

Cisco ISE and Juniper EX Switches for 802.1X-Based Authentication

Published
2021-02-03

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Cisco ISE and Juniper EX Switches for 802.1X-Based Authentication
Copyright © 2021 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | iv

Documentation and Release Notes | iv

Documentation Conventions | iv

Documentation Feedback | vii

Requesting Technical Support | vii

Self-Help Online Tools and Resources | viii

Creating a Service Request with JTAC | viii

1

How to Configure Cisco ISE and Juniper EX Switches for 802.1X-Based Authentication

Configure Cisco ISE and Juniper EX Switches for 802.1X-Based Authentication | 10

About This Network Configuration Example | 10

Overview | 10

Topology | 11

Step-by-Step Procedure | 12

Import the Juniper Wired Device Profile | 12

Add EX Switches to the Juniper Device Profile | 13

Create Authorization Profiles | 14

Create Endpoint Identity Groups | 18

Add Endpoints | 19

Create User Identity Groups | 20

Add Users | 21

Set Authentication Policies | 25

Set Authorization Policies | 27

Configure a Cisco ISE Policy to Enable Guest Access | 29

Configure a Colorless Port Using IETF Egress-VLAN-ID Attributes | 34

Configure the 802.1X Protocol on the EX Switch | 41

Configure Windows 10 | 42

Testing and Validation | 47

Verify IP Phone Authentication Status | 48

Verify Connections to Windows 10 Clients | 50

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | iv
- Documentation Conventions | iv
- Documentation Feedback | vii
- Requesting Technical Support | vii

This Network Configuration Example (NCE) shows you how to configure Cisco Identity Services Engine 2.X (Cisco ISE) and Juniper EX switches for IEEE 802.1X-based authentication. Cisco ISE allows you to import network device profiles in XML format, enabling integration with any IEEE 802.1X standard network device. This example shows you how to import the Juniper network device profile.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks[®] technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

Table 1 on page v defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page v defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

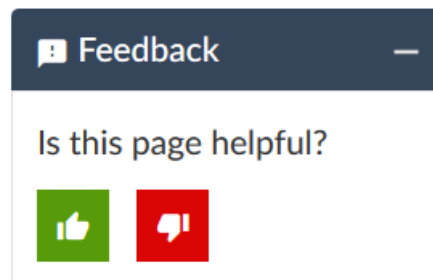
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

1

CHAPTER

How to Configure Cisco ISE and Juniper EX Switches for 802.1X-Based Authentication

Configure Cisco ISE and Juniper EX Switches for 802.1X-Based Authentication | 10

Configure Cisco ISE and Juniper EX Switches for 802.1X-Based Authentication

IN THIS SECTION

- [About This Network Configuration Example | 10](#)
- [Overview | 10](#)
- [Topology | 11](#)
- [Step-by-Step Procedure | 12](#)
- [Testing and Validation | 47](#)

About This Network Configuration Example

This network configuration example (NCE) shows you how to configure Cisco Identity Services Engine 2.X (Cisco ISE) and Juniper EX switches for IEEE 802.1X-based authentication.

NOTE: Juniper's content testing team has validated and updated this example.

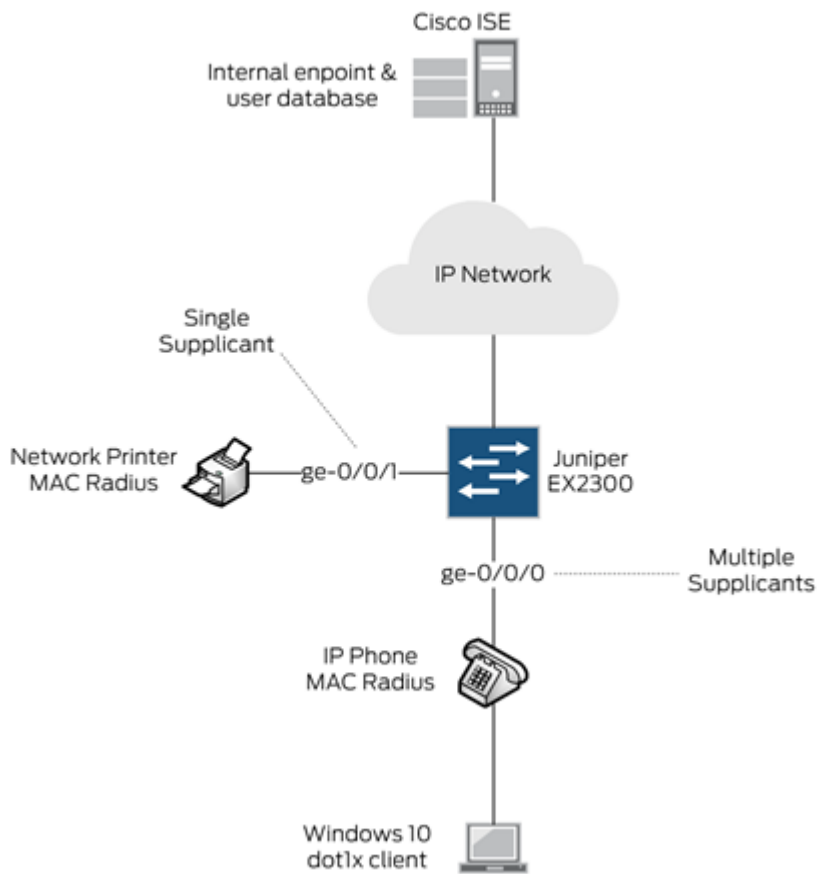
Overview

Cisco ISE 2.X comes with many pre-imported network device profiles, but it doesn't come with one for Juniper. Network device profiles specify how to handle MAC Radius, dot1x authentication, VLAN and ACL assignment, and CoA features.

Cisco ISE allows you to import network device profiles in XML format, enabling integration with any IEEE 802.1X standard network device. This example shows you how to import the Juniper network device profile, and configure settings to allow IEEE 802.1X-based authentication with Cisco ISE and Juniper EX switches.

Topology

In this example, we use the following network topology:



Here's more details about the hardware and software components used in this example:

Device	Software Version	Role
Juniper EX2300-C-12P	Junos 18.2R1-S1	Switch and Authenticator
Cisco ISE	2.4.0.357 Patch2-18080100	RADIUS Server
Polycom VVX 310 IP Phone	SIP/5.5.1.11526/22-Nov-16 15:05	Supplicant (MAC Radius)
Windows 10 Professional	All recommended patches as of 2018-08-22	Supplicant (Dot1x)
Network Printer	N/A	Supplicant (MAC Radius)
Juniper Mist AP43	0.6.18981	Supplicant (MAC Radius)

All users and endpoints are stored in the internal Cisco ISE database.

For external user database integration such as Microsoft Active Directory, LDAP and Certificate Based Authentication, refer to the [Cisco Identity Services Engine Administrator Guide, Release 2.4](#).

Step-by-Step Procedure

1. [Import the Juniper Wired Device Profile | 12](#)
2. [Add EX Switches to the Juniper Device Profile | 13](#)
3. [Create Authorization Profiles | 14](#)
4. [Create Endpoint Identity Groups | 18](#)
5. [Add Endpoints | 19](#)
6. [Create User Identity Groups | 20](#)
7. [Add Users | 21](#)
8. [Set Authentication Policies | 25](#)
9. [Set Authorization Policies | 27](#)
10. [Configure a Cisco ISE Policy to Enable Guest Access | 29](#)
11. [Configure a Colorless Port Using IETF Egress-VLAN-ID Attributes | 34](#)
12. [Configure the 802.1X Protocol on the EX Switch | 41](#)
13. [Configure Windows 10 | 42](#)

Import the Juniper Wired Device Profile

Assuming you've got Cisco ISE up and running on your network, the first thing you'll need to do is add a Juniper EX switch device profile.

1. Download the latest [Juniper EX Switch Device Profile for Cisco ISE](#) (validated with Cisco ISE 2.7).
2. In Cisco ISE, choose **Administration > Network Resources > Network Device Profiles**.
3. Click **Import** and select the Juniper EX switch device profile you downloaded in step 1. Once you import the Juniper network device profile, it will be listed in the Cisco ISE Network Device Profiles list as Juniper_Wired.

