDN): q34dc1.dom34.lab.forescout.com
CounterACT Appliance is joined to domain.
Test cannot continue, since test credentials are not configured for RADIUS Plugin use. Configure test credentials and re-run this test.

Testing functionality of authentication source q30dc1 of type Active Directory
Domain controller name (FQDN): q30dc1.dom30.lab.forescout.com
CounterACT Appliance is joined to domain.
Test cannot continue, since test credentials are not configured for RADIUS Plugin use. Configure test credentials and re-run this test.

Testing functionality of authentication source ext_rad_10.31.2.116 of type RADIUS
Testing external server RADIUS service status on port 1812: SUCCESS

*************************************************************************
 Notice:
 Any authentication is rejected by default by the preadmission policy.
 To allow authentication add preceding preadmission rules that handle authorized hosts.
 Alternatively, uncheck the 'deny' option in the last preadmission rule.
*************************************************************************
```

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 CounterACT Administration 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.
- Verification of the certificate provided by the endpoint supplicant identifies that this certificate is revoked by the issuing certificate authority.
- Authorization denial (after being authenticated). A denial of access has any one of the following CounterACT sources:
  - Policy action authorization
  - MAR authorization
  - Pre-admission authorization rule

Prerequisites

Before you run a policy based on this template:

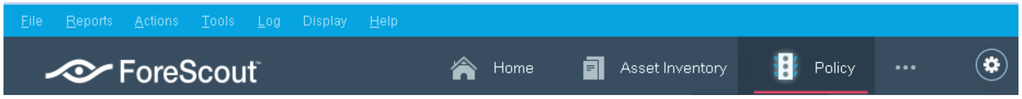
- It is recommended to run *802.1X Readiness* policies and that network devices and endpoints were determined ready for 802.1X authentication.
- Verify that the RADIUS Plugin is running and 802.1X endpoint authentication is operating in the organization's network.
- (***Optional***) To identify rejections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

Run the Template

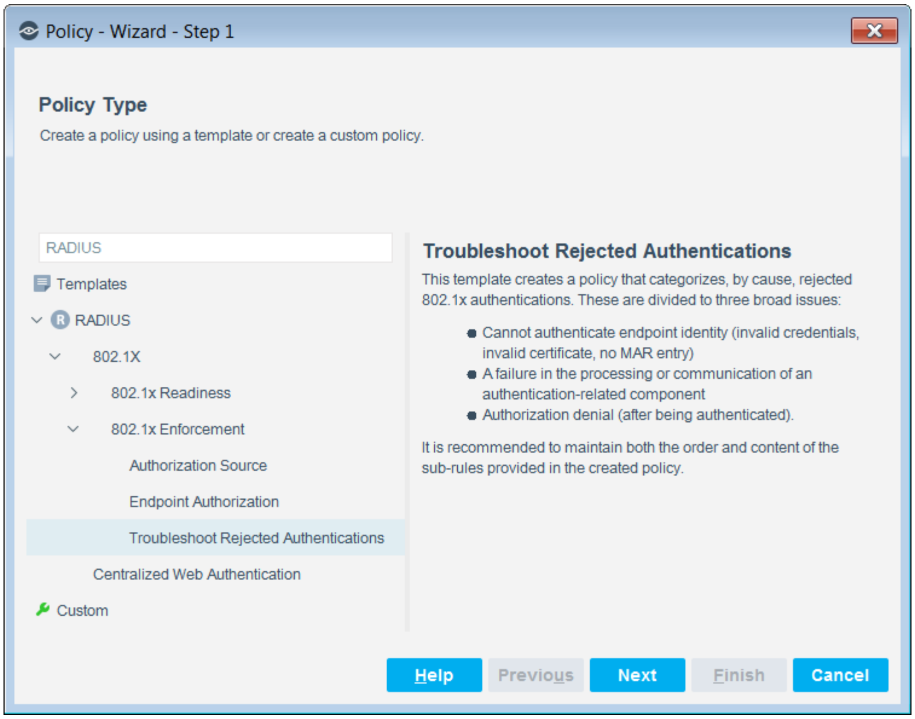
This section describes how to create a policy based on the template.

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 **RADIUS** > **802.1X** > **802.1X Enforcement** and then select **Troubleshoot Rejected Authentications**.



Policy Type

Create a policy using a template or create a custom policy.

Troubleshoot Rejected Authentications

This template creates a policy that categorizes, by cause, rejected 802.1x authentications. These are divided to three broad issues:

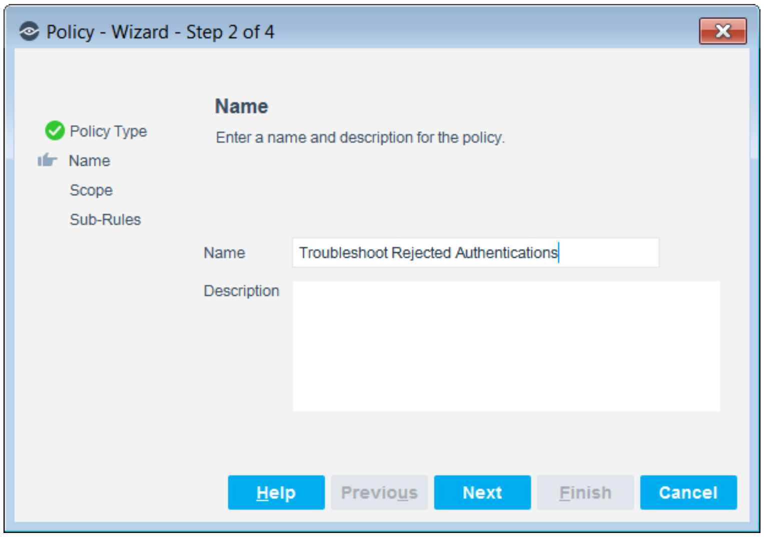
- Cannot authenticate endpoint identity (invalid credentials, invalid certificate, no MAR entry)
- A failure in the processing or communication of an authentication-related component
- Authorization denial (after being authenticated).

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

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, Reports and in other features. Precise names make working with policies and reports more efficient.



Policy - Wizard - Step 2 of 4

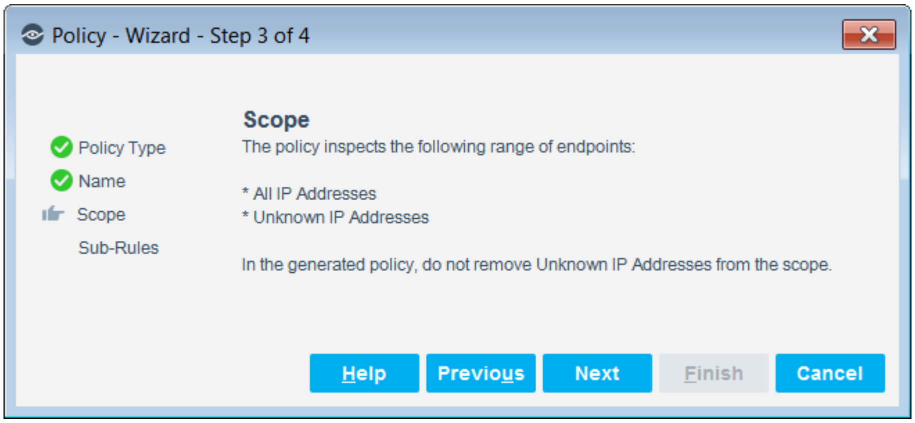
Name

Enter a name and description for the policy.

Name: Troubleshoot Rejected Authentications

Description:

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.



Policy - Wizard - Step 3 of 4

Scope

The policy inspects the following range of endpoints:

* All IP Addresses
* Unknown IP Addresses

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

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

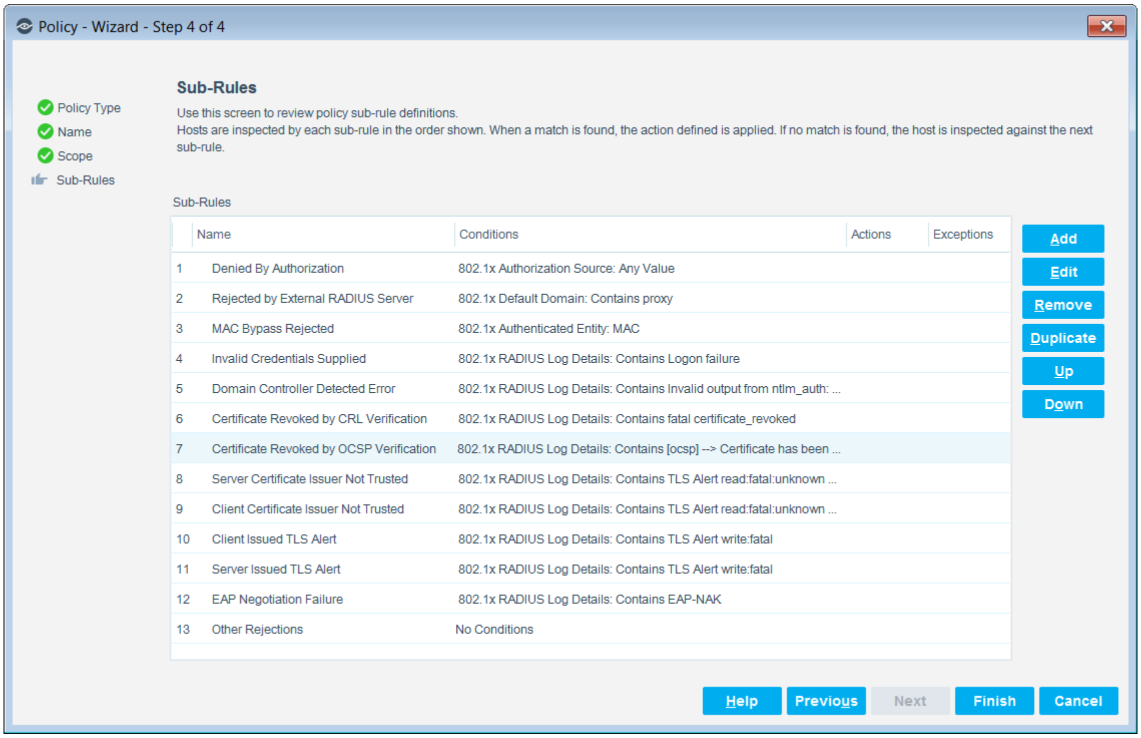
CounterACT-detected endpoints that meet the following criterion match the main rule of this policy:

- 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 Home view.*

Troubleshoot Rejected Authentications Sub Rules

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



Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	Denied By Authorization	802.1x Authorization Source: Any Value		
2	Rejected by External RADIUS Server	802.1x Default Domain: Contains proxy		
3	MAC Bypass Rejected	802.1x Authenticated Entity: MAC		
4	Invalid Credentials Supplied	802.1x RADIUS Log Details: Contains Logon failure		
5	Domain Controller Detected Error	802.1x RADIUS Log Details: Contains Invalid output from ntlm_auth: ...		
6	Certificate Revoked by CRL Verification	802.1x RADIUS Log Details: Contains fatal certificate_revoked		
7	Certificate Revoked by OCSP Verification	802.1x RADIUS Log Details: Contains [ocsp] --> Certificate has been ...		
8	Server Certificate Issuer Not Trusted	802.1x RADIUS Log Details: Contains TLS Alert read:fatal:unknown ...		
9	Client Certificate Issuer Not Trusted	802.1x RADIUS Log Details: Contains TLS Alert read:fatal:unknown ...		
10	Client Issued TLS Alert	802.1x RADIUS Log Details: Contains TLS Alert write:fatal		
11	Server Issued TLS Alert	802.1x RADIUS Log Details: Contains TLS Alert write:fatal		
12	EAP Negotiation Failure	802.1x RADIUS Log Details: Contains EAP-NAK		
13	Other Rejections	No Conditions		

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.*

Sub-Rule Name	Description
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 RADIUS Plugin. The MAR is the plugin's warehouse of endpoints that authenticate using MAB.
4. Invalid Credentials Supplied	Endpoints matching this sub-rule had their authentication rejected by the RADIUS server. ***CAUSE***: Either computer-supplied or user-supplied credentials did not match the credentials in the Active Directory of the domain.
5. Domain Controller Detected Error	Endpoints matching this sub-rule had their authentication rejected by the *CounterACT* RADIUS server. ***CAUSE***: The domain controller did not provide an adequate response to the RADIUS server.
6. Certificate Revoked by CRL Verification	Endpoints matching this sub-rule had their authentication rejected by the *CounterACT* RADIUS server. ***CAUSE***: Certificate verification by CRL reported that the issuing certificate authority *revoked* the certificate provided by the endpoint supplicant

Sub-Rule Name	Description
7. Certificate Revoked by OCSP Verification	Endpoints matching this sub-rule had their authentication rejected by the *CounterACT* RADIUS server. ***CAUSE***: Certificate verification by the issuing certificate authority, accomplished by OCSP, reported that the certificate provided by the endpoint supplicant is *revoked*.
8. Server Certificate Issuer Not Trusted	Endpoints matching this sub-rule had their authentication rejected by the *CounterACT* RADIUS server. ***CAUSE***: The endpoint supplicant did not trust the certificate authority that issued the RADIUS server's server certificate.
9. Client Certificate Issuer Not Trusted	Endpoints matching this sub-rule had their authentication rejected by the *CounterACT* RADIUS server. ***CAUSE***: The RADIUS server did not trust the certificate authority that issued the endpoint supplicant's client certificate.
10. Client Issued TLS Alert	Endpoints matching this sub-rule had their authentication rejected by the *CounterACT* RADIUS server. ***CAUSE***: The endpoint supplicant stopped the TLS handshake with the RADIUS server. This might indicate that the server certificate is invalid.
11. Server Issued TLS Alert	Endpoints matching this sub-rule had their authentication rejected by the *CounterACT* RADIUS server. ***CAUSE***: The RADIUS server stopped the TLS handshake with the endpoint supplicant. This might indicate that the client certificate is invalid.
12. EAP Negotiation Failure	Endpoints matching this sub-rule had their authentication rejected by the *CounterACT* RADIUS server. ***CAUSE***: 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.

Sub-Rule Name	Description
13. 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 for review/analysis.

To send test failure output:

1. Log in to the CounterACT device CLI.
2. Run the following commands:
   a. fstool tech-support debug dot1x --level 6
   b. **`fstool dot1x test normal`**

   Test results display in the screen.
3. Copy the test output and paste it into a text file.
4. Send this file to ForeScout technical support.

Plugin Properties and Custom Policies

This section provides information about the following plugin topics:

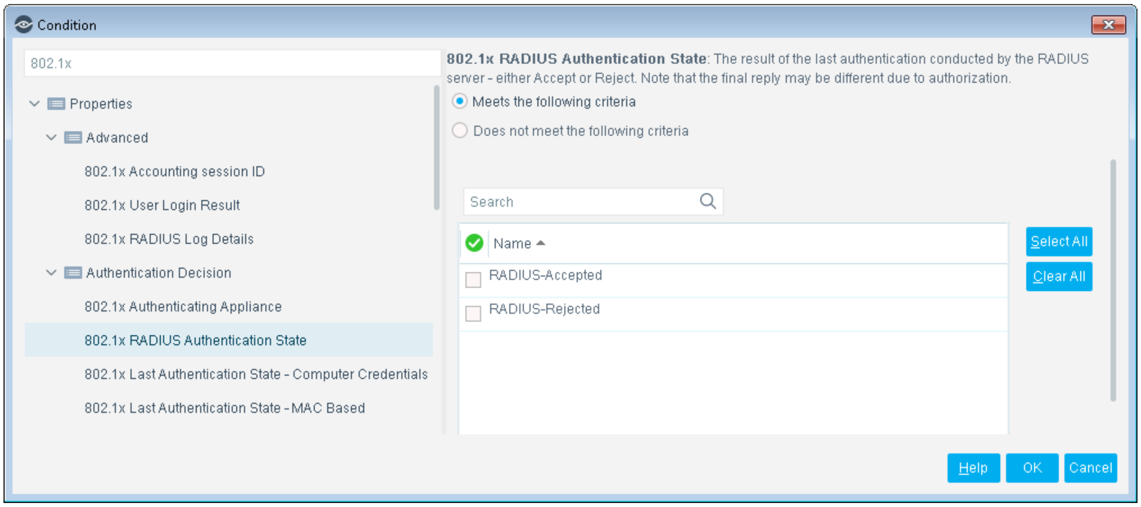
- Properties for Use in Policy Conditions
- Create Custom Policies

Properties for Use in Policy Conditions

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


Condition
802.1x
Properties
Advanced
802.1x Accounting session ID
802.1x User Login Result
802.1x RADIUS Log Details
Authentication Decision
802.1x Authenticating Appliance
802.1x RADIUS Authentication State
802.1x Last Authentication State - Computer Credentials
802.1x Last Authentication State - MAC Based
Search
Name
Select All
Clear All
Help
OK
Cancel

802.1x RADIUS Authentication State: The result of the last authentication conducted by the RADIUS server - either Accept or Reject. Note that the final reply may be different due to authorization.