Network Device Profiles

[Edit](#)
[Add](#)
[Duplicate](#)
[Import](#)
[Cisco Communities Import](#)
[Export Selected](#)
[Delete Selected](#)

Name	Description	Vendor	Source
AlcatelWired	Profile for Alcatel switches	Alcatel	Cisco Provided
ArubaWireless	Profile for Aruba wireless network access devices	Aruba	Cisco Provided
BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
Cisco	Generic profile for Cisco network access devices	Cisco	Cisco Provided
HPWired	Profile for HP switches	HP	Cisco Provided
HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP	Cisco Provided
HPWireless	Profile for HP wireless network access devices	HP	Cisco Provided
Juniper_Wired	NAD Profile for Juniper switches (EX series)	Juniper	User Defined
MotorolaWireless	Profile for Motorola wireless network access devices	Motorola	Cisco Provided
RuckusWireless	Profile for Ruckus wireless network access devices	Ruckus	Cisco Provided

Add EX Switches to the Juniper Device Profile

You can add your EX switches individually, or as an IP address range.

1. In Cisco CSE, choose **Administration > Network Resources > Network Devices**.
2. In the Network Device screen, select the Juniper_Wired device profile.
3. Give a name and IP address for your EX switch. If you are adding multiple EX switches, you can specify an IP address range.

[Network Devices List](#) > [New Network Device](#)

Network Devices

* Name

Description

* IP : /

❗ IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

4. Specify a RADIUS password. You'll need this later when configuring the EX switches.

✓ **▼ RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

RADIUS DTLS Settings ⓘ

DTLS Required ☐ ⓘ

Shared Secret ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA ⓘ

DNS Name

General Settings

Enable KeyWrap ☐ ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ☒ ASCII ☐ HEXADECIMAL

Create Authorization Profiles

Authorization profiles allow you to apply different attributes to users or endpoints. You can change the VLAN by name or by VLAN ID. You can also assign a firewall filter that you have already configured on the switch. In this example, we create four authorization profiles:

- Juniper_VoIP_VLAN_500
- Juniper_VoIP_VLAN_100
- Juniper_VoIP_VLAN_100_ACL
- Juniper_VoIP_VLAN_100_dACL

The first profile sets the VoIP VLAN to 500 using the Juniper-VoIP-VLAN attribute.

1. In Cisco ISE, choose **Policy > Results**, then from the left pane, choose **Authorization > Authorization Profiles**.
2. Name the profile **Juniper_VoIP_VLAN_500**.
3. Set the VLAN ID/Name to **500**.
4. Click **Add**.

Authorization Profiles > **Juniper_VoIP_VLAN_500**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Common Tasks

Advanced Attributes Settings

Juniper:Juniper-VoIP-Vlan =

Attributes Details

Access Type = ACCESS_ACCEPT
Juniper-VoIP-Vlan = 500

The second authorization profile sets the Data VLAN to 100 using the standard RADIUS attribute for VLAN ID.

1. In Cisco ISE, choose **Policy > Results**, then from the left pane, choose **Authorization > Authorization Profiles**.
2. Name the profile **Juniper_VoIP_VLAN_100**.
3. Set the VLAN ID/Name to **100**.
4. Click **Add**.



Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile  

▼ Common Tasks

☒ VLAN Tag ID **1** ID/Name

☐ Web Redirection (CWA, MDM, NSP, CPP) 

► Advanced Attributes Settings

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:100
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

The third profile sets the Data VLAN to 100 and applies a local firewall filter/ACL to the supplicant. This firewall filter/ACL must already be configured on the switch. The firewall filter/ACL is applied using the standard Filter-ID radius attribute. Enter the name of the local filter configured on the switch.

1. In Cisco ISE, choose **Policy > Results**, then from the left pane, choose **Authorization > Authorization Profiles**.
2. Name the profile **Juniper_VoIP_VLAN_100_ACL**.
3. Under Common Tasks, set ACL (Filter-ID) to **deny-all**.
4. Set the VLAN ID/Name to **100**.
5. Click **Add**.

Authorization Profiles > [Juniper_Data_VLAN_100_ACL](#)

Authorization Profile

* Name

Description

* Access Type

Network Device Profile 

▼ Common Tasks

☒ ACL (Filter-ID)

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:100
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6

The fourth authorization profile sets the Data VLAN to 100 and applies a dynamic/downloadable firewall filter/ACL to the supplicant. This firewall filter/ACL is created dynamically, so you don't need to configure it locally on the switch. This authorization profile uses the Juniper-Switching-Filter attribute.

NOTE: The syntax and feature sets differ from regular Junos firewall filters/ACLs. Multiple entries are separated by commas. See [Juniper-Switching-Filter VSA Match Conditions and Actions](#) for information about the syntax.


Authorization Profiles > **Juniper_Data_VLAN_100_dACL**

Authorization Profile

* Name

Description

* Access Type




Network Device Profile 

Common Tasks

☒ VLAN Tag ID **1** ID/Name

☐ Web Redirection (CWA, MDM, NSP, CPP) 

Advanced Attributes Settings

Juniper:Juniper-Switching-Filter  = match destination-ip 1.1.1.1/32...  - 

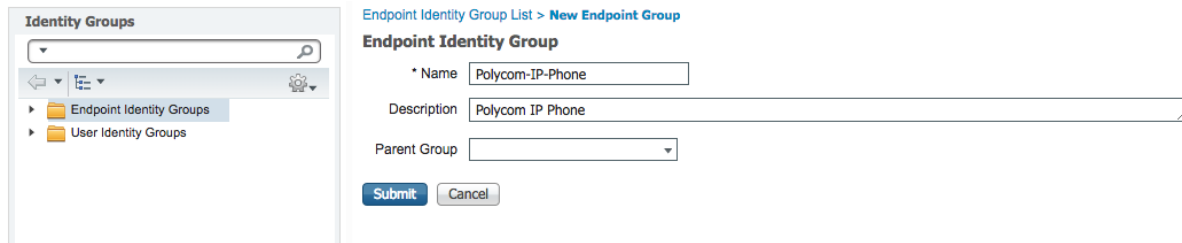
Attributes Details

Access Type = ACCESS_ACCEPT
 Tunnel-Private-Group-ID = 1:100
 Tunnel-Type = 1:13
 Tunnel-Medium-Type = 1:6
 Juniper-Switching-Filter = match destination-ip 1.1.1.1/32 action deny, match destination-ip 2.2.2.2/32 action deny, match destination-ip 0.0.0.0/0 action allow

Create Endpoint Identity Groups

Endpoints, such as IP Phones, can be grouped together in endpoint identity groups to make it easier to apply common attributes, for example, VoIP VLAN.

1. In Cisco ISE, choose **Administration > Groups > Endpoint Identity Groups**.
2. Click **Add**.
3. Enter a Name and Description under **Endpoint Identity Group**.
4. Click **Submit**.



The screenshot shows the Cisco ISE web interface for creating a new endpoint identity group. On the left, a sidebar titled 'Identity Groups' shows a tree view with 'Endpoint Identity Groups' and 'User Identity Groups'. The main area is titled 'Endpoint Identity Group List > New Endpoint Group'. Below this, the 'Endpoint Identity Group' form is displayed with the following fields: 'Name' (text input with 'Polycom-IP-Phone'), 'Description' (text area with 'Polycom IP Phone'), and 'Parent Group' (dropdown menu). At the bottom of the form are 'Submit' and 'Cancel' buttons.

Add Endpoints

The Polycom IP Phone in this setup is not configured for dot1x authentication. Instead, we rely on MAC RADIUS and MAC Authentication Bypass (MAB).

1. In Cisco ISE, choose **Context Visibility > Endpoints**.
2. Click **+**.
3. Add the IP Phone's MAC address and assign it a policy group.
4. Click **Save**.

Add Endpoint



General Attributes

Mac Address *	<input type="text" value="00:04:F2:8B:69:D1"/>
Description	<input type="text" value="Polycom IP Phone"/>
Static Assignment	<input checked="" type="checkbox"/>
Policy Assignment	<input type="text" value="Polycom-Device"/>
Static Group Assignment	<input checked="" type="checkbox"/>
Identity Group Assignment	<input type="text" value="Polycom-IP-Phone"/>

Cancel

Save

Create User Identity Groups

User Identity Groups allow you to apply specific attributes to users that are members of the group. In this example, we create three new User Identity Groups:

- VLAN_100_User_ID_Group
- VLAN_100_ACL_User_ID_Group
- VLAN_100_dACL_User_ID_Group

1. In Cisco ISE, choose **Administration > Groups > User Identity Groups**.
2. Click **Add**.
3. Enter a name for the User Identity Group and click **Submit**.

User Identity Groups > New User Identity Group

Identity Group

* Name

Description

The image displays two screenshots of the Cisco ISE 'New User Identity Group' configuration page. Both screenshots show a left-hand navigation pane with 'User Identity Groups' selected. The top screenshot shows the 'Name' field as 'VLAN_100_ACL_User_ID_Group' and the 'Description' as 'VLAN 100 with ACL User ID Group'. The bottom screenshot shows the 'Name' field as 'VLAN_100_dACL_User_ID_Group' and the 'Description' as 'VLAN 100 with dACL User ID Group'. Both screenshots show 'Submit' and 'Cancel' buttons at the bottom.

Add Users

In this example, we create three local users named user1, user2 and user3. Each user is assigned to a different User Identity Group.

1. In Cisco ISE, choose **Administration > Identity Management**.
2. Click **Add**.
3. Enter a name and login password.
4. From the User Groups drop-down list, choose the User Identity Group that you want to assign to the new user.

In this example, we assign the new users to these User Identity Groups:

- user1 to VLAN_100_User_ID_Group
- user2 to VLAN_100_ACL_User_ID_Group
- user3 to VLAN_100_dACL_User_ID_Group

Network Access Users List > [New Network Access User](#)

▼ **Network Access User**

* Name

Status ☒ Enabled ▼

Email

▼ **Passwords**

Password Type: ▼

	Password	Re-Enter Password	
* Login Password	<input type="password" value="....."/>	<input type="password" value="....."/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ

▼ **User Information**

First Name

Last Name

▶ **Account Options**

▶ **Account Disable Policy**

▼ **User Groups**

VLAN_100_User_ID_Group

▼

—

▼ **Network Access User**

* Name

Status ☒ Enabled ▼

Email

▼ **Passwords**

Password Type: ▼

	Password	Re-Enter Password	
* Login Password	<input type="password" value="....."/>	<input type="password" value="....."/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ

▼ **User Information**

First Name

Last Name

▶ **Account Options**

▶ **Account Disable Policy**

▼ **User Groups**

.....

VLAN_100_ACL_User_ID_Group ▼

—

[Network Access Users List](#) > [New Network Access User](#)

▼ Network Access User

* Name

Status ☒ Enabled ▼

Email

▼ Passwords

Password Type:

Password
 Re-Enter Password
 ⓘ

* Login Password
 ⓘ

Enable Password
 ⓘ

▼ User Information

First Name

Last Name

▶ Account Options

▶ Account Disable Policy

▼ User Groups

Here's an overview of the three users we just created:

Network Access Users

Edit Add Change Status Import Export Delete Duplicate							
Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled	user1		User	One		VLAN_100_User_ID_Group	
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled	user2		User	Two		VLAN_100_ACL_User_ID_Group	
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled	user3		User	Three		VLAN_100_dACL_User_ID_Group	

Set Authentication Policies

The authentication policy contains three entries per default.

The predefined MAB and dot1x rules have conditions that are tied to the network device profile. When requests come from a Juniper device, the switch automatically uses the attributes configured in the Juniper network device profile to authenticate a MAB and dot1x request. The authentication policy named Default contains a default network access policy for allowed protocols. This network access policy is compatible with Juniper EX switches.

In this example, we use the Default authentication policy.

- 1. Choose **Policy > Policy Sets**.
- 2. Click > to the far right of the Default policy set and choose **Default Network Access** from the drop-down box.

Policy Sets → Default

Status	Policy Set Name	Description	Conditions
	Default	Default policy set	

▼ Authentication Policy (3)

	Status	Rule Name	Conditions
	MAB	OR	<div>Wired_MAB</div> <div>Wireless_MAB</div>
	Dot1X	OR	<div>Wired_802.1X</div> <div>Wireless_802.1X</div>
	Default		

Reset Save

Allowed Protocols / Server Sequence	Hits
Default Network Access x +	489

Use	Hits	Actions
Internal Endpoints x Options	138	
All_User_ID_Stores x Options	28	
All_User_ID_Stores x Options	0	

Cisco ISE Default Network Access Profile

Here's the Cisco ISE configuration for the Default Network Access profile for Juniper EX switches.

[Allowed Protocols Services List](#) > [Default Network Access](#)

Allowed Protocols

Name	Default Network Access
Description	Default Allowed Protocol Service

▼ Allowed Protocols

Authentication Bypass

☒ Process Host Lookup ⓘ

Authentication Protocols

☒ Allow PAP/ASCII

☐ Allow CHAP

☐ Allow MS-CHAPv1

☐ Allow MS-CHAPv2

☒ Allow EAP-MD5

▼ ☒ Allow EAP-TLS

☐ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ⓘ

☐ Enable Stateless Session Resume

Session ticket time to live

Proactive session ticket update will occur after % of Time To Live has expired

☐ Allow LEAP

▼ ☒ Allow PEAP

PEAP Inner Methods

☒ Allow EAP-MS-CHAPv2

☒ Allow Password Change Retries (Valid Range 0 to 3)

☒ Allow EAP-GTC

☒ Allow Password Change Retries (Valid Range 0 to 3)

☒ Allow EAP-TLS

☐ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ⓘ

☐ Require cryptobinding TLV ⓘ

☐ Allow PEAPv0 only for legacy clients

Set Authorization Policies

The order of the authorization policies is important and may vary depending on your setup. Make sure that you don't have more general rules above the rules you are about to create, otherwise they won't match.

In this example, we create four new rules, each with three conditions:

- VLAN 500 for Polycom IP Phones connected to Juniper EX Switches
- VLAN 100 for dot1x users connected to Juniper EX Switches
- VLAN 100 with ACL for dot1x users connected to Juniper EX Switches
- VLAN 100 with dACL for dot1x users connected to Juniper EX Switches

1. Expand **Authorization Policy** and click the + button in the top left corner of the screen.
2. Enter a name for the rule, for example, **VLAN 500 for Polycom IP Phones connected to Juniper EX Switches**.
3. Click **condition** to open the Condition Studio.
4. Drag and drop from the library on the left side to the editor on the right side. Build the different attributes you want to match on.
5. When you're finished don't click **Save**. Instead, click the **USE** button in the bottom right corner.

Here's an example of the Conditions Studio:

Conditions Studio



Library

Search by Name

- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed
- Non_Cisco_Profiling_Phones
- Non_Compliant_Devices
- Switch_Local_Web_Authentication
- Switch_Web_Authentication
- Wired_802.1X
- Wired_MAB
- Wireless_802.1X
- Wireless_Access
- Wireless_MAB
- WLC_Web_Authentication

Editor

Network_Access_Authentication_Passed

DEVICE: Device Type

Equals All Device Types#Juniper EX Switches

AND

IdentityGroup: Name

Equals Endpoint Identity Groups:Polycom-IP-Phone

+ New AND OR

Set to 'Is not' Duplicate Save

Close

Use

Let's analyze these four new rules. Each rule has three conditions. The first two conditions are the same, but the third condition matches on a different attribute. A rule is applied to a port only when all three conditions are met.