● Meets the following criteria

○ Does not meet the following criteria

□ RADIUS-Accepted

□ RADIUS-Rejected

Advanced

Property	Description
802.1X Accounting Session Id	The **Accounting Session Id**, RADIUS attribute **(44)**, used on the last accounting request.
802.1X RADIUS Log Details:	Lists Debug Log Messages of the last, failed authentication.
802.1X User Login Result	User credentials validation result, according to the **ntlm_auth** process.

Authentication Decision

Property	Description
802.1X Authenticating Appliance	The IP address of the appliance performing the authentication.
802.1X Last Authentication State - Computer Credentials	The result of the last authentication attempt made by the endpoint using computer credentials. ▪ **RADIUS-Accepted** – The RADIUS server successfully authenticated the endpoint. ▪ **RADIUS-Rejected** – The endpoint failed to authenticate with the RADIUS server.

Property	Description
802.1X Last Authentication State - MAC Based	The result of the last authentication attempt made by the endpoint using its MAC address (MAB). ▪ **`RADIUS-Accepted`** – The RADIUS server successfully authenticated the endpoint. ▪ **`RADIUS-Rejected`** – The endpoint failed to authenticate with the RADIUS server.
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

Property	Description
802.1X Authenticated Entity	What entity was authenticated: ▪ **`User - Authenticated`** using user credentials ▪ **`Computer - Authenticated`** using computer credentials ***Note***: For computer authentication of a Macintosh endpoint, the plugin always resolves this property as **`User`**. ▪ **`MAC - Authenticated`** using MAC address bypass (MAB).
802.1X Authenticating Domain	The domain that the plugin used for endpoint 802.1X authentication.
802.1X Authentication Type	Identifies the selected **EAP Type** in the last authentication. Supported types are: ▪ EAP-TLS ▪ MAB ▪ PEAP ▪ PEAP-EAP-TLS
802.1X Calling Station Id	**`Calling-Station-Id`**, RADIUS attribute **`(31)`**, used on last authentication request
802.1X Default Domain	Per Appliance handling 802.1X authentication, the domain configured for the ***default*** authenticating user directory. This information is defined in the Authentication Source tab of the RADIUS Plugin.

Property	Description
802.1X Host Name	The **`User-Name`**, RADIUS attribute **`(1)`**, used in last authentication request, when computer credentials are used to authenticate.
802.1X Reauthentication Method	The method used with the last re-authentication of the endpoint. For plugin supported methods, see Re-Authentication Methods.
802.1X Requested Domain	The domain that an endpoint requested to be used for 802.1X authentication.
802.1X Tunneled User Name	The user name used for the inner authentication phase of both Protected EAP-MSCHAPv2 and Protected EAP-TLS authentication processes. Usually both inner and outer user names are the same. However, when the supplicant's **Identity Privacy** field is configured, then the inner user-name (the Tunneled User Name) is the supplicant's true user name.
802.1X User Name	The **`User-Name`**, RADIUS attribute **`(1)`**, used in last authentication request.

Authentication Events

Property	Description
802.1X Last Authentication Time	The last time an authentication completed for the endpoint with either a **`RADIUS Accept`** or **`RADIUS Reject`** message.
802.1X Last Authorize Action Failure	The last time the *RADIUS Authorize* action failed.
802.1X Last Rejected Authentication Time	The last time an authentication completed with **`RADIUS-Reject`** for this endpoint.
802.1X Last Successful Authentication Time	The last time an authentication completed with **`RADIUS-Accept`** for this endpoint.

Authorization

Property	Description
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 *RADIUS Authorize* action, for example, reported errors, re-authentication handling information and success/failure reason.

Property	Description
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 *RADIUS Authorize* action for the RADIUS server to impose on the endpoint.

Client Certificate

Property	Description
802.1X Client Cert Alternate Subject	Alternate Subject of the Client Certificate.
802.1X Client Cert commonName	Common-Name of the Client Certificate.
802.1X Client Cert Expiration	Expiration of the Client Certificate.
802.1X Client Cert Issuer	Issuer of the Client Certificate.
802.1X Client Cert Serial	Serial of the Client Certificate.
802.1X Client Cert Subject	Subject of the Client Certificate.

MAR

Property	Description
802.1X MAR Comment	Descriptive, free text defined in the MAR for this endpoint.
802.1X MAR Restrict To	The authorization defined in the MAR for this endpoint.

NAS Device

Property	Description
802.1X Called Station ID	The **`Called-Station-ID`**, RADIUS attribute **`(30)`**, used on the last authentication request.
802.1X Endpoint SSID	The **`WLAN SSID`** used in the 802.1X authentication.
802.1X NAS IP Address	The 802.1X **`NAS-IP-Address`**, RADIUS attribute **`(4)`**, as appears in the RADIUS Request (IPv4 address of the switch or the WiFi AP/Controller).
802.1X NAS IPv6 Address	The 802.1X **`NAS-IPv6-Address`**, RADIUS attribute **`(95)`**, as appears in the RADIUS Request (IPv6 address of the switch or the WiFi AP/Controller).

Property	Description
802.1X NAS Port Number	The **NAS-port**, 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 *association ID* is assigned to every mobile station upon a successful association exchange. As a result, for a wireless access point, if the association exchange was completed prior to authentication, then the **NAS-port** attribute contains the association ID, which is a 16 bit, unsigned integer.
802.1X NAS Port Type	The **NAS-port-type**, RADIUS attribute **(61)**, as appears in RADIUS Request. Supported port types are: ▪ Ethernet LAN ▪ Virtual ▪ Wireless LAN

Windows 7 Supplicant

Property	Description
Automatically use Windows logon, password and domain	Automatically use Windows login, password and domain.
Do not prompt user to authorize new servers or trusted certification authorities	Do not prompt user to authorize new servers or trusted certification authorities.
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

Property	Description
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.

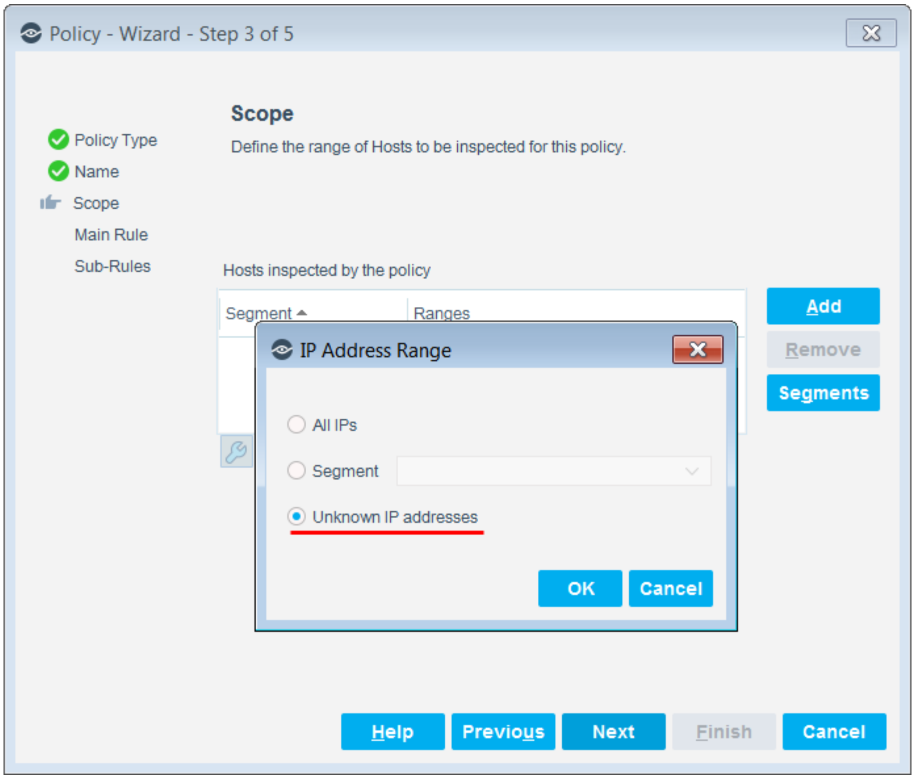
This section describes the policy properties that are available when the RADIUS Plugin is installed. For a description of the available actions, see Actions.

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.



Scope

Define the range of Hosts to be inspected for this policy.

Hosts inspected by the policy

○ All IPs

○ Segment

● Unknown IP addresses

The Unknown IP addresses option is available with CounterACT. Refer to CounterACT 8.0 Online Help for more information.

Actions

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

- RADIUS Authorize Action
- 802.1X Update MAR Action

RADIUS Authorize Action

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

An applied *RADIUS Authorize* action can be cancelled. When cancelling this action, the RADIUS Plugin removes the imposed authorization from the CounterACT RADIUS server's cache.

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

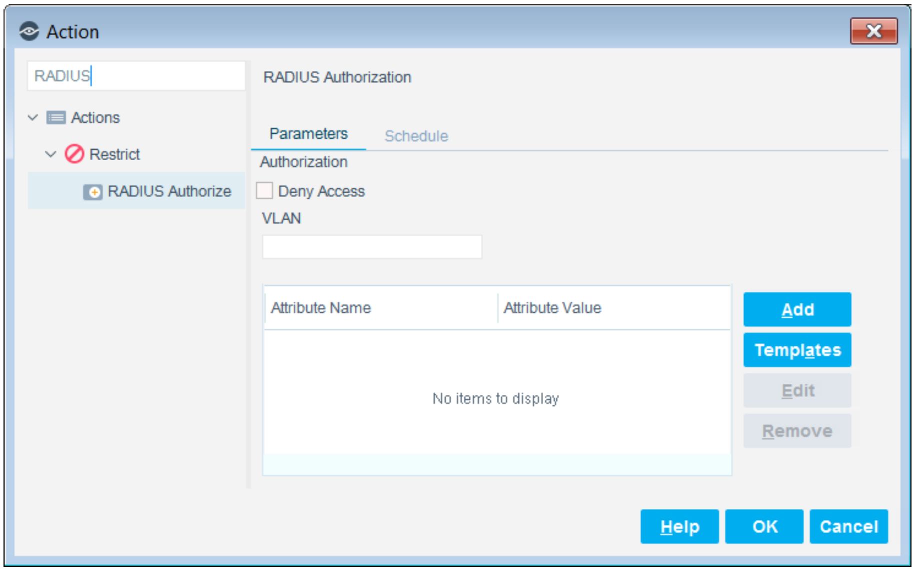
When none of the above CounterACT sources provide the CounterACT RADIUS server with the authorization to impose on an authenticated endpoint, the CounterACT RADIUS server does not include any authorization in its reply to the NAS device. In this case, the NAS device determines the authorization to impose 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 *RADIUS Authorize* action to evaluated endpoints found to match the sub-rule. It is recommended to tailor the authorization defined in each policy sub-rule *RADIUS Authorize* action, to address your organization's unique authorization needs.

To define authorization in the action:

1. 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 **RADIUS 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 Home view, right-click one or more selected endpoint entries.
   b. In the displayed menu, navigate to **Restrict** and select the **RADIUS Authorize** action. The action's Parameters tab opens.
   c. Continue with step 3.
3. In the Parameters tab, define any of the following authorization options:

Field	Description
Deny Access	For details about defining authorization options, see the table provided in Rule Authorization.
VLAN	
Attribute-Value Pair	



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 RADIUS Authorize Action

Cancelling the *RADIUS 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:

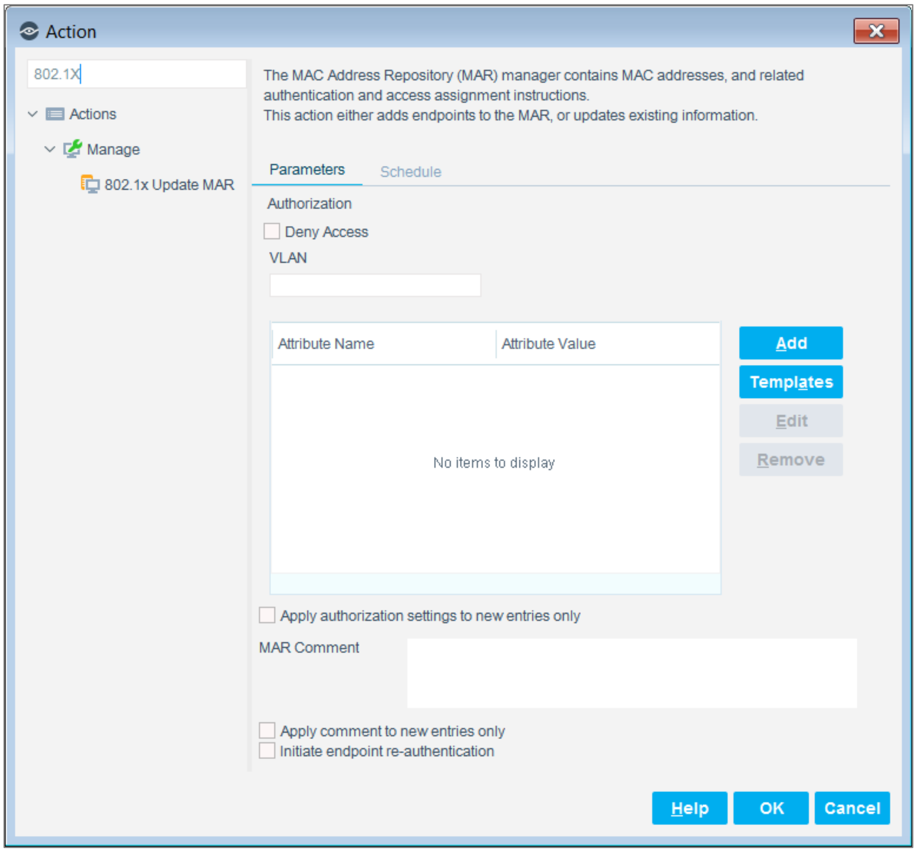
Column	Description
MAC Address	The MAC address of the endpoint, which authenticates using MAB.
MAR Comment	(Optional) Descriptive comment about the endpoint.
Last Edited By	Read-only information. Identifies the method last used to either add or edit the MAR entry. Possible methods are: ▪ ***Manually by CounterACT Operator***: CounterACT user manually added/edited the MAR entry. ▪ ***CounterACT Policy***: The *802.1X Update MAR* action, whether initiated by policy or manually by user, added/edited the MAR entry ▪ ***Imported***: The entry was imported into the MAR.
Authorization	(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.

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 Home view, right-click one or more selected endpoint entries.
   b. In the displayed menu, navigate to **Manage** and select the **802.1X Update MAR** action. The action's Parameters tab opens.
   c. Continue with step 3.
3. In the Parameters tab, define the following:

Field	Description
Deny Access	For details about defining authorization options, see the table provided in Rule Authorization.
VLAN	
Attribute-Value Pair	

Field	Description
Apply authorization settings to new entries only	Selecting this option instructs the CounterACT RADIUS server to impose the action's defined authorization only on MAR entries being added. If option is not selected, the action's defined authorization is imposed on both added and existing MAR entries being edited.
MAR Comment	Descriptive comment about the endpoint.
Apply comment to new entries only	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.
Initiate endpoint re-authentication	Selecting this option instructs the CounterACT RADIUS server to trigger the re-authentication (force DHCP renew) of the MAR entry (the endpoint), whether added or edited. Use this option alone or in combination with 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.



The MAC Address Repository (MAR) manager contains MAC addresses, and related authentication and access assignment instructions.
This action either adds endpoints to the MAR, or updates existing information.

Authorization

□ Deny Access

VLAN

No items to display

□ Apply authorization settings to new entries only

MAR Comment

□ Apply comment to new entries only

□ Initiate endpoint re-authentication

4. When defining the action in a policy, do the following:

   a. Select **OK**.

   b. Select **Apply** to save the updated plugin configuration.

Use Cases

This section presents information about the following plugin use cases:

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

Categorize Endpoint Authorizations

Read this section if you want to:

- Categorize authenticated endpoints according to their 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.

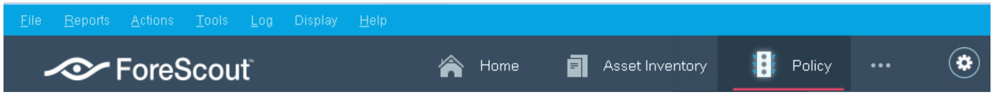
- Verify that the RADIUS Plugin is running and 802.1X endpoint authentication is operating in the organization's network.
- Verify that active 802.1X Endpoint Authorization policies have their sub-rule actions enabled.

Run the Template

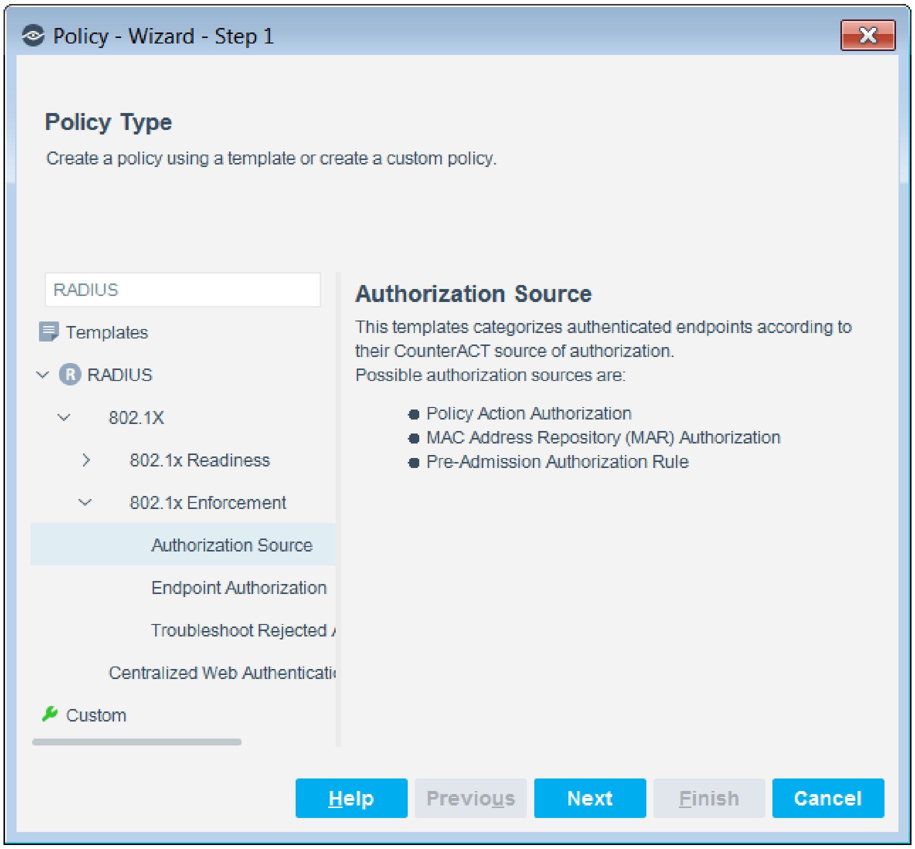
This section describes how to create a policy based on the template.

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 **RADIUS** > **802.1X** > **802.1X Enforcement** and then select **Authorization Source**.



Policy Type

Create a policy using a template or create a custom policy.

Authorization Source

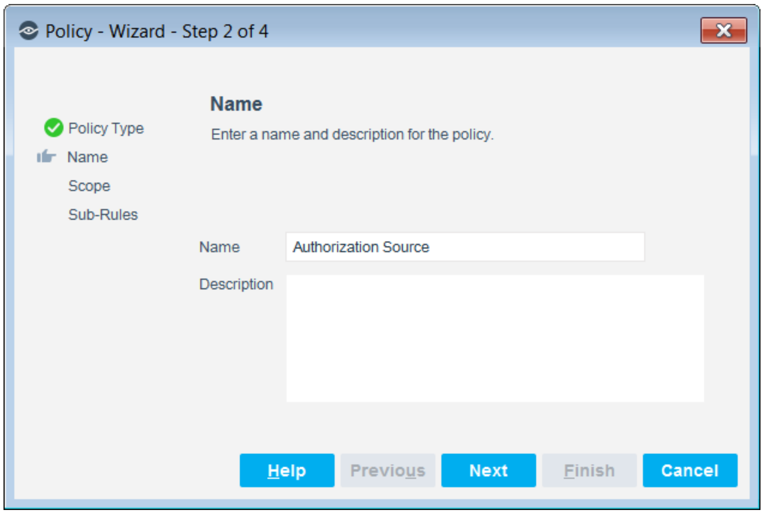
This templates categorizes authenticated endpoints according to their CounterACT source of authorization.
Possible authorization sources are:

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

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, Reports and in other features. Precise names make working with policies and reports more efficient.


Policy - Wizard - Step 2 of 4

Name

Enter a name and description for the policy.

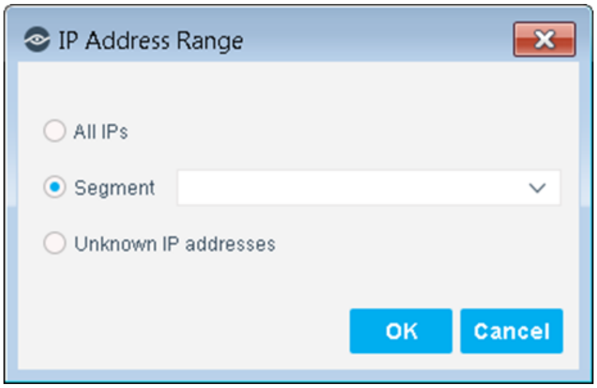
Name: Authorization Source

Description:

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

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


IP Address Range

○ All IPs

● Segment

○ Unknown IP addresses

Define Policy Scope

The following options are available:

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

You can filter the range by including only certain 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:

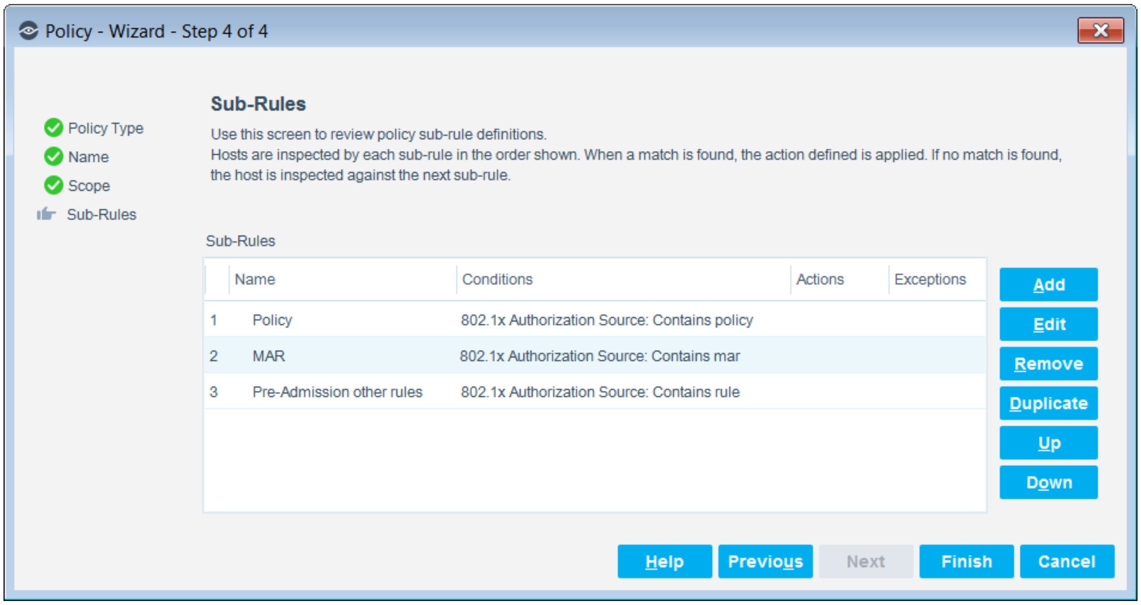
- Endpoint authentication state is accepted by the RADIUS server

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.



Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	Policy	802.1x Authorization Source: Contains policy		
2	MAR	802.1x Authorization Source: Contains mar		
3	Pre-Admission other rules	802.1x Authorization Source: Contains rule		

Endpoints authorizations are inspected against each sub-rule in the order listed, as follows:

Sub-Rule Name	Description
1. Policy	Endpoints matching this sub-rule had their authorization supplied by the *RADIUS Authorize* action; application of this action could have been due to either policy evaluation or manually initiated by the CounterACT user.
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:

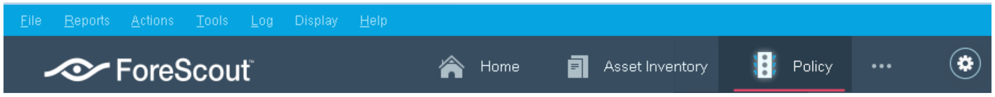
- It is recommended to run *802.1X Readiness* policies and that network devices and endpoints were determined ready for 802.1X authentication.
- Verify that the RADIUS Plugin is running and 802.1X endpoint authentication is operating in the organization's network.

Run the Template

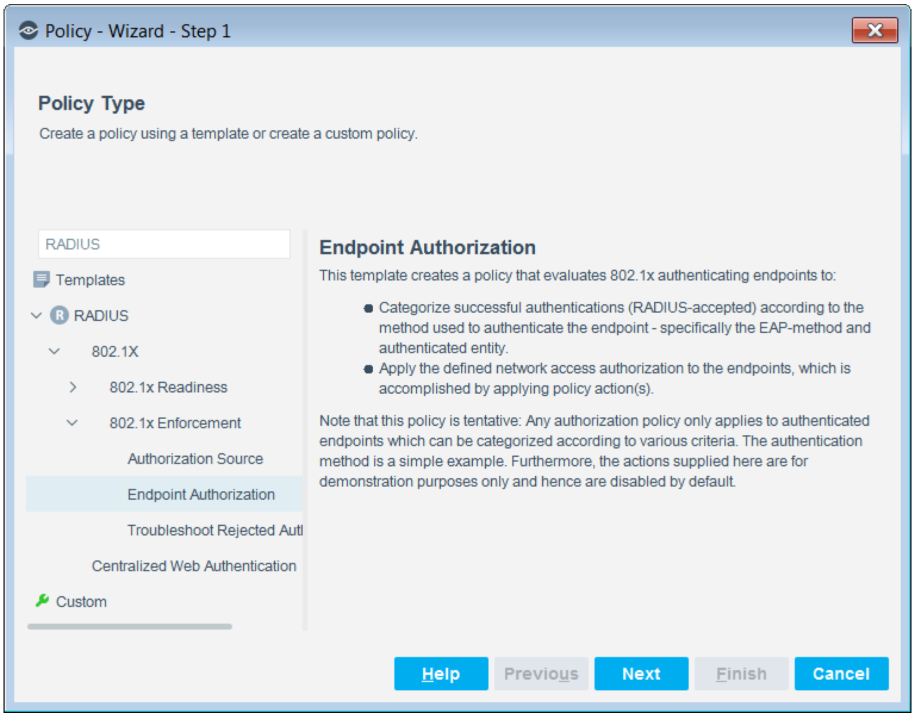
This section describes how to create a policy based on the template.

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 **RADIUS** > **802.1X** > **802.1X Enforcement** and then select **Endpoint Authorization**.



Policy Type

Create a policy using a template or create a custom policy.

Endpoint Authorization

This template creates a policy that evaluates 802.1x authenticating endpoints to:

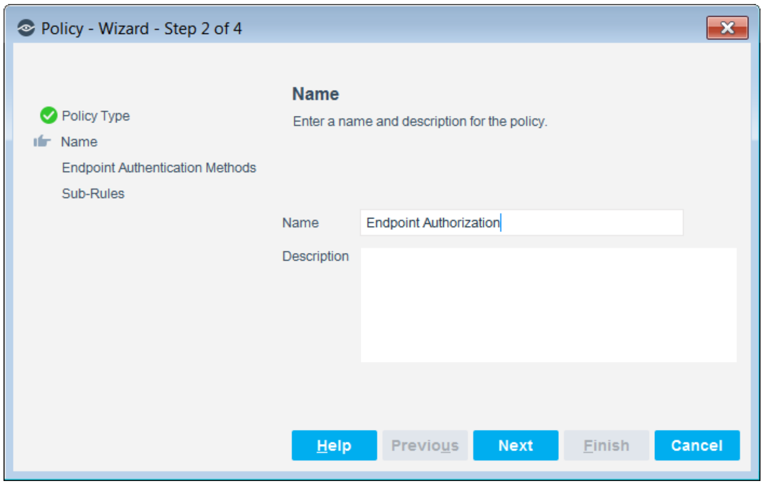
- Categorize successful authentications (RADIUS-accepted) according to the method used to authenticate the endpoint - specifically the EAP-method and authenticated entity.
- Apply the defined network access authorization to the endpoints, which is accomplished by applying policy action(s).

Note that this policy is tentative: Any authorization policy only applies to authenticated endpoints which can be categorized according to various criteria. The authentication method is a simple example. Furthermore, the actions supplied here are for demonstration purposes only and hence are disabled by default.

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, Reports and in other features. Precise names make working with policies and reports more efficient.


Policy - Wizard - Step 2 of 4
Policy Type
Name
Endpoint Authentication Methods
Sub-Rules
Help
Previous
Next
Finish
Cancel

Name

Enter a name and description for the policy.