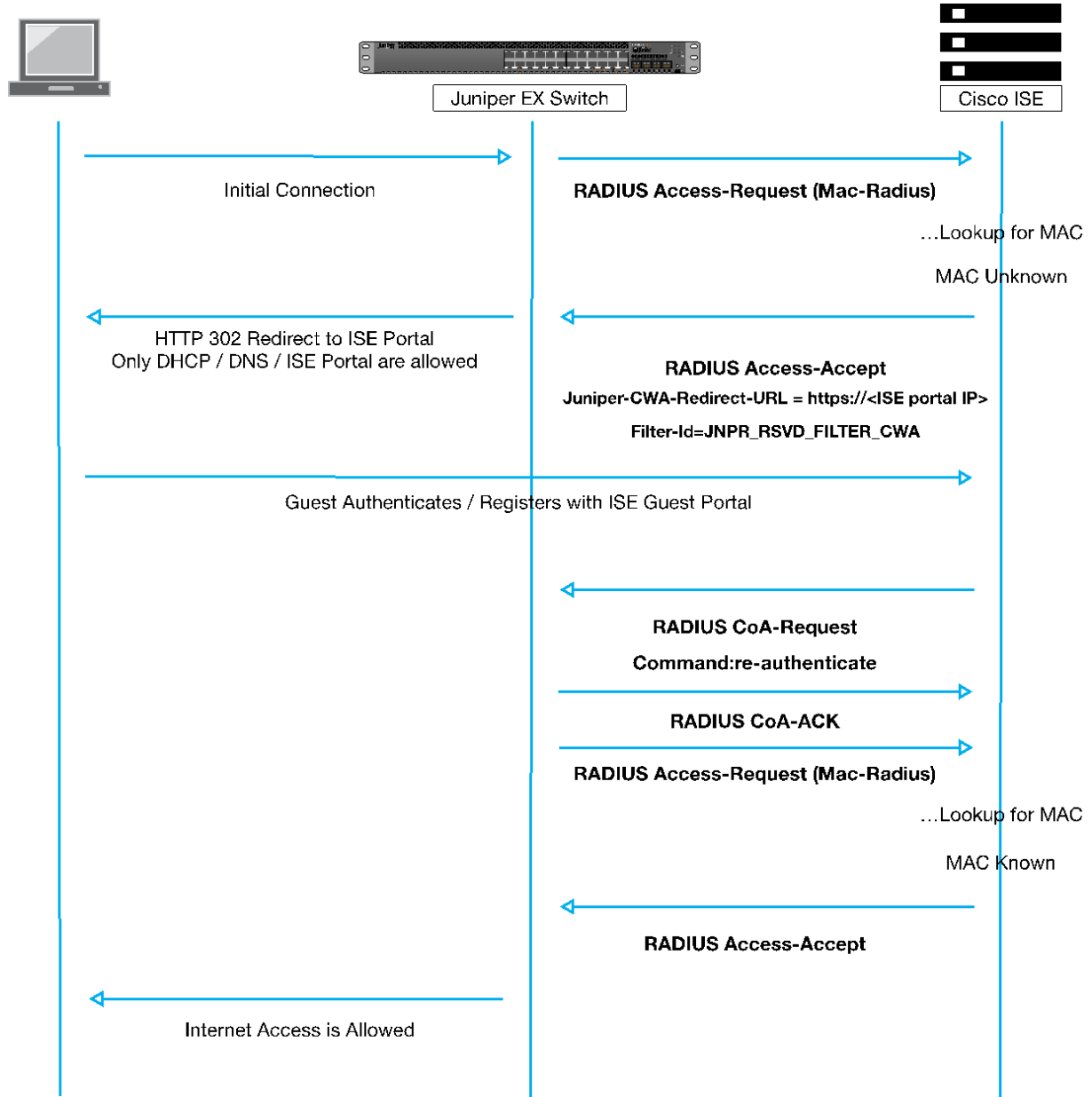
✓	VLAN 500 for Polycom IP Phones connected to Juniper EX Switches	AND	Network_Access_Authentication_Passed DEVICE Device Type EQUALS All Device Types#Juniper EX Switches IdentityGroup Name EQUALS Endpoint Identity Groups#Polycom-IP-Phone
✓	VLAN 100 for dot1x users connected to Juniper EX Switches	AND	Network_Access_Authentication_Passed DEVICE Device Type EQUALS All Device Types#Juniper EX Switches IdentityGroup Name EQUALS User Identity Groups#VLAN_100_User_ID_Group
✓	VLAN 100 with ACL for dot1x users connected to Juniper EX Switches	AND	Network_Access_Authentication_Passed DEVICE Device Type EQUALS All Device Types#Juniper EX Switches IdentityGroup Name EQUALS User Identity Groups#VLAN_100_ACL_User_ID_Group
✓	VLAN 100 with dACL for dot1x users connected to Juniper EX Switches	AND	Network_Access_Authentication_Passed DEVICE Device Type EQUALS All Device Types#Juniper EX Switches IdentityGroup Name EQUALS User Identity Groups#VLAN_100_dACL_User_ID_Group

Juniper_VoIP_VLAN_500	+	Select from list	+	134	⚙
Juniper_Data_VLAN_100	+	Select from list	+	20	⚙
Juniper_Data_VLAN_100_ACL	+	Select from list	+	1	⚙
Juniper_Data_VLAN_100_dACL	+	Select from list	+	7	⚙

Rule	If the endpoint	Then the switch assigns the port/supplicant to
VLAN 500 for Polycom IP Phones connected to Juniper EX Switches	Passes network access authentication AND the request comes from a Juniper EX switch AND the endpoint is in the Polycom-IP-Phone group	Voice VLAN 500
VLAN 100 for dot1x users connected to Juniper EX Switches	Passes network access authentication AND the request comes from a Juniper EX switch AND the endpoint is in the VLAN_100_User_ID_Group	Data VLAN 100
VLAN 100 with ACL for dot1x users connected to Juniper EX Switches	Passes network access authentication AND the request comes from a Juniper EX switch AND the endpoint is in the VLAN_100_ACL_User_ID_Group	Data VLAN 100 and an ACL
VLAN 100 with dACL for dot1x users connected to Juniper EX Switches	Passes network access authentication AND the request comes from a Juniper EX switch AND the endpoint is in the VLAN_100_dACL_User_ID_Group	Data VLAN 100 and a dynamic/downloadable ACL

Configure a Cisco ISE Policy to Enable Guest Access

For guest access use-cases involving the Cisco ISE guest portal, Juniper EX switches support Juniper-CWA-Redirect-URL VSA along with a special Filter-Id JNPR_RSVD_FILTER_CWA to redirect unknown guest clients to the Cisco ISE portal. The following diagram outlines the guest access flow with Cisco ISE:



Here's the Juniper EX switch configuration for this scenario:

```

set groups top access profile dot1x authentication-order radius
set groups top access profile dot1x radius authentication-server <ISE IP>
set groups top access profile dot1x radius accounting-server <ISE IP>

set groups top access profile dot1x radius-server <ISE IP> dynamic-request-port
3799
set groups top access profile dot1x radius-server <ISE IP> secret
"$9$ikPQtpBESe01Nbs2GUHqmf39tulSyK"
set groups top access profile dot1x radius-server <ISE IP> source-address <switch
IP>
set protocols dot1x authenticator authentication-profile-name dot1x
set protocols dot1x authenticator interface wired-1x mac-radius
set groups wired-1x interfaces <*> unit 0 family ethernet-switching vlan members
corp
set interfaces interface-range wired-1x member ge-0/0/1
set interfaces interface-range wired-1x apply-groups wired-1x

```

Here's how to configure a Cisco ISE policy to enable guest access:

1. In Cisco ISE, choose **Policy Sets > Wired Access**.
2. Verify that the WIRED MAB authentication policy is set to **Internal Endpoints** for the data store and **Continue** for **If User not found** and **If Process fail**.

Policy Sets → Wired Access

Reset Policyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Wired Access		OR Wired_MAB Wired_802.1X	Default Network Access	10

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	WIRED MAB	Wired_MAB	Internal Endpoints Options If Auth fail CONTINUE If User not found CONTINUE If Process fail CONTINUE	9	⚙️

3. Create two authorization policies. If the client (MAC) already registered in the GuestEndpoints Identity Group, Cisco ISE will send a "Permit Access" message. Otherwise, Cisco ISE will send a CWA Redirect attribute to move the client to the Cisco ISE guest portal.