Name: Endpoint Authorization

Description:

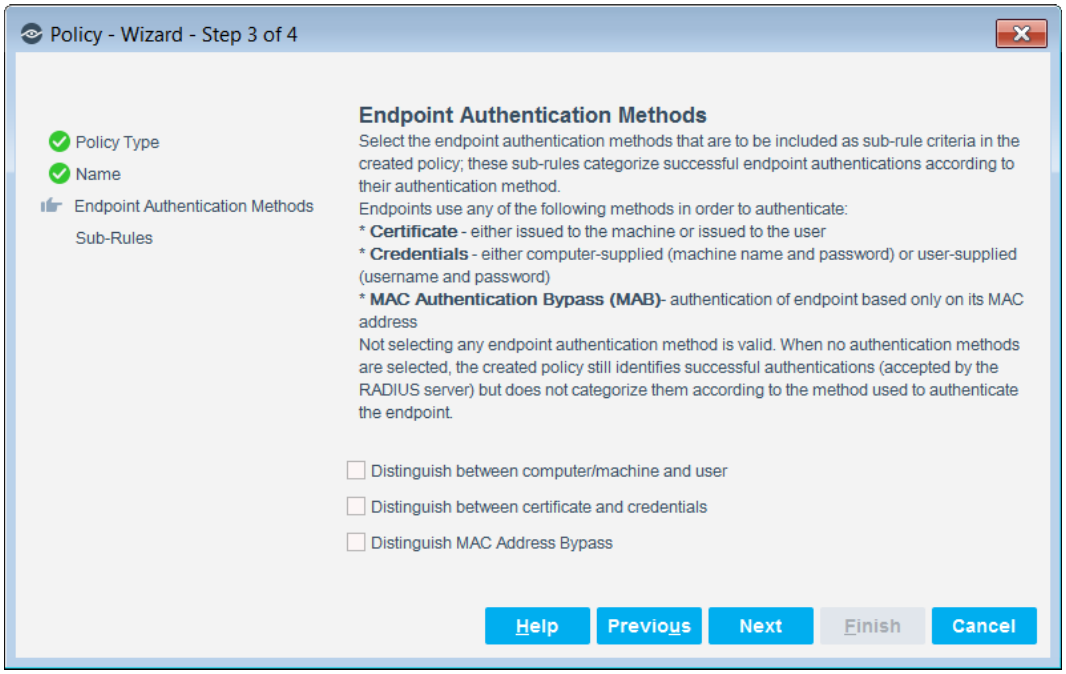
1. Define a unique name for the policy you are creating based on this template and enter a description.
   – Use a name that clearly reflects what the policy does. Use a descriptive name that identifies what your policy verifies and what actions will be taken.

- 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.


Policy - Wizard - Step 3 of 4
Policy Type
Name
Endpoint Authentication Methods
Sub-Rules
Help
Previous
Next
Finish
Cancel

Endpoint Authentication Methods

Select the endpoint authentication methods that are to be included as sub-rule criteria in the created policy; these sub-rules categorize successful endpoint authentications according to their authentication method.

Endpoints use any of the following methods in order to authenticate:

* **Certificate** - either issued to the machine or issued to the user

* **Credentials** - either computer-supplied (machine name and password) or user-supplied (username and password)

* **MAC Authentication Bypass (MAB)**- authentication of endpoint based only on its 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.

□ Distinguish between computer/machine and user

□ Distinguish between certificate and credentials

□ Distinguish MAC Address Bypass

1. Select the endpoint authentication methods that the policy uses to categorize successful endpoint authentications. The following options are available:
   - **Distinguish between computer/machine and user**: Categorize successful authentications accomplished using either computer/machine-provided information or user-provided information.
   - **Distinguish between certificate and credentials**: Categorize successful authentications accomplished using either a certificate or credentials.
   - **Distinguish MAC Address Bypass**: Categorize successful authentications accomplished based only on the endpoint MAC address.

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

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

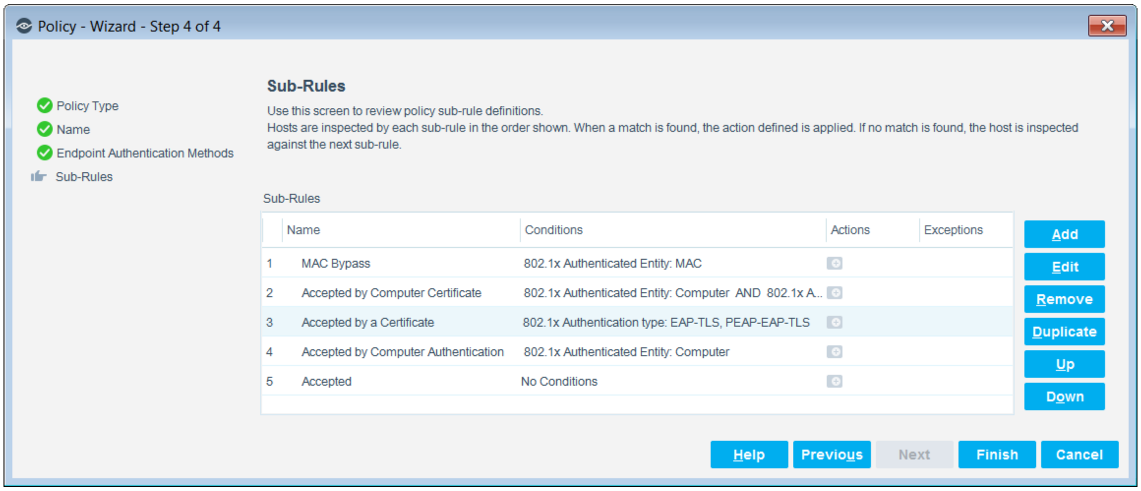
CounterACT-detected endpoints that meet the following criterion match the main rule of this policy:

- 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.



Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	MAC Bypass	802.1x Authenticated Entity: MAC	⊕	
2	Accepted by Computer Certificate	802.1x Authenticated Entity: Computer AND 802.1x A...	⊕	
3	Accepted by a Certificate	802.1x Authentication type: EAP-TLS, PEAP-EAP-TLS	⊕	
4	Accepted by Computer Authentication	802.1x Authenticated Entity: Computer	⊕	
5	Accepted	No Conditions	⊕	

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

Sub-Rule Name	Description
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 RADIUS Plugin. The MAR is the plugin's warehouse of endpoints that authenticate using MAC address bypass (MAB). If the *RADIUS Authorize* action of this sub-rule is enabled, the authorization defined in this action is imposed on matching endpoints. Edit the sub-rule action and review the defined authorization, provided by the policy template.
2. Accepted by Computer Certificate	Endpoints matching this sub-rule had their authentication accepted by the RADIUS server given the following conditions: ▪ A machine certificate was presented by the endpoint ▪ The network authentication method of the endpoint supplicant was **EAP-TLS** If the *RADIUS Authorize* action of this sub-rule is enabled, the authorization defined in this action is imposed on matching endpoints. Edit the sub-rule action and review the defined authorization, provided by the policy template.
3. Accepted by a Certificate	Endpoints matching this sub-rule had their authentication accepted by the RADIUS server given the following conditions: ▪ A client certificate (issued either to the machine or to the user) was presented by the endpoint. ▪ The network authentication method of the endpoint supplicant was **EAP-TLS** If the *RADIUS Authorize* action of this sub-rule is enabled, the authorization defined in this action is imposed on matching endpoints. Edit the sub-rule action and review the defined authorization, provided by the policy template.
4. Accepted by Computer Authentication	Endpoints matching this sub-rule had their authentication accepted by the RADIUS server given the following condition: ▪ Either computer-supplied credentials or a machine certificate was used to authenticate the endpoint. If the *RADIUS Authorize* action of this sub-rule is enabled, the authorization defined in this action is imposed on matching endpoints. Edit the sub-rule action and review the defined authorization, provided by the policy template.

Sub-Rule Name	Description
5. Accepted	Endpoints matching this sub-rule had their authentication accepted by the RADIUS server and used an authentication method not detected by any previous sub-rule. If the *RADIUS Authorize* action of this sub-rule is enabled, the authorization defined in this action is imposed on matching endpoints. Edit the sub-rule action and review the defined authorization, provided by the policy template.

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

- Deny Access only
- VLAN Assignment only
- VLAN Assignment and one or more attribute-value pair (AVP) assignments
- One or more attribute-value pair (AVP) assignments only

It is recommended to tailor the authorization defined in each sub-rule action of the policy you created using the Endpoint Authorization template, to address your organization's unique authorization needs. For information about defining authorization in the action, see Actions.

Corporate Wired and Wireless Authentication

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

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

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

- 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

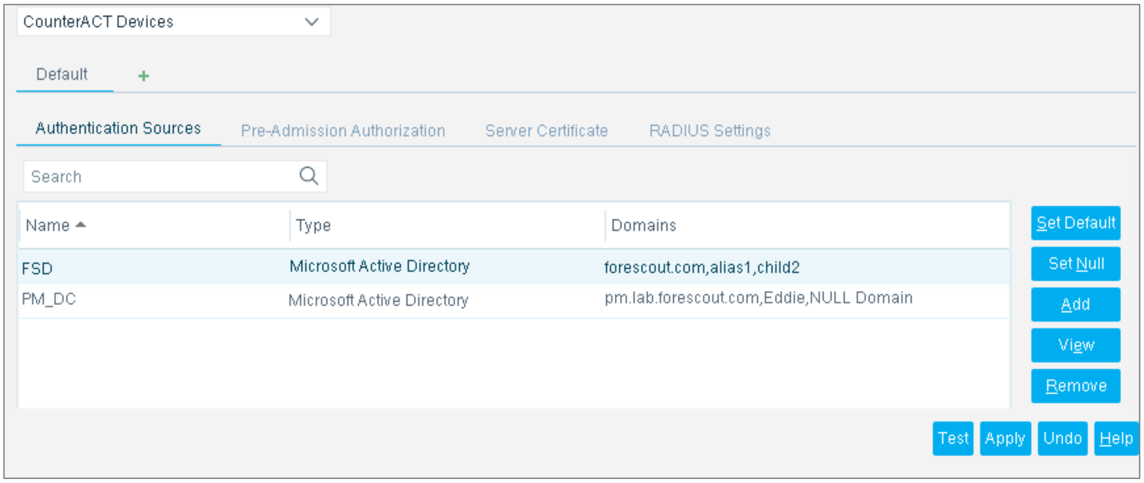
When the RADIUS Plugin (the CounterACT RADIUS server) must interoperate with multiple user directory domains, perform the following configuration tasks in the plugin's Authentication Sources tab:

- Add organizational domains as authentication sources; the available domains 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.

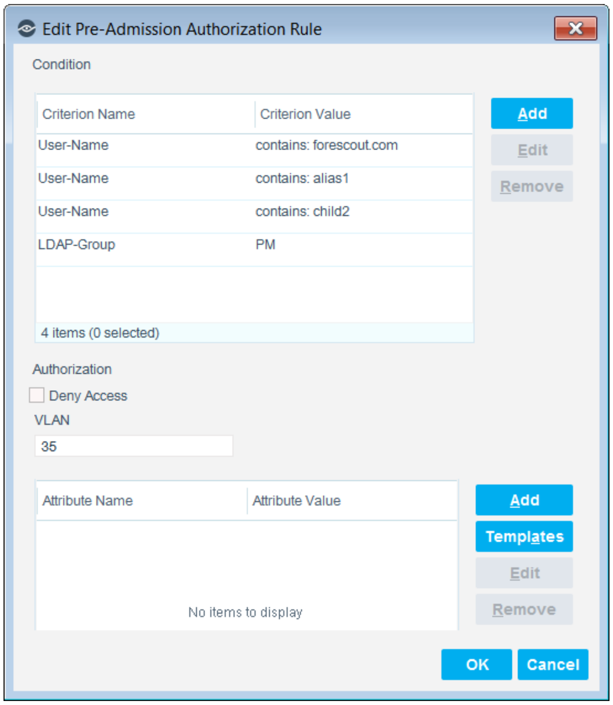
Pre-Admission Authorization in a Multi-Domain Environment

The following are several examples of pre-admission authorization rules that a CounterACT user might configure, when the RADIUS Plugin (the CounterACT RADIUS server) operates in a multi-domain environment. For details, see Configure Pre-Admission Authorization.



Name ▲	Type	Domains
FSD	Microsoft Active Directory	forescout.com,alias1,child2
PM_DC	Microsoft Active Directory	pm.lab.forescout.com,Eddie,NULL Domain

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



Condition

Criterion Name	Criterion Value
User-Name	contains: forescout.com
User-Name	contains: alias1
User-Name	contains: child2
LDAP-Group	PM

4 items (0 selected)

Authorization

☐ Deny Access

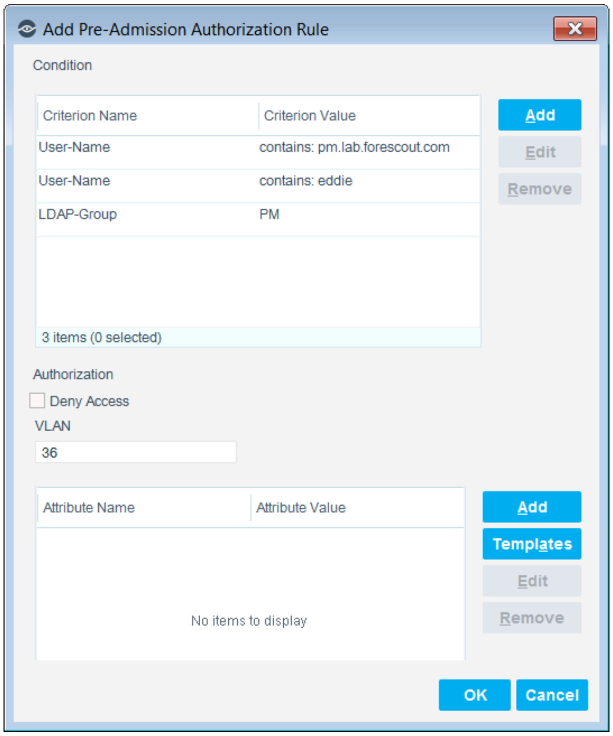
VLAN

35

Attribute Name	Attribute Value

No items to display

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



Criterion Name	Criterion Value
User-Name	contains: pm.lab.forescout.com
User-Name	contains: eddie
LDAP-Group	PM

3 items (0 selected)

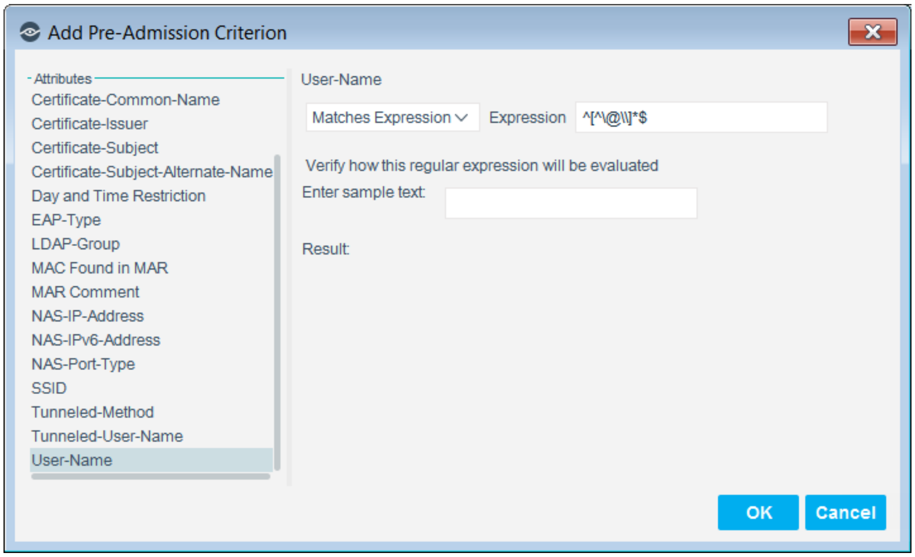
□ Deny Access

VLAN: 36

Attribute Name	Attribute Value

No items to display

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



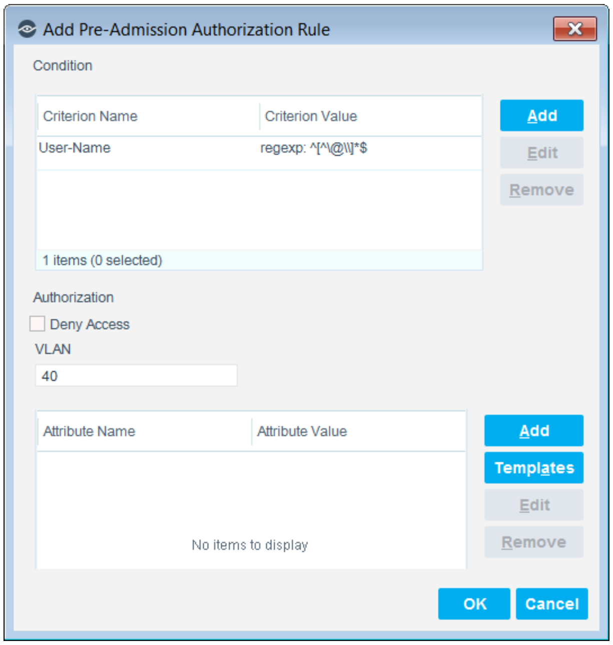
User-Name

Matches Expression   Expression: ^[^\@\\]*$

Verify how this regular expression will be evaluated

Enter sample text:

Result:



Add Pre-Admission Authorization Rule

Condition

Criterion Name	Criterion Value
User-Name	regexp: ^[^\@\\]*$

1 items (0 selected)

Authorization

□ Deny Access

VLAN

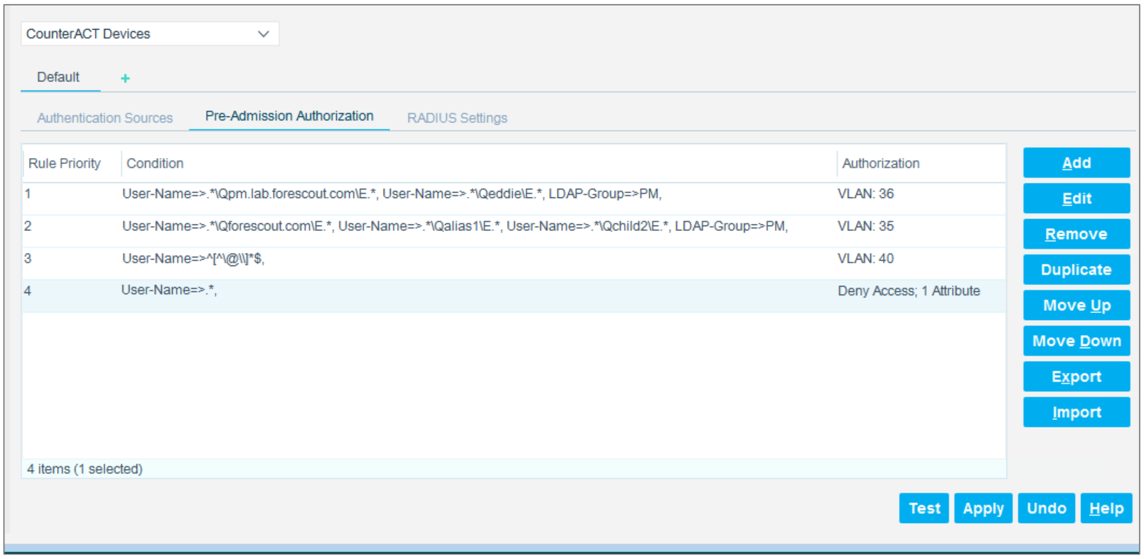
40

Attribute Name	Attribute Value

No items to display

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:



Rule Priority	Condition	Authorization
1	User-Name=>.*\Qpm.lab.forescout.com\E.*, User-Name=>.*\Qeddie\E.*, LDAP-Group=>PM,	VLAN: 36
2	User-Name=>.*\Qforescout.com\E.*, User-Name=>.*\Qalias1\E.*, User-Name=>.*\Qchild2\E.*, LDAP-Group=>PM,	VLAN: 35
3	User-Name=>^[^\@\\]*$,	VLAN: 40
4	User-Name=>.*,	Deny Access; 1 Attribute

4 items (1 selected)

CounterACT RADIUS Server as a Proxy

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

- Add the external RADIUS server as the authentication source; the available external RADIUS servers from which to select are configured in the User Directory Plugin.
- If you want to 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 *RADIUS 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 RADIUS 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 RADIUS Plugin.

🗎 *As of RADIUS Plugin version 4.2.0 (previously the 802.1X Plugin), IP-MAC visibility is solely provided 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 RADIUS Plugin to use MAC address bypass (MAB) to authenticate MAC addresses, which are received in RADIUS requests, that are not listed in the MAR. For 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.

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

Meraki Attribute-Value Pair for Rule Authorization

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

Vendor	Attribute	Value
Meraki	Cisco-AVPair	**url-redirect= http://${appliance_address}/captiveredirect/a?t=${client_token}** During expression evaluation, **{appliance_address}** is dynamically replaced with the FQDN of the CounterACT Appliance. This dynamic replacement requires that the option **Attempt to redirect using DNS name** is enabled on the Appliance (Options > NAC > HTTP Redirection > HTTP Redirection Settings).

Meraki Management Configuration

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

- Make sure that the CoA re-authentication method is enabled
- When the managing Appliance is not 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:

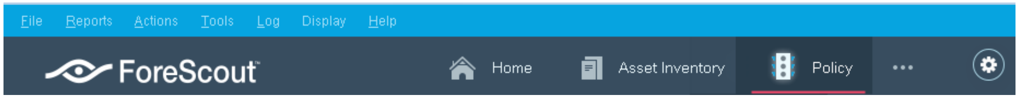
- Enable MAC Address Bypass
- Configure Pre-Admission Authorization Rule

Run the Template

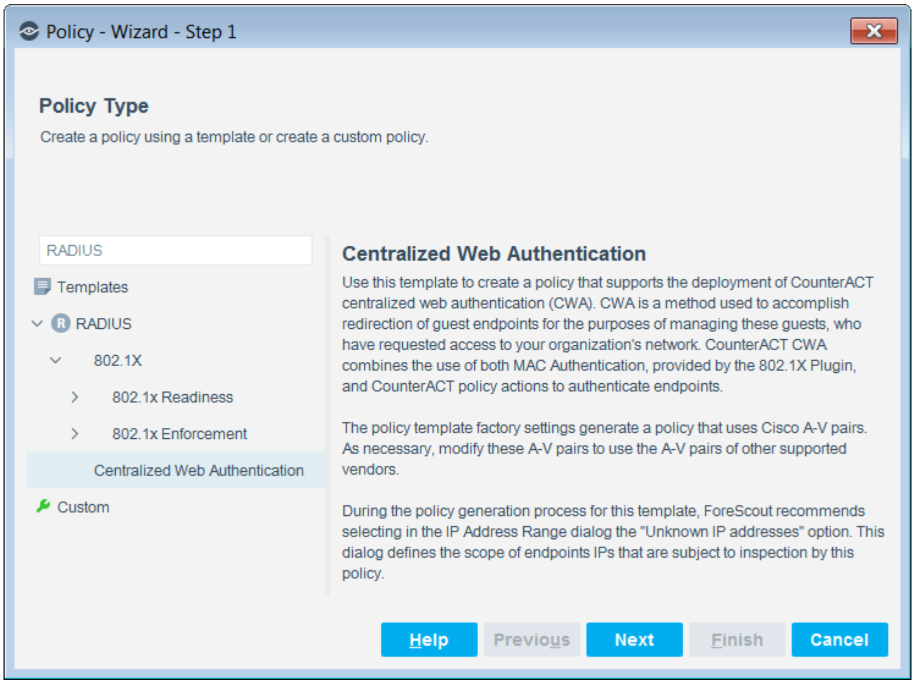
This section describes how to create a policy based on the template.

To run the template:

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



2. Select **Add**. The Policy Wizard opens.
3. In the navigation tree, select **RADIUS** and then select **Centralized Web Authentication**.



Policy Type

Create a policy using a template or create a custom policy.

Centralized Web Authentication

Use this template to create a policy that supports the deployment of CounterACT centralized web authentication (CWA). CWA is a method used to accomplish redirection of guest endpoints for the purposes of managing these guests, who have requested access to your organization's network. CounterACT CWA combines the use of both MAC Authentication, provided by the 802.1X Plugin, and CounterACT policy actions to authenticate endpoints.

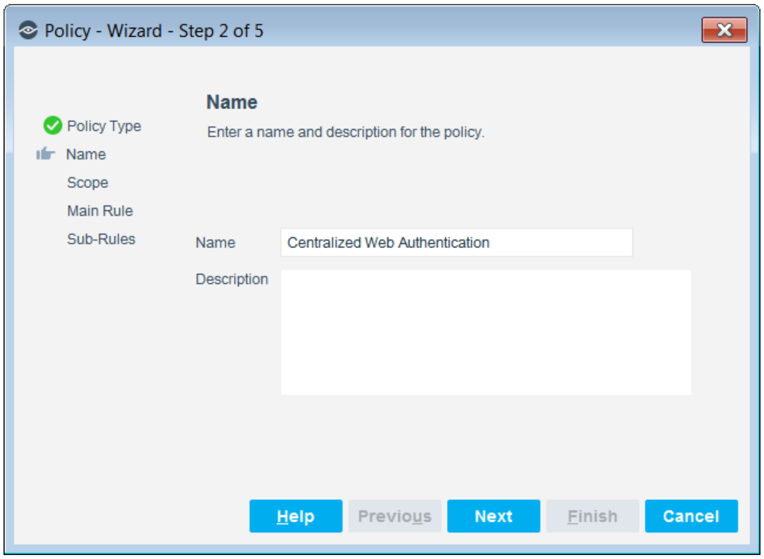
The policy template factory settings generate a policy that uses Cisco A-V pairs. As necessary, modify these A-V pairs to use the A-V pairs of other supported vendors.

During the policy generation process for this template, ForeScout recommends selecting in the IP Address Range dialog the "Unknown IP addresses" option. This dialog defines the scope of endpoints IPs that are subject to inspection by this policy.

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, Reports and in other features. Precise names make working with policies and reports more efficient.



Name

Enter a name and description for the policy.

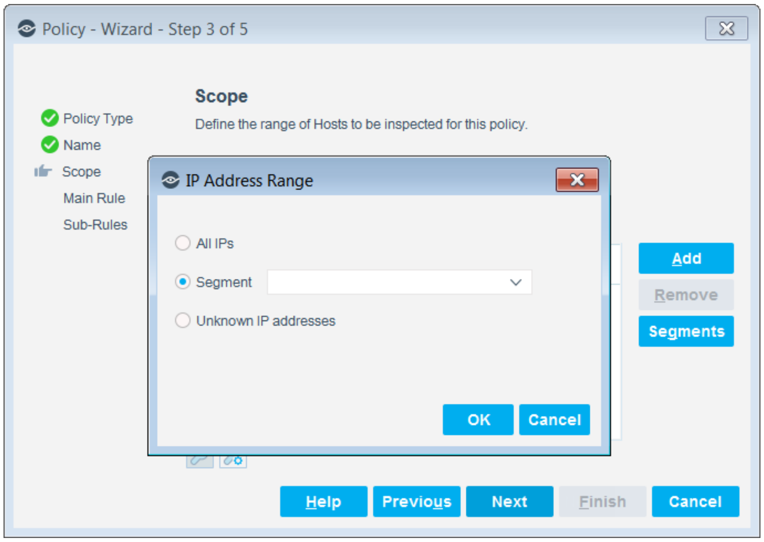
Name: Centralized Web Authentication

Description:

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.

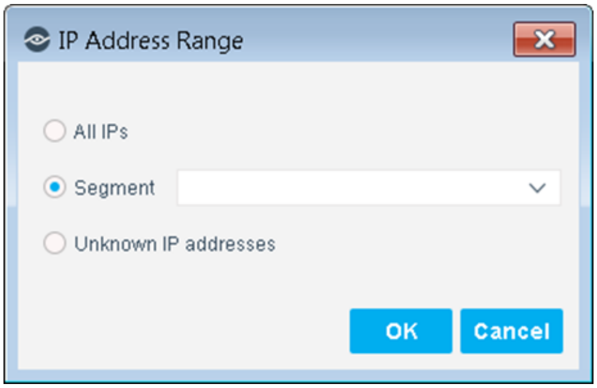


Policy - Wizard - Step 3 of 5

Scope

Define the range of Hosts to be inspected for this policy.

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



Define Policy Scope

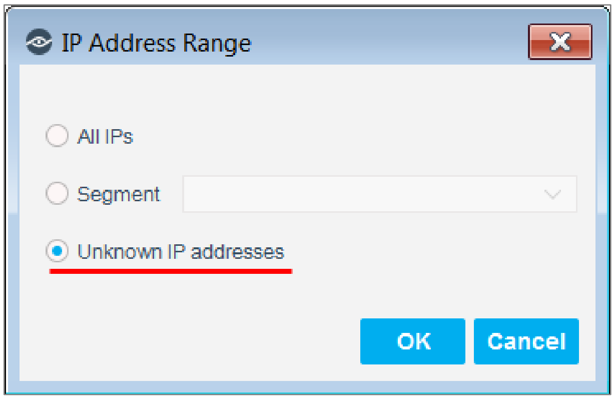
The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.

- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close this dialog box, and select **Segments** from the Scope page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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

When defining the policy scope, a best practice is to select the **Unknown IP addresses** option in the IP Address Range dialog box, *in addition to using any of the other IP address options*. The **Unknown IP addresses** option lets you detect and handle endpoints based on their MAC address when an IP address is not yet available to CounterACT.

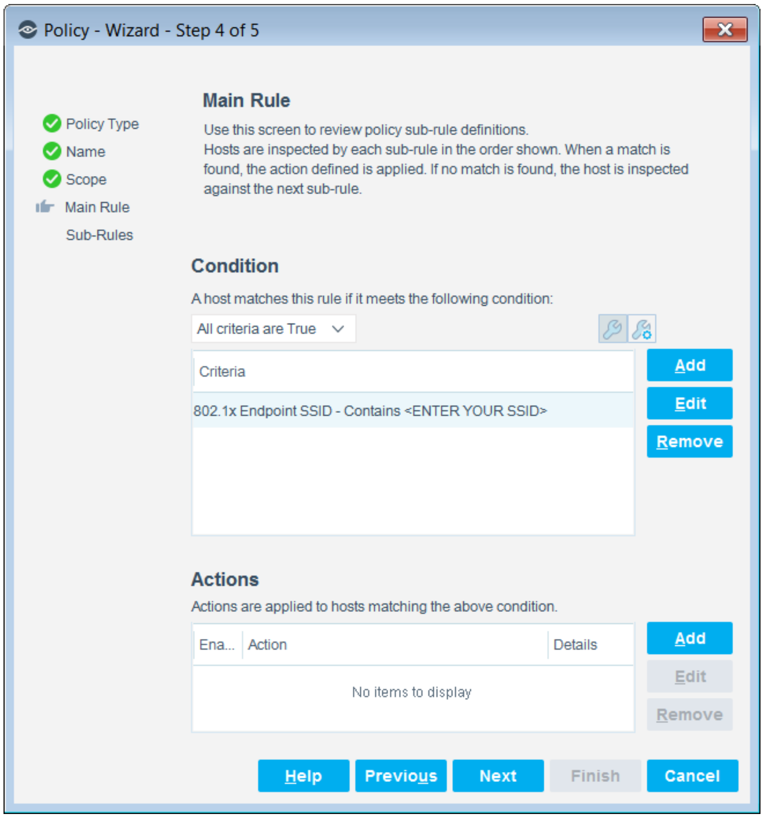


2. In the Scope page, select **Add** to re-open the IP Address Range dialog box and specify an additional *IP address option.*
3. Select **Next.** The Main Rule page opens

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*>



Main Rule

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
802.1x Endpoint SSID - Contains <ENTER YOUR SSID>

Actions

Actions are applied to hosts matching the above condition.