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Registered Guest	AND IdentityGroup-Name EQUALS Endpoint Identity Groups:GuestEndpoints Wired_MAB	PermitAccess	0	⚙️
✓	Unregistered Guest	Wired_MAB	Guest Redirect Wired	9	⚙️

Here's an example of the Guest Redirect Wired authorization profile configuration.

NOTE: You'll need to configure a static IP address instead of the FQDN for the CWA Filter to work. Alternatively, you can use a Juniper-Switching-Filter with a FQDN-based redirect URL.

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile:

Common Tasks

☒ ACL (Filter-ID):

☒ Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Centralized Web Auth: Value:

☒ Display Certificates Renewal Message

☒ Static IP/Host name/FQDN:

☐ Suppress Profiler CoA for endpoints in Logical Profile

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
 Filter-ID = JNPR_RSVD_FILTER_CWA
 Juniper-CWA-Redirect-URL = https://10.0.75.27:port/portal/gateway?SessionId=SessionIdValue&portal=deaaa863-1df0-4198-baf1-8d5b690d4361&daysToExpiry=value&action=cwa

4. Verify the configuration in the EX switch CLI:


```

root@ZTP-BRQLAB-EX12P-1> show dot1x interface ge-0/0/6 detail
ge-0/0/6.0
  Role: Authenticator|
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Mac Radius Authentication Protocol: EAP-MD5
  Reauthentication: Enabled
  Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: not configured
  Number of connected supplicants: 1
    Supplicant: 803f5d000dc9, 80:3F:5D:00:0D:C9
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: CWA Authentication
      Authenticated VLAN: lab-bonjour
      Dynamic Filter: JNPR_RSVD_FILTER_CWA
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3599 seconds
      Session Accounting Interim Interval: 600 seconds
      Accounting Update due in 599 seconds
      CWA Redirect URL :
      https://10.0.75.27:8443/portal/gateway?SessionId=0a004b1b/qSx9hV7cXn3FT/i
      Pb654VKunsaBAv8aT5D/OhhCAZc&portal=deaaa863-1df0-4198-baf1-
      8d5b690d4361&action=cwa&token=5f25dd4e72eff945fcae1497edef0fb8
      Eapol-Block: Not In Effect
      Domain: Data

```

Once the client authenticates with Cisco ISE, Cisco ISE sends a CoA. Upon re-authentication, the CLI output for the EX switch shows a successful MAC Authentication:

```

root@ZTP-BRQLAB-EX12P-1> show dot1x interface ge-0/0/6 detail
ge-0/0/6.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Mac Radius Authentication Protocol: EAP-MD5
  Reauthentication: Enabled
  Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: not configured
  Number of connected supplicants: 1
    Supplicant: 803f5d000dc9, 80:3F:5D:00:0D:C9
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
      Authenticated VLAN: lab-bonjour
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3408 seconds
      Session Accounting Interim Interval: 600 seconds
      Accounting Update due in 408 seconds
      Eapol-Block: Not In Effect
      Domain: Data

```

Configure a Colorless Port Using IETF Egress-VLAN-ID Attributes

With Junos 20.4 and above, you can automatically configure switch ports into access/trunk ports and assign multiple VLANs based on the RADIUS (Cisco ISE) response. For example, you can have a common port configuration on the switch and then reconfigure it automatically based on the identity of a connecting device, such as a Mist AP, a printer, or a corporate laptop.

Here's an example of how to automatically configure a port into a trunk port for Mist AP with an untagged native VLAN for management:

```

root@ex2300-brqlab-ztp> show ethernet-switching interface ge-0/0/4
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                        LH - MAC limit hit, DN - interface down,
                        MMAS - Mac-move action shutdown, AS - Autostate-exclude enabled,
                        SCTL - shutdown by Storm-control, MI - MAC+IP limit hit)

Logical      Vlan      TAG  MAC  MAC+IP  STP      Logical      Tagging
interface   members                limit  limit  state   interface flags
ge-0/0/4.0
management   51  16384  0      Forwarding  tagged,untagged
mgmt-primary  5   16384  0      Forwarding  tagged
corp          10  16384  0      Forwarding  tagged
mgmt-sw       50  16384  0      Forwarding  tagged
bonjour       200 16384  0      Forwarding  tagged
{master:0}

```

By default, the port is configured as an access port with 802.1X and MAC-Radius enabled.

```

root@ex2300-brqlab-ztp> show configuration protocols dot1x | display set
set protocols dot1x traceoptions file dot1x.log
set protocols dot1x traceoptions flag all
set protocols dot1x authenticator authentication-profile-name dot1x
set protocols dot1x authenticator interface mistap-1x mac-radius
set protocols dot1x authenticator interface wired-1x mac-radius

{master:0}
root@ex2300-brqlab-ztp> show ethernet-switching interface ge-0/0/4
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                        LH - MAC limit hit, DN - interface down,
                        MMAS - Mac-move action shutdown, AS - Autostate-exclude enabled,
                        SCTL - shutdown by Storm-control, MI - MAC+IP limit hit)

Logical      Vlan      TAG  MAC  MAC+IP  STP      Logical      Tagging
interface    members
ge-0/0/4.0
management   51    16384  0      Discarding
tagged,untagged
untagged

```

Here's how to create a new profiler policy in Cisco ISE to auto-profile Mist APs based on Mist MAC-OUI. The profiler policy will send the full switch port configuration (trunk, with native vlan 51 and all the other required VLAN tagged).

1. Choose **Policy > Profiling > Profiling Policies > Create New**.

Profiler Policy List > **MistAP**

Profiler Policy

* Name Description

Policy Enabled ☒

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

* Network Scan (NMAP) Action

Create an Identity Group for the policy ☒ Yes, create matching Identity Group
☐ No, use existing Identity Group hierarchy

* Parent Policy

* Associated CoA Type

System Type Administrator Created

Rules

If Condition Then

If Condition Expression

2. Create two rules using Radius_Calling_Station_ID_STARTSWITH 5c-5b-35 or d2-20-b0 to specify the current Mist MAC OUIs.
3. Save your profiler policy.
4. Navigate to your profiler policy and add another authorization rule:

☒ 802.1X Wired OR ☐ Wired_802.1X

☐ Wired_MAB

Default Network Access 12

Policy Sets → 802.1X Wired

Status	Policy Set Name	Description	Conditions
<div>Search</div>			
<div><div></div></div>	802.1X Wired	OR	<div><div></div>Wired_802.1X</div> <div><div></div>Wired_MAB</div>
<div>➤ Authentication Policy (2)</div>			
<div>➤ Authorization Policy - Local Exceptions</div>			
<div>➤ Authorization Policy - Global Exceptions</div>			
<div>▼ Authorization Policy (4)</div>			
<div><div>+</div></div>	Status	Rule Name	Conditions
			Results
			Profiles
<div>Search</div>			
<div><div></div></div>	Authorization Rule 3	AND	<div><div></div>Wired_MAB</div> <div><div></div>IdentityGroup Name EQUALS Endpoint Identity Groups:Profiled MistAP</div>
			<div><div>✖TRUNK-MIST-AP</div></div> <div><div></div></div>

The authorization profile looks like this:

Authorization Profiles > **TRUNK-MIST-AP**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

Common Tasks

- ☐ ACL
- ☐ Security Group

Advanced Attributes Settings

Radius:Egress-VLANID	=	52428851	Tag ID	1	Edit Tag
Radius:Egress-VLANID	=	51380274	Tag ID	1	Edit Tag
Radius:Egress-VLANID	=	51380234	Tag ID	1	Edit Tag
Radius:Egress-VLANID	=	51380424	Tag ID	1	Edit Tag
Radius:Egress-VLANID	=	51380229	Tag ID	1	Edit Tag
Radius:Tunnel-Medium-Type	=	802	Tag ID	1	Edit Tag
Radius:Tunnel-Type	=	VLAN	Tag ID	1	Edit Tag

How did we get all the numbers above? We used the following formula:

1. Create hex values for each VLAN you want to push in access-accept. The hex format is **0x31000005**. The first seven characters can either be 0x31000 (tagged) or 0x32000 (untagged). The last three characters are the actual VLAN ID converted to hex. You can use a [Decimal to hexadecimal converter](#) to figure out the hexadecimal value. For example, to send untagged VLAN 51, the value is 0x32000033.
2. Once you enter this hex value, convert the whole value back to decimal. You can use this [Hexidecimal to decimal converter](#) to figure out the decimal value.