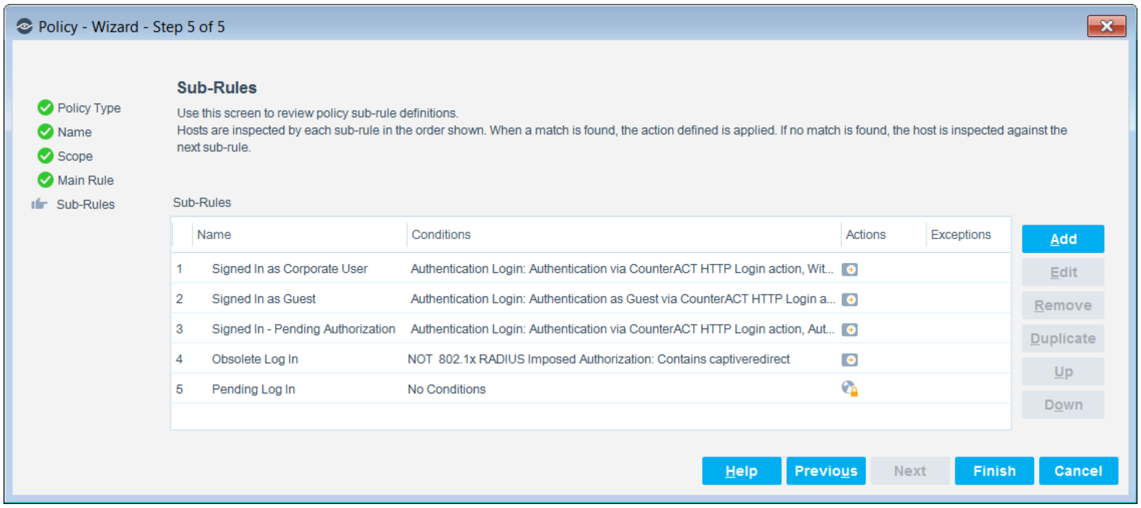
Ena...	Action	Details

No items to display

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.



Sub-Rules

Use this screen to review policy sub-rule definitions.

Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Sub-Rules

	Name	Conditions	Actions	Exceptions
1	Signed In as Corporate User	Authentication Login: Authentication via CounterACT HTTP Login action, Wit...	⊕	
2	Signed In as Guest	Authentication Login: Authentication as Guest via CounterACT HTTP Login a...	⊕	
3	Signed In - Pending Authorization	Authentication Login: Authentication via CounterACT HTTP Login action, Aut...	⊕	
4	Obsolete Log In	NOT 802.1x RADIUS Imposed Authorization: Contains captiveredirect	⊕	
5	Pending Log In	No Conditions	🔒	

Endpoints matching the policy main rule are inspected against each sub-rule in the order listed, as follows:

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

Sub-Rule Name	Description
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 *RADIUS 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 *RADIUS 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, refer to the User Directory Plugin Configuration Guide. See Additional CounterACT Documentation for information on how to access this guide.

EDU-ROAM

Edu-Roam (education roaming) is a world-wide roaming access service developed for the international research and education community. The service allows students, researchers and staff from participating institutions and cities to obtain Internet connectivity across town, campus and when visiting other participating institutions.

When the CounterACT RADIUS server must proxy to an external RADIUS server in support of an Edu-Roam deployment, use the following RADIUS Plugin configuration guidelines:

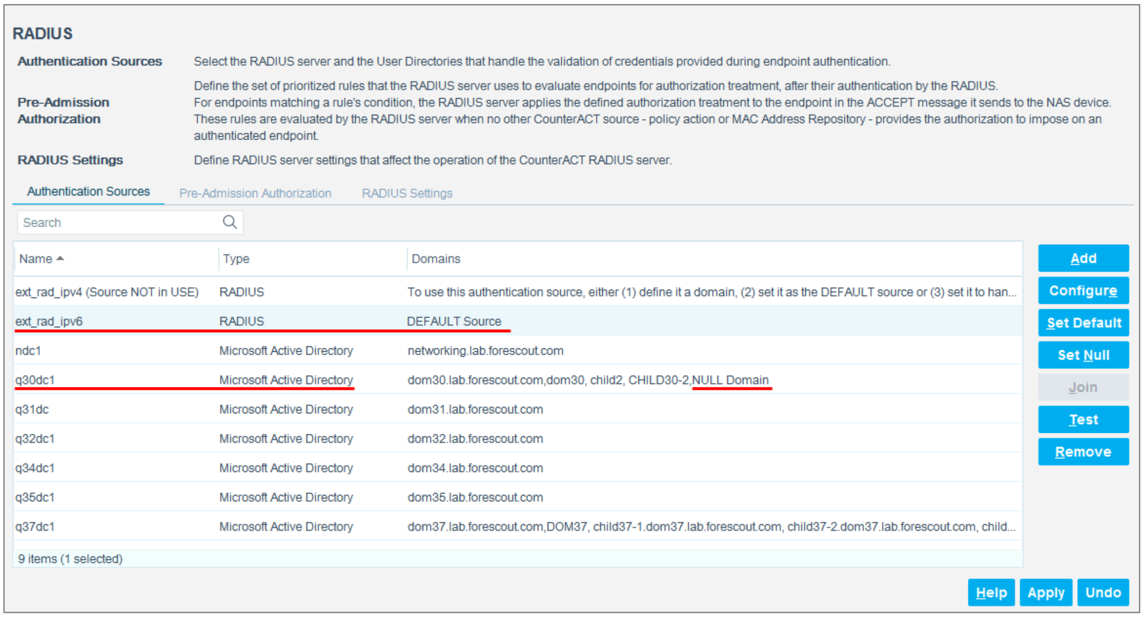
Authentication Sources

In the Authentication Sources tab, 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.



RADIUS

Authentication Sources Select the RADIUS server and the User Directories that handle the validation of credentials provided during endpoint authentication.

Pre-Admission Authorization Define the set of prioritized rules that the RADIUS server uses to evaluate endpoints for authorization treatment, after their authentication by the RADIUS. For endpoints matching a rule's condition, the RADIUS server applies the defined authorization treatment to the endpoint in the ACCEPT message it sends to the NAS device. These rules are evaluated by the RADIUS server when no other CounterACT source - policy action or MAC Address Repository - provides the authorization to impose on an authenticated endpoint.

RADIUS Settings Define RADIUS server settings that affect the operation of the CounterACT RADIUS server.

Name ▲	Type	Domains
ext_rad_ipv4 (Source NOT in USE)	RADIUS	To use this authentication source, either (1) define it a domain, (2) set it as the DEFAULT source or (3) set it to han...
ext_rad_ipv6	RADIUS	DEFAULT Source
ndc1	Microsoft Active Directory	networking.lab.forescout.com
q30dc1	Microsoft Active Directory	dom30.lab.forescout.com,dom30, child2, CHILD30-2,NULL Domain
q31dc	Microsoft Active Directory	dom31.lab.forescout.com
q32dc1	Microsoft Active Directory	dom32.lab.forescout.com
q34dc1	Microsoft Active Directory	dom34.lab.forescout.com
q35dc1	Microsoft Active Directory	dom35.lab.forescout.com
q37dc1	Microsoft Active Directory	dom37.lab.forescout.com,DOM37, child37-1.dom37.lab.forescout.com, child37-2.dom37.lab.forescout.com, child...

9 items (1 selected)

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*.

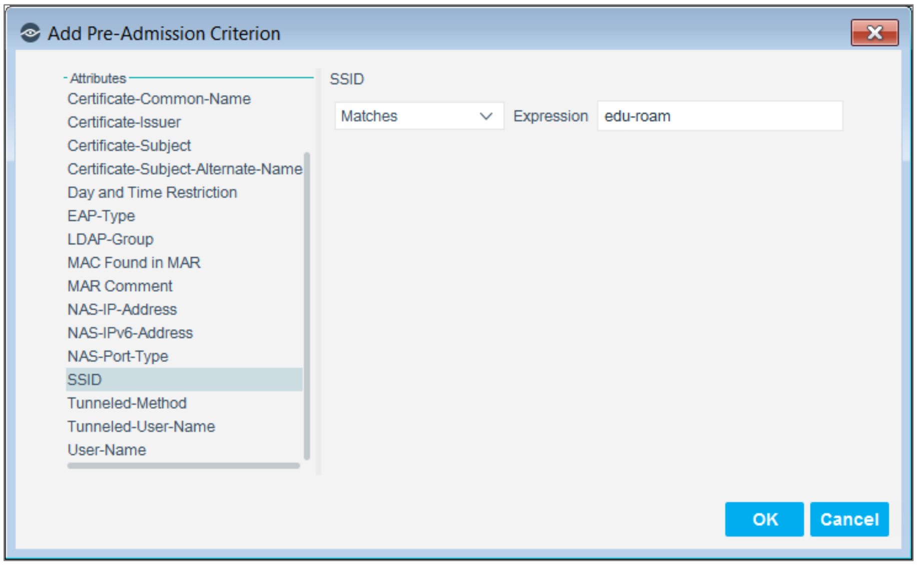
- Authorize local users, on **SSID** *edu-roam*, to access the organization's network.

  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.

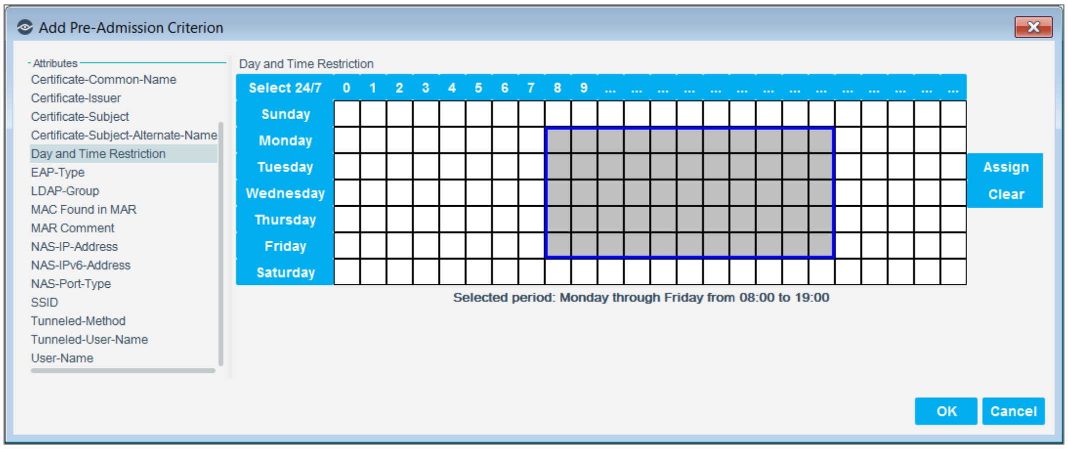
Edu-Roam Endpoint Authorization



Add Pre-Admission Criterion

SSID

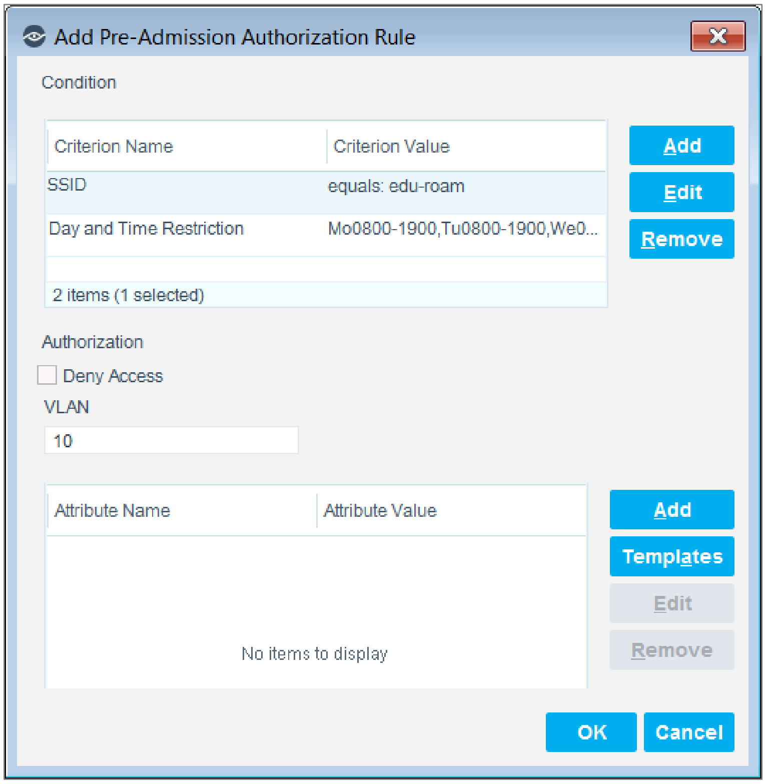
Matches Expression edu-roam



Add Pre-Admission Criterion

Day and Time Restriction

Selected period: Monday through Friday from 08:00 to 19:00



Add Pre-Admission Authorization Rule

Condition

Criterion Name	Criterion Value
SSID	equals: edu-roam
Day and Time Restriction	Mo0800-1900,Tu0800-1900,We0...

2 items (1 selected)

Authorization

☐ Deny Access

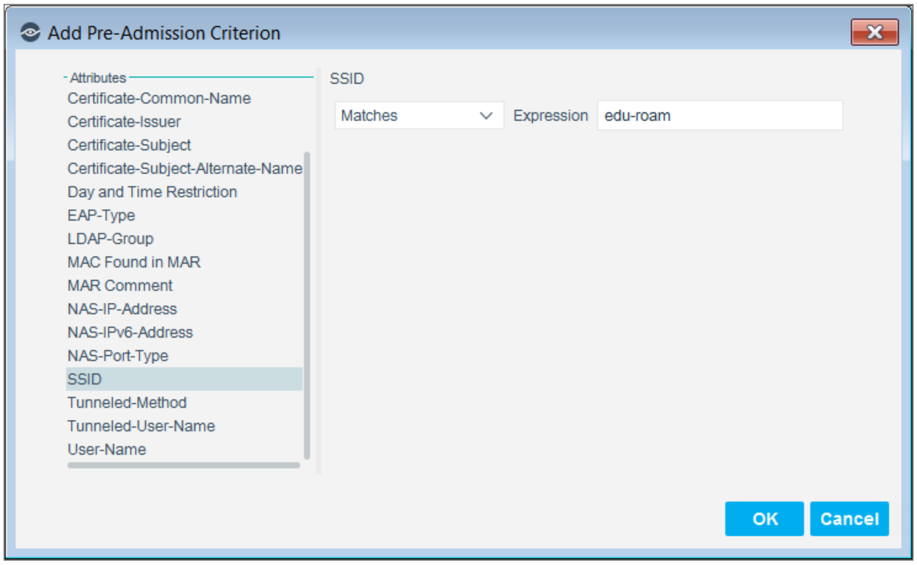
VLAN

10

Attribute Name	Attribute Value

No items to display

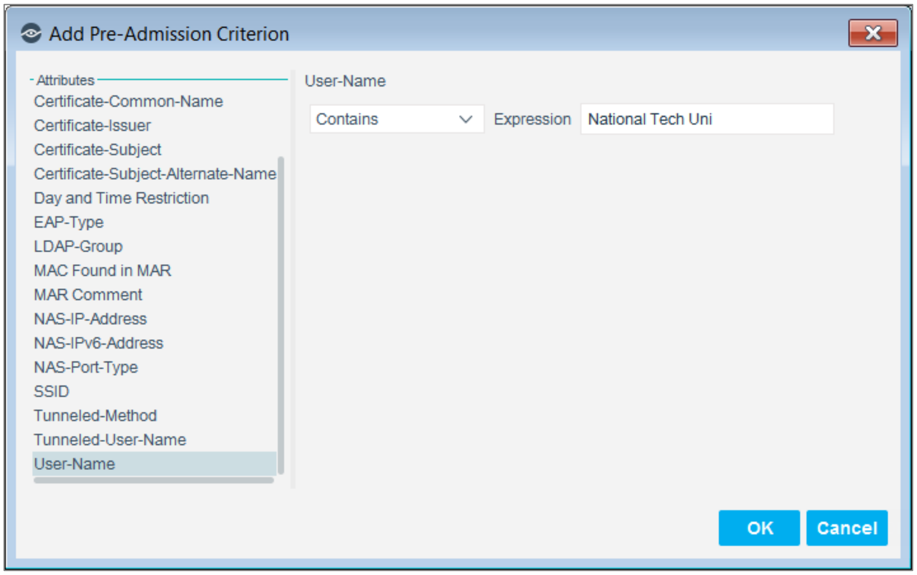
Local Endpoint Authorization



Add Pre-Admission Criterion

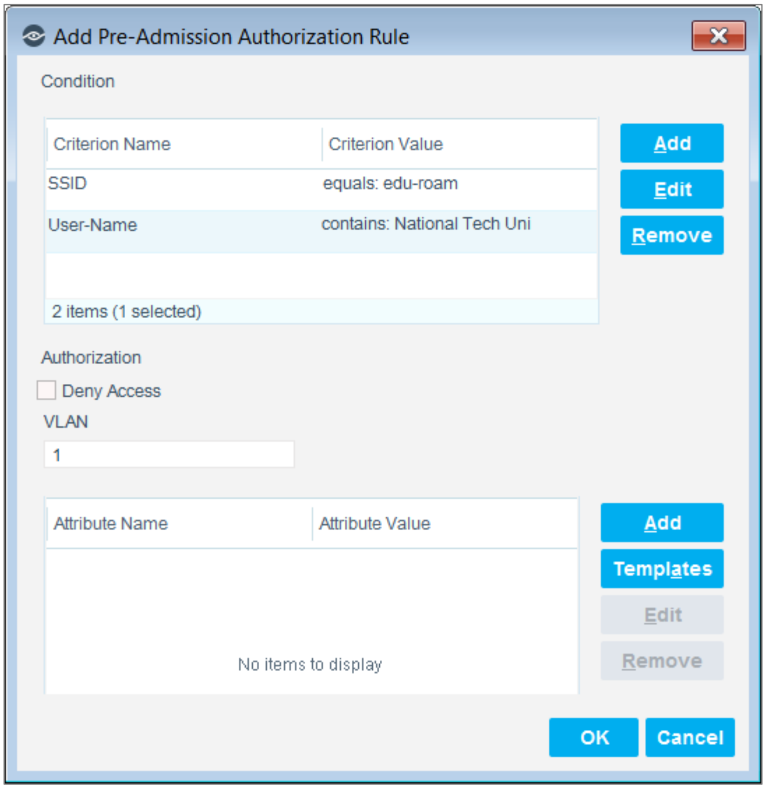
SSID

Matches Expression edu-roam



User-Name

Contains Expression National Tech Uni



Condition

Criterion Name	Criterion Value
SSID	equals: edu-roam
User-Name	contains: National Tech Uni

2 items (1 selected)

Authorization

☐ Deny Access

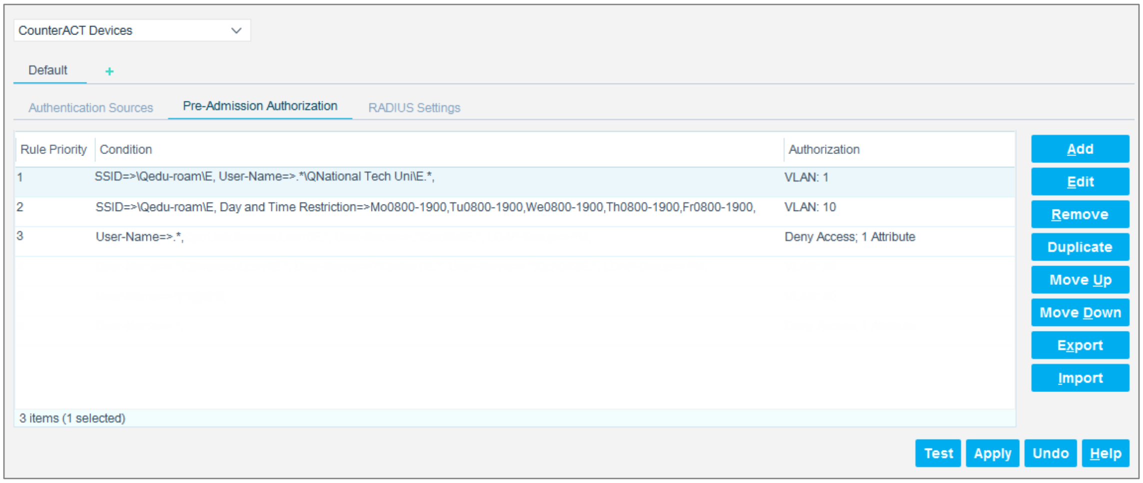
VLAN

1

Attribute Name	Attribute Value

No items to display

Pre-Admission Authorization Tab Rule Display



Rule Priority	Condition	Authorization
1	SSID=>\Qedu-roam\E, User-Name=>.*\QNational Tech Uni\E.*,	VLAN: 1
2	SSID=>\Qedu-roam\E, Day and Time Restriction=>Mo0800-1900,Tu0800-1900,We0800-1900,Th0800-1900,Fr0800-1900,	VLAN: 10
3	User-Name=>.*,	Deny Access; 1 Attribute

3 items (1 selected)

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.

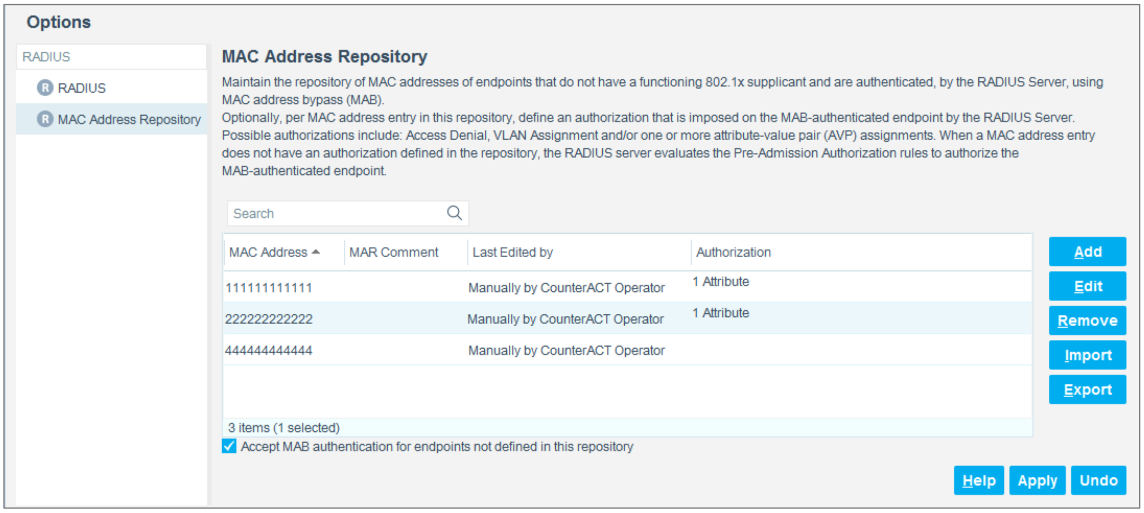
For details about defining authorization options, see the table provided in Rule Authorization.

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

- Local Mode
- Proxy Mode

Local Mode

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



MAC Address Repository

Maintain the repository of MAC addresses of endpoints that do not have a functioning 802.1x supplicant and are authenticated, by the 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 RADIUS Server. Possible authorizations include: Access Denial, 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 RADIUS server evaluates the Pre-Admission Authorization rules to authorize the MAB-authenticated endpoint.

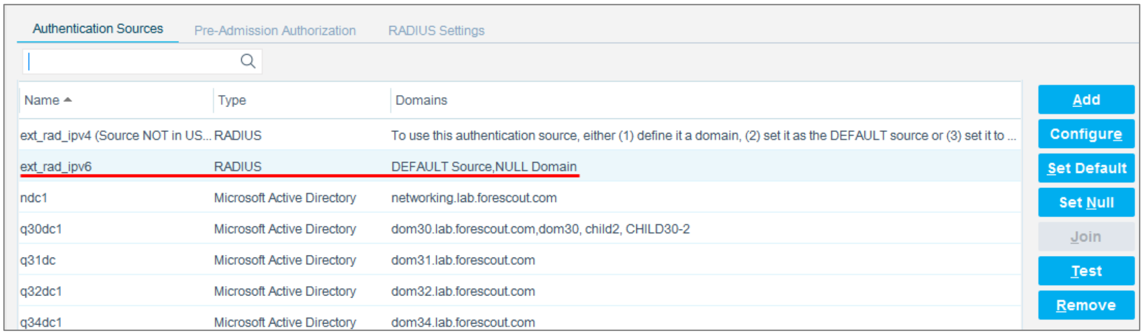
MAC Address ▲	MAR Comment	Last Edited by	Authorization
111111111111		Manually by CounterACT Operator	1 Attribute
222222222222		Manually by CounterACT Operator	1 Attribute
444444444444		Manually by CounterACT Operator	

3 items (1 selected)

☑ Accept MAB authentication for endpoints not defined in this repository

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.



Name ▲	Type	Domains
ext_rad_ipv4 (Source NOT in US...	RADIUS	To use this authentication source, either (1) define it a domain, (2) set it as the DEFAULT source or (3) set it to ...
ext_rad_ipv6	RADIUS	DEFAULT Source,NULL Domain
ndc1	Microsoft Active Directory	networking.lab.forescout.com
q30dc1	Microsoft Active Directory	dom30.lab.forescout.com,dom30, child2, CHILD30-2
q31dc	Microsoft Active Directory	dom31.lab.forescout.com
q32dc1	Microsoft Active Directory	dom32.lab.forescout.com
q34dc1	Microsoft Active Directory	dom34.lab.forescout.com

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

Network Device Administration

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

To accomplish, perform the following:

- In the organization's network device, configure:
  - The IP address of the CounterACT device as the RADIUS server
  - The pre-shared key of the CounterACT RADIUS server
- In the User Directory Plugin, configure the Active Directory server that will be queried about user group membership (LDAP-Group)
- In the RADIUS Plugin:
  - In the RADIUS Settings tab, select the **Enable PAP-Authentication** option.

    🗎 *PAP authentication is not secure and, therefore, must be explicitly selected for use.*

  - In the Authentication Sources tab, add the Active Directory server as an authentication source and configure test credentials and join credentials. Join the applicable AD domain and run the plugin test.
  - In the Pre-Admission Authorization tab, add the following pre-admission rule:

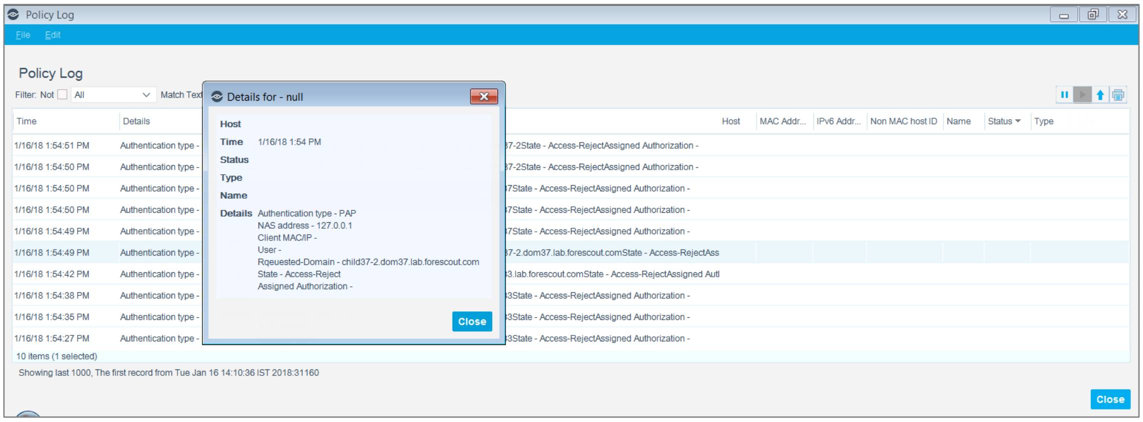
    > Rule Condition that evaluates the **`Authentication-Type`** attribute for a match on the value **`PAP`**.

    > Rule Authorization that uses the attribute template *Cisco-Network Device Administration*. This template contains the **`Service-Type`** attribute with the value **`NAS-Prompt-User`** and the **`Cisco-AV Pair`** attribute with the value **`shell:priv-lv=#`**. Replace the pound sign (#) with a valid privilege level value that allows user execution of shell commands on the network device, which are authorized for that privilege level.

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

To generate a policy log and view PAP Authentication activities:

1. In the Console toolbar, select **Log** > **Policy Log**. The Policy Log dialog opens.
2. In the dialog, define a time scope, a host scope and the number of records you want the log to display.
3. Select **OK**. The Policy Log window opens displaying the generated results.
4. Using the **Filter** options/fields, located above the display, re-generate filtered log results that display PAP authentication activities.