In this example, if you convert 0x32000033 to decimal, the value is 52428851.

3. Configure the Cisco ISE authorization profile using the decimal value.

Authorization Profiles > **TRUNK-MIST-AP**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

▼ Common Tasks

- ☐ ACL
- ☐ Security Group

▼ Advanced Attributes Settings

Radius:Egress-VLANID	=	52428851	
Radius:Egress-VLANID	=	51380274	
Radius:Egress-VLANID	=	51380234	
Radius:Egress-VLANID	=	51380424	
Radius:Egress-VLANID	=	51380229	
Radius:Tunnel-Medium-Type	=	802	Tag ID 1 <input type="button" value="Edit Tag"/>
Radius:Tunnel-Type	=	VLAN	Tag ID 1 <input type="button" value="Edit Tag"/>

4. Plug in a Mist AP and verify the output:

```
root@ex2300-brqlab-ztp> show dot1x interface ge-0/0/4 detail
ge-0/0/4.0
```

```
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Mac Radius Authentication Protocol: EAP-MD5
  Reauthentication: Enabled
  Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: not configured
  Number of connected supplicants: 1
    Supplicant: 5c5b3550c74c, 5C:5B:35:50:C7:4C
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
      Authenticated VLAN: management
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3598 seconds
      Egress Vlan: 5, 10, 50, 51, 200
      Eapol-Block: Not In Effect
      Domain: Data
```

```
{master:0}
```

```
root@ex2300-brqlab-ztp> show ethernet-switching interface ge-0/0/4
```

```
Routing Instance Name : default-switch
```

```
Logical Interface flags (DL - disable learning, AD - packet action drop,
                        LH - MAC limit hit, DN - interface down,
                        MMAS - Mac-move action shutdown, AS - Autostate-exclude enabled,
                        SCTL - shutdown by Storm-control, MI - MAC+IP limit hit)
```

Logical interface	Vlan members	TAG	MAC limit	MAC+IP limit	STP state	Logical interface flags	Tagging
ge-0/0/4.0			16384	0			tagged,untagged
	management	51	16384	0	Forwarding		untagged
	mgmt-primary	5	16384	0	Forwarding		tagged
	corp	10	16384	0	Forwarding		tagged
	mgmt-sw	50	16384	0	Forwarding		tagged
	bonjour	200	16384	0	Forwarding		tagged

```
{master:0}
```


Configure the 802.1X Protocol on the EX Switch

```

set protocols lldp interface all
set protocols lldp-med interface all //LLDP-MED is used to signal to the IP Phone what
tagged Voice VLAN to use.

set interfaces ge-0/0/0 description "IP Phone and PC"
set interfaces ge-0/0/0 unit 0 family ethernet-switching interface-mode
access
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members
blackhole

set interfaces ge-0/0/1 description "Network Printer"
set interfaces ge-0/0/1 unit 0 family ethernet-switching interface-mode
access
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members
blackhole

set vlans blackhole vlan-id 666
set vlans data vlan-id 100
set vlans voice vlan-id 500

set access radius-server 172.30.104.85 secret secret-radius-password-here
set access profile cisco-ise-dot1x authentication-order radius
set access profile cisco-ise-dot1x radius authentication-server
172.30.104.85

set access profile cisco-ise-dot1x radius accounting-server 172.30.104.85
set access profile cisco-ise-dot1x radius options nas-port-type ethernet
ethernet
set access profile cisco-ise-dot1x accounting order radius
set access profile cisco-ise-dot1x accounting accounting-stop-on-failure
set access profile cisco-ise-dot1x accounting accounting-stop-on-access-
deny
set access profile cisco-ise-dot1x accounting coa-immediate-update
set access profile cisco-ise-dot1x accounting update-interval 30

set protocols dot1x authenticator authentication-profile-name cisco-ise-
dot1x
set protocols dot1x authenticator radius-options use-vlan-id

```

Note, the timers below may require tweaking for your specific environment.

```

set protocols dot1x authenticator interface ge-0/0/0.0 authentication-order
dot1x
set protocols dot1x authenticator interface ge-0/0/0.0 authentication-order
mac-radius
set protocols dot1x authenticator interface ge-0/0/0.0 supplicant multiple
set protocols dot1x authenticator interface ge-0/0/0.0 transmit-period 1
set protocols dot1x authenticator interface ge-0/0/0.0 mac-radius
set protocols dot1x authenticator interface ge-0/0/0.0 reauthentication
3600
set protocols dot1x authenticator interface ge-0/0/0.0 supplicant-timeout
10
set protocols dot1x authenticator interface ge-0/0/0.0 maximum-requests 3
set protocols dot1x authenticator interface ge-0/0/0.0 guest-vlan blackhole
set protocols dot1x authenticator interface ge-0/0/0.0 server-reject-vlan
blackhole
set protocols dot1x authenticator interface ge-0/0/0.0 server-fail vlan-
name blackhole
set protocols dot1x authenticator interface ge-0/0/0.0 server-fail-voip
use-cache

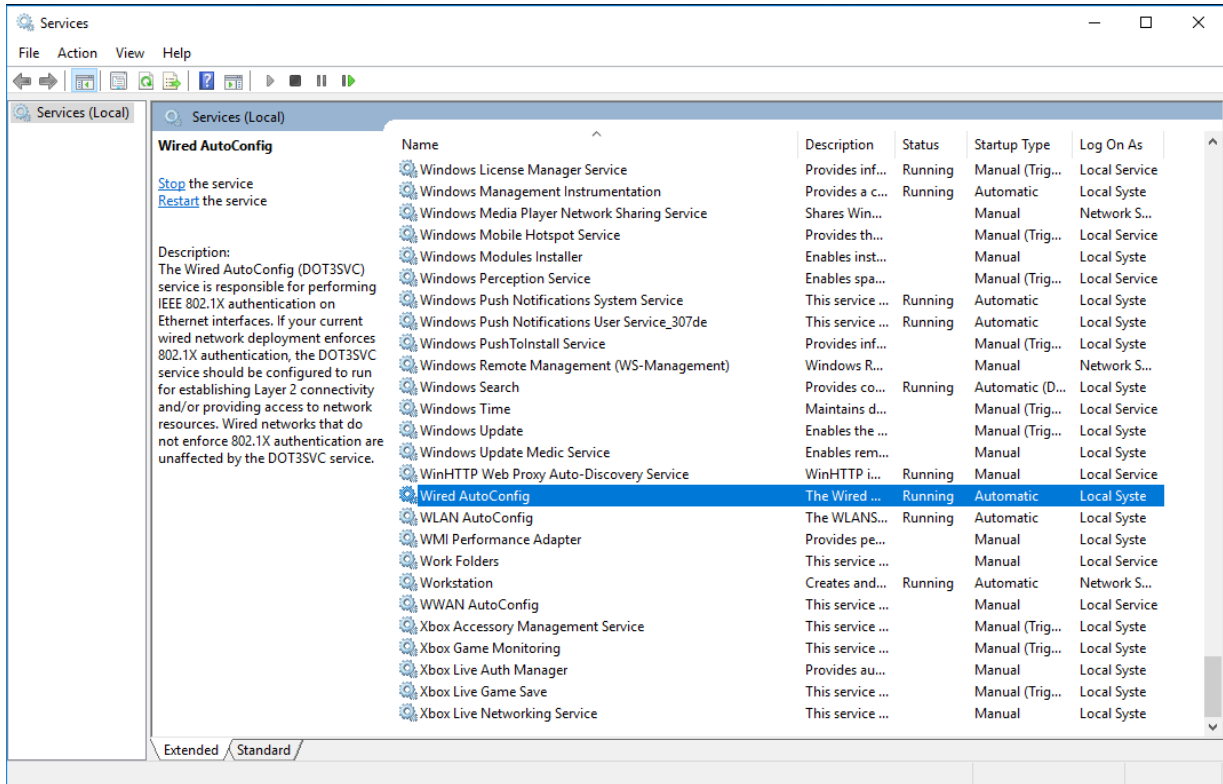
set protocols dot1x authenticator interface ge-0/0/0.1 authentication-order
mac-radius
set protocols dot1x authenticator interface ge-0/0/0.1 supplicant single
set protocols dot1x authenticator interface ge-0/0/0.1 transmit-period 1
set protocols dot1x authenticator interface ge-0/0/0.1 mac-radius
set protocols dot1x authenticator interface ge-0/0/0.1 reauthentication
3600
set protocols dot1x authenticator interface ge-0/0/0.1 supplicant-timeout
10
set protocols dot1x authenticator interface ge-0/0/0.1 maximum-requests 3
set protocols dot1x authenticator interface ge-0/0/0.1 guest-vlan blackhole
set protocols dot1x authenticator interface ge-0/0/0.1 server-reject-vlan
blackhole
set protocols dot1x authenticator interface ge-0/0/0.1 server-fail vlan-
name blackhole

set firewall family ethernet-switching filter deny_all term t1 then discard

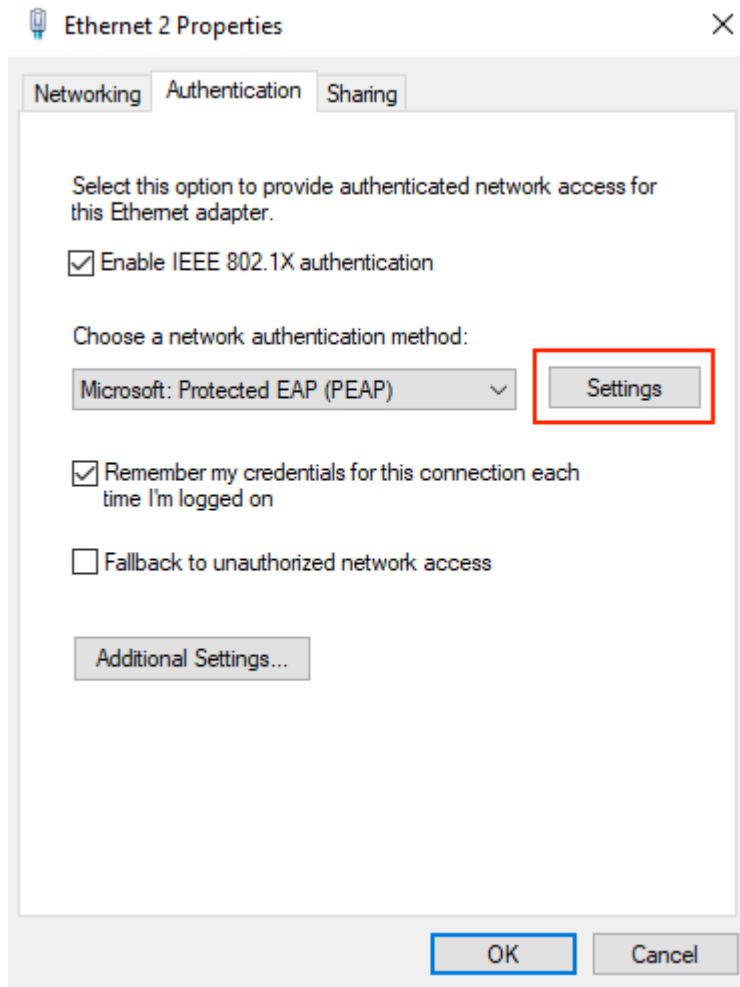
```

Configure Windows 10


1. Press the Windows key on your keyboard and search for services.msc.
2. Right click to enable the Wired Autoconfig service.



3. Choose **Control Panel/Settings > Network and Internet > Ethernet > Change Adapter Settings**.
4. Right click on the adapter used for your wired connection.
5. Click the **Authentication** tab and then click **Settings**.



6. Clear the check box to verify the server identity certificate.



CAUTION: This is for testing purposes only. Never disable this in production. Always provision your clients with trusted CA certifications.

7. Click **OK**.

Protected EAP Properties

When connecting:

☐ Verify the server's identity by validating the certificate

☐ Connect to these servers (examples: srv1;srv2;.*\,srv3\,com):

Trusted Root Certification Authorities:

- ☐ AddTrust External CA Root
- ☐ Baltimore CyberTrust Root
- ☐ Certum Trusted Network CA
- ☐ Class 3 Public Primary Certification Authority
- ☐ DigiCert Assured ID Root CA
- ☐ DigiCert Global Root CA
- ☐ DigiCert High Assurance EV Root CA

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

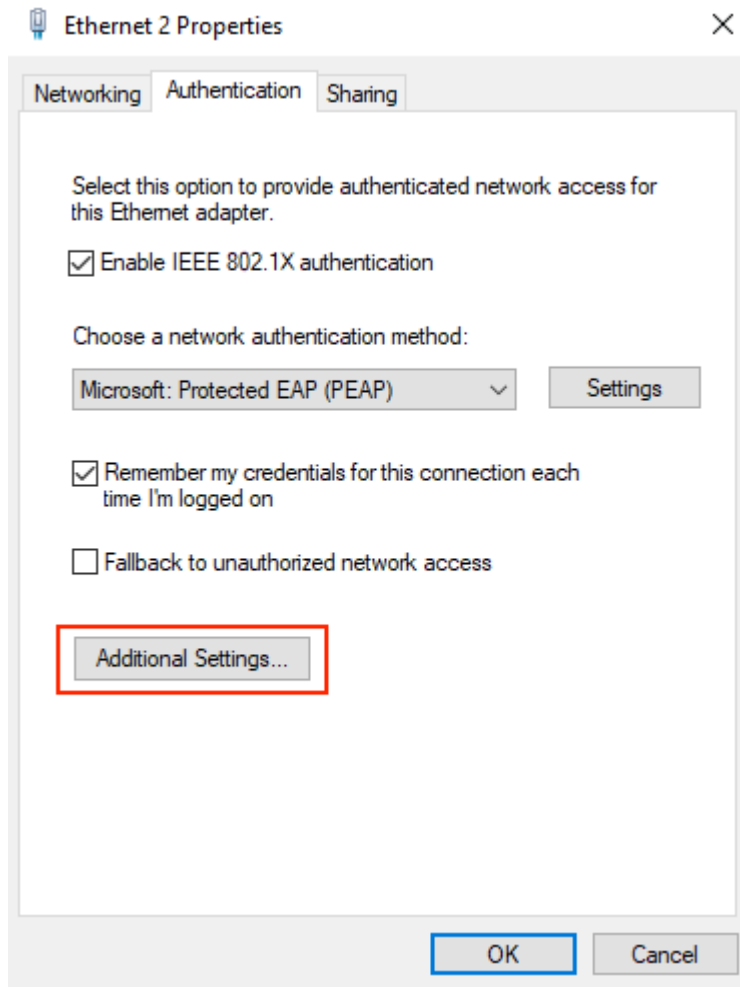
☒ Enable Fast Reconnect

☐ Disconnect if server does not present cryptobinding TLV

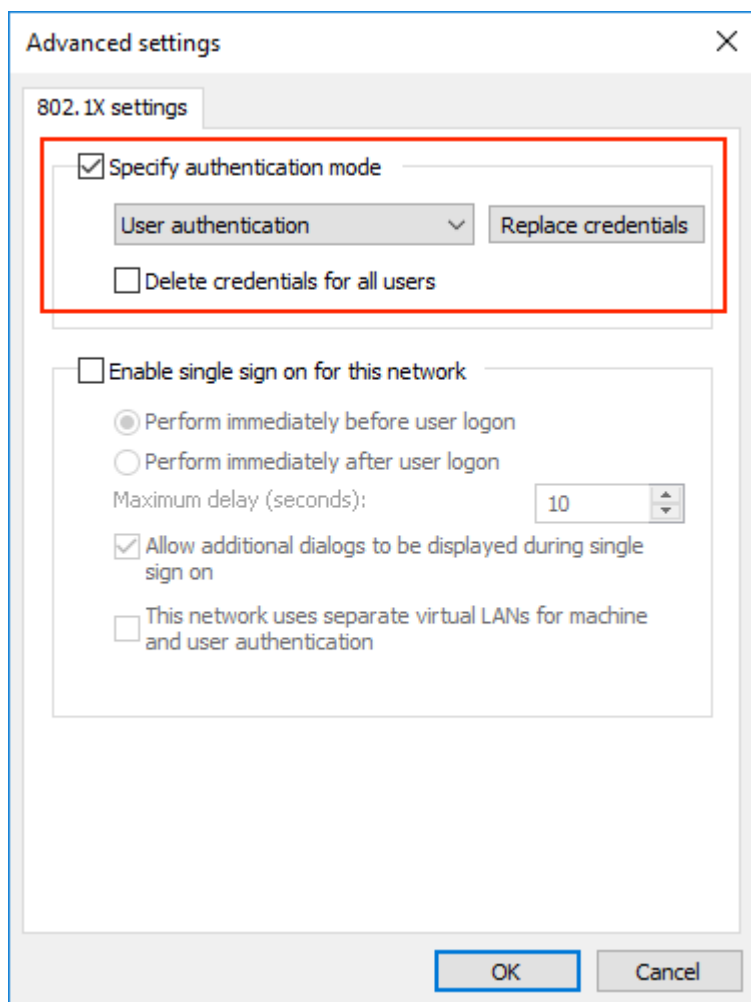
☐ Enable Identity Privacy

OK Cancel

NOTE: In a production environment, you need to install the Cisco ISE certificate. Refer to the [Cisco Identity Services Engine Administrator Guide, Release 2.4](#).



8. Select **User Authentication mode** and click **Replace Credentials**.
9. Enter the username and password, for example user1, user2 or user3.
10. Click **OK**.



Testing and Validation

IN THIS SECTION

- [Verify IP Phone Authentication Status | 48](#)
- [Verify Connections to Windows 10 Clients | 50](#)

Verify IP Phone Authentication Status

1. After connecting the IP Phone to port ge-0/0/0, run the **show dot1x interface ge-0/0/0** command to verify it is authenticated using MAC Authentication Bypass.

```
root@ex2300-r04-01> show dot1x interface ge-0/0/0
802.1X Information:
Interface    Role          State          MAC address    User
ge-0/0/0.0   Authenticator Authenticated   00:04:F2:8B:D1 0004f28b69d1
```

2. Run the **show dot1x interface ge-0/0/0 detail** command to view the detailed output and verify that you are using MAC Radius to authenticate the IP Phone.

```
root@ex2300-r04-01> show dot1x interface ge-0/0/0 detail
ge-0/0/0.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 1 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Mac Radius Authentication Protocol: EAP-MD5
  Reauthentication: Enabled
  Reauthentication interval: 3600 seconds
  Supplicant timeout: 10 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 3
  Guest VLAN member: blackhole
  Number of connected supplicants: 1
    Supplicant: 0004f28b69d1, 00:04:F2:8B:D1
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
      Authenticated VLAN: blackhole
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3364 seconds
      Session Accounting Interim Interval: 1800 seconds
      Accounting Update due in 1564 seconds
      Eapol-Block: Not In Effect
```

3. Run the **show ethernet-switching interface ge-0/0/0** command to verify that Cisco ISE has applied Voice VLAN 500 as a tagged VLAN on port ge-0/0/0.


```

root@ex2300-r04-01> show ethernet-switching interface ge-0/0/0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                        LH - MAC limit hit, DN - interface down,
                        MMAS - Mac-move action shutdown, AS - Autostate-exclude enabled,