5. Double-click a log entry to open a **Details for** <*host*> window.



Policy Log

Filter: Not □ All Match Text

Time	Details	Host	MAC Addr...	IPv6 Addr...	Non MAC host ID	Name	Status	Type
1/16/18 1:54:51 PM	Authentication type - 37-2State - Access-RejectAssigned Authorization -							
1/16/18 1:54:50 PM	Authentication type - 37-2State - Access-RejectAssigned Authorization -							
1/16/18 1:54:50 PM	Authentication type - 37State - Access-RejectAssigned Authorization -							
1/16/18 1:54:50 PM	Authentication type - 37State - Access-RejectAssigned Authorization -							
1/16/18 1:54:49 PM	Authentication type - 37State - Access-RejectAssigned Authorization -							
1/16/18 1:54:49 PM	Authentication type - 37-2.dom37.lab.forescout.comState - Access-RejectAss							
1/16/18 1:54:42 PM	Authentication type - 3.lab.forescout.comState - Access-RejectAssigned Autl							
1/16/18 1:54:38 PM	Authentication type - 3State - Access-RejectAssigned Authorization -							
1/16/18 1:54:35 PM	Authentication type - 3State - Access-RejectAssigned Authorization -							
1/16/18 1:54:27 PM	Authentication type - 3State - Access-RejectAssigned Authorization -							

10 items (1 selected)

Showing last 1000, The first record from Tue Jan 16 14:10:36 IST 2018:31160

Details for - null

Host

Time 1/16/18 1:54 PM

Status

Type

Name

Details Authentication type - PAP
NAS address - 127.0.0.1
Client MAC/IP -
User -
Rqeuested-Domain - child37-2.dom37.lab.forescout.com
State - Access-Reject
Assigned Authorization -

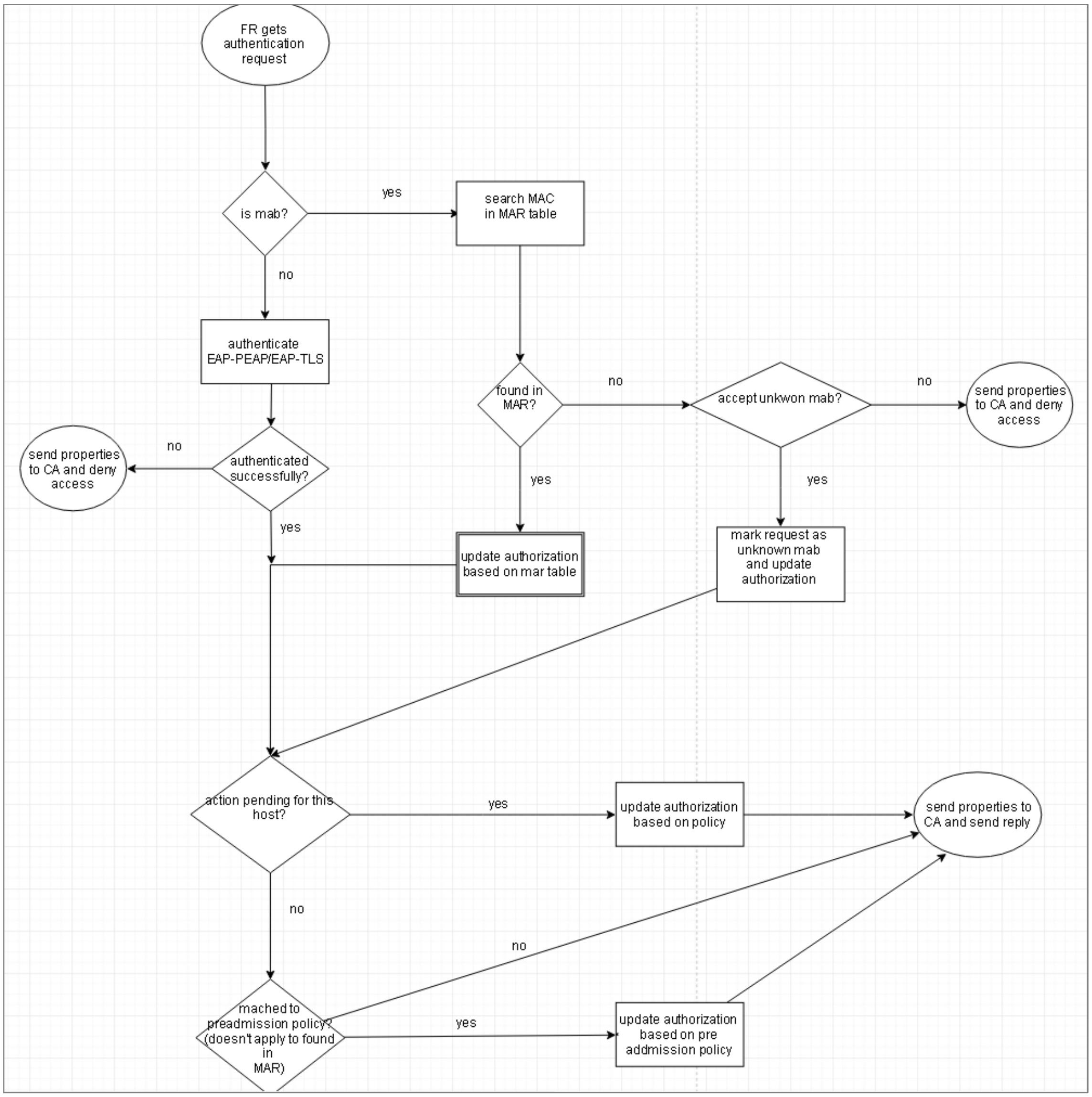
Advanced Topics

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:


FR gets authentication request
is mab?
yes
search MAC in MAR table
no
authenticate EAP-PEAP/EAP-TLS
found in MAR?
no
accept unkwon mab?
no
send properties to CA and deny access
send properties to CA and deny access
no
authenticated successfully?
yes
yes
yes
update authorization based on mar table
mark request as unknown mab and update authorization
action pending for this host?
yes
update authorization based on policy
send properties to CA and send reply
no
no
mached to preadmission policy? (doesn't apply to found in MAR)
yes
update authorization based on pre addmission policy

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

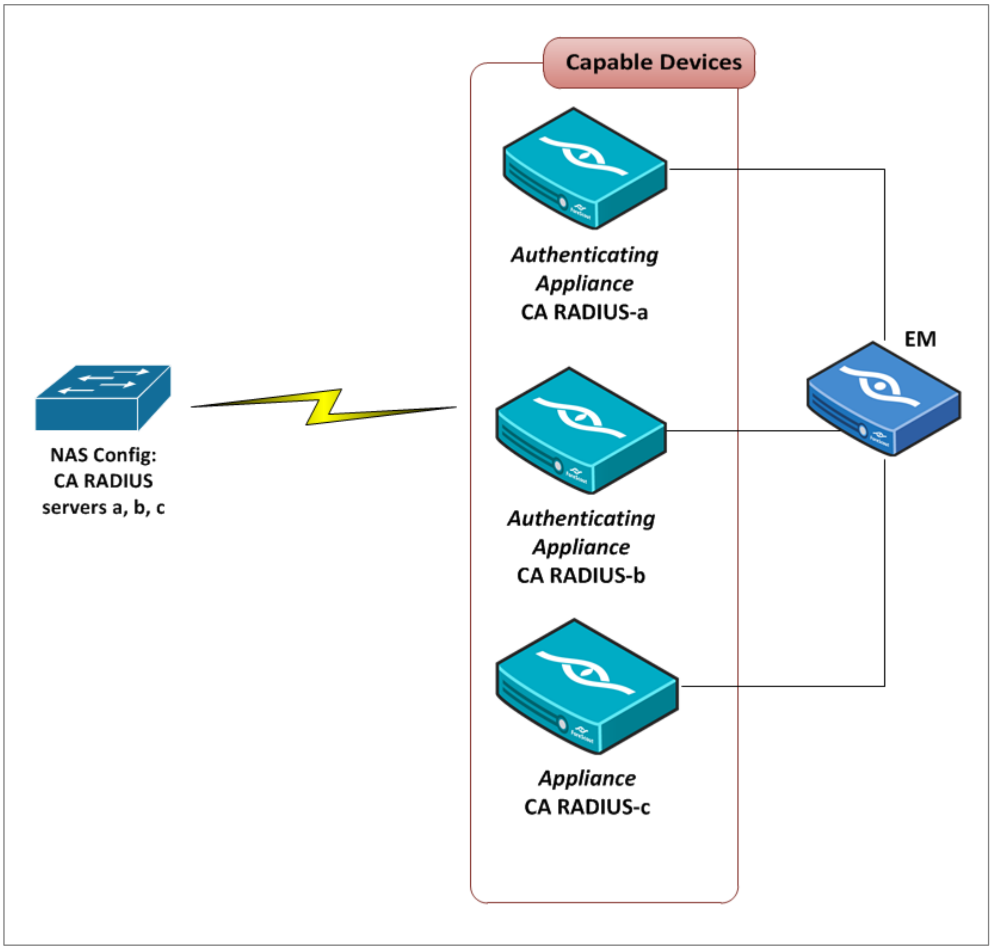
The RADIUS Plugin employs any of the following re-authentication methods:

Method	Protocol	NAS Type	Vendor	Packet Content	Priority
COA	RADIUS-CoA	General	Cisco	Port=1700, with Cisco VSA=**"subscriber:command=reauthenticate"**	1
POD General	RADIUS-POD	General	General	Port = 3799 with Accounting SID	2
POD Cisco	RADIUS-POD	General	Cisco	Port = 3799 with Accounting SID, **"Service-Type=Login"**	3
Port Authenticate	SNMP	Switch	General	MIB = **"1.0.8802.1.1.1.1.1.2.1.5"** + port index	4
Aironet *De-authentication*	SNMP	WLAN Device	Cisco/Aironet	MIB = **"1.3.6.1.4.1.14179.2.1.4.1.22"**	5
Xirrus De-authentication	SNMP	WLAN Device	Xirrus	MIB = **"1.3.6.1.4.1.21013.1.2.22.3.0"**	6
Port Bounce	SNMP	Switch	General	MIB = **"1.3.6.1.2.1.2.2.1.7"** + port index	7

🗎 *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 RADIUS Plugin. The following diagram presents a standard 802.1X deployment:


Capable Devices
Authenticating Appliance CA RADIUS-a
Authenticating Appliance CA RADIUS-b
Appliance CA RADIUS-c
EM
NAS Config: CA RADIUS servers a, b, c

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 RADIUS Plugin compiles an internal list of all *capable* CounterACT RADIUS servers.
2. Starting with the authenticating Appliance, the managing Appliance evaluates each capable device to identify the Appliance/CounterACT RADIUS server that 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, do the following to point to the proper IP address:
  a. Log in to the CounterACT device CLI.
  b. Run the following command:
     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:

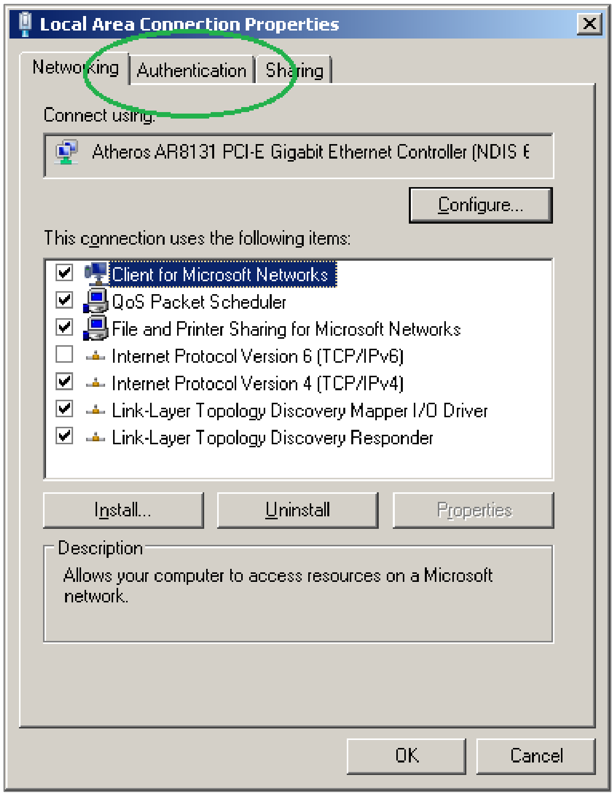
- Supplicant on Windows 7/Windows XP Endpoints
- Supplicant on MAC Endpoints

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.



Connect using:

Atheros AR8131 PCI-E Gigabit Ethernet Controller (NDIS 6

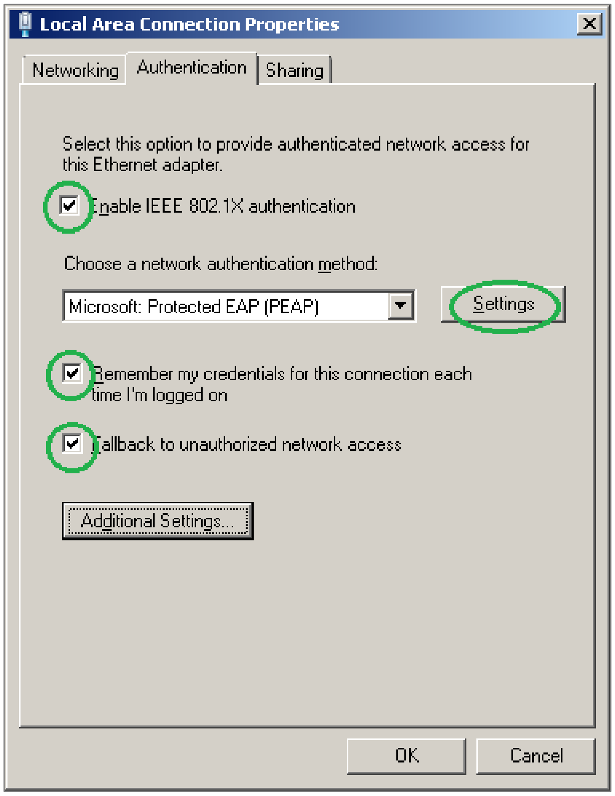
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☐ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Allows your computer to access resources on a Microsoft network.

4. Select the **Authentication** tab.



Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

5. In the tab, configure the following:

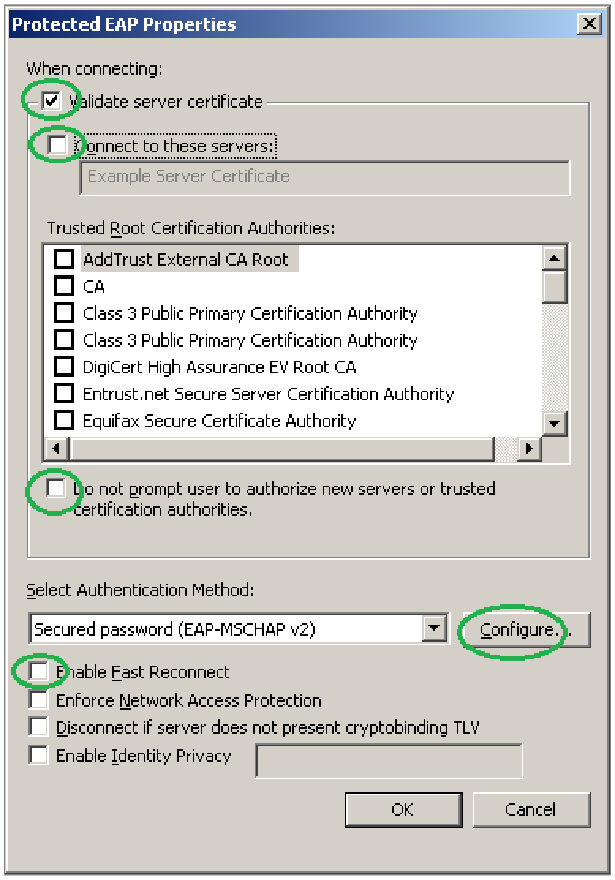
   a. Select the **Enable IEEE 802.1X authentication** option to start the supplicant or clear this option to stop the supplicant.

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

   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

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Example Server Certificate

Trusted Root Certification Authorities:

□ AddTrust External CA Root
□ CA
□ Class 3 Public Primary Certification Authority
□ Class 3 Public Primary Certification Authority
□ DigiCert High Assurance EV Root CA
□ Entrust.net Secure Server Certification Authority
□ Equifax Secure Certificate Authority

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

□ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

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.

Authentication Module Information

The RADIUS Plugin is installed with the CounterACT Authentication Module.

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

The Authentication Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

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

Refer to the *CounterACT Authentication Module Guide* for more module information, such as module requirements, upgrade and rollback instructions. See *Additional CounterACT Documentation* for information about how to access the module guide.

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

🗎 *Software downloads are also available from these portals.*

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

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

To access the Product Updates Portal:

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

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

🗎 *If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.*

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT 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.

CounterACT Administration Guide

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 **Modules**.
2. Select the plugin and then select **Help**.

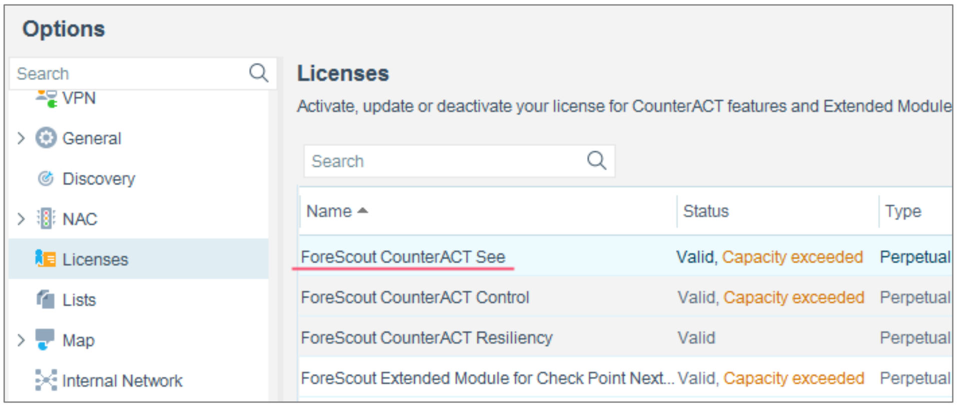
Documentation Portal

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

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Licenses

Activate, update or deactivate your license for CounterACT features and Extended Module

Name ▲	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21