                        SCTL - shutdown by Storm-control, MI - MAC+IP limit hit)

Logical      Vlan      TAG  MAC  MAC+IP STP      Logical      Tagging
interface   members                                interface flags
ge-0/0/0.0
            blackhole  666  16384 0      Forwarding  tagged,untagged
            voice      500  16384 0      Forwarding  tagged

```

- Run the `show lldp neighbors interface ge-0/0/0` command to view the LLDP output and verify that the IP Phone is using tagged VLAN 500 for Voice.

```

root@ex2300-r04-01> show lldp neighbors interface ge-0/0/0
LLDP Neighbor Information:
Local Information:
Index: 9 Time to live: 120 Time mark: Tue Aug 28 11:12:20 2018 Age: 0 secs
Local Interface : ge-0/0/0
Parent Interface : -
Local Port ID : 513
Ageout Count : 0

Neighbour Information:
Chassis type : Network address
Chassis ID : 0.0.0.0
Port type : Mac address
Port ID : 00:04:f2:8b:69:d1
Port description : 1
System name : Polycm VVX 310

System Description : Polycm;VVX-VVX_310;3111-46161-001,2;SIP/5.5.1.11526/22-Nov-16 15:05;UP/5.7.1.13261/22-Nov-16 15:40;

System capabilities
Supported: Bridge Telephone
Enabled : Telephone
Media endpoint class: Class III Device

MED Hardware revision : 3111-46161-001,2
MED Firmware revision : UP/5.7.1.13261/22-Nov-16 15:40
MED Software revision : SIP/5.5.1.11526/22-Nov-16 15:05
MED Serial number : 0004f28b69d1
MED Manufacturer name : Polycm
MED Model name : VVX-VVX_310

Organization Info
  OUI : IEEE 802.3 Private (0x00120f)
  Subtype : MAC/PHY Configuration/Status (1)
  Info : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation Capability (0x6c01), MAU Type (0x1e)
  Index : 1

Organization Info
  OUI : TIA TR 41 Committee (0x0012bb)
  Subtype : Media Capabilities (1)
  Info : Capabilities [LLDP-Med capable, Network policy capable, Location ID not capable, MDI-PSE not capable, MDI-PD capable, Inventory capable (0x33)]
  Info : Class Type [Extended Class 3 (3)]
  Index : 2

Organization Info
  OUI : TIA TR 41 Committee (0x0012bb)
  Subtype : Network policy (2)
  Info : Application Type [Voice]
  Info : Status [Policy defined, Tagged, VID (500), L2 Priority (5), DSCP Priority (46)]
  Index : 3

Organization Info
  OUI : TIA TR 41 Committee (0x0012bb)
  Subtype : Network policy (2)
  Info : Application Type [Voice signaling]
  Info : Status [Policy defined, Tagged, VID (500), L2 Priority (5), DSCP Priority (44)]
  Index : 4

```

- Verify authentication status in Cisco ISE. Choose **Operations > Live Logs**.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address	Network Device	Device Port	Identity Group
Aug 28, 2018 11:30:49.558 AM			58	00:04:F2:8B:69:D1	00:04:F2:8B:69:D1	Polysom-De...	Default >> MAB	Default >> VLAN 500 for Polysom IP Phones ...	Juniper_VoIP_VLAN_500			ge-0/5/5	
Aug 28, 2018 12:09:10.424 AM				00:04:F2:8B:69:D1	00:04:F2:8B:69:D1	Polysom-De...	Default >> MAB	Default >> VLAN 500 for Polysom IP Phones ...	Juniper_VoIP_VLAN_500		ex2300-r04-01	ge-0/5/5	Polysom-IP-Phone

6. Choose **Operations > Live Sessions**.

	802.1X Wired	OR	Wired_802.1X Wired_MAB	Default Network Access	+	12		
--	--------------	----	---------------------------	------------------------	---	----	--	--

Verify Connections to Windows 10 Clients

IN THIS SECTION

- [Verify User 1 | 50](#)
- [Verify User 2 | 52](#)
- [Verify User 3 | 55](#)
- [Verify CoA Session Disconnect with Port Bounce | 57](#)

Verify User 1

1. Enter the dot1x credentials in Windows for user1 and connect the PC to the IP Phone. Verify that User1 is authenticated:

```

root@ex2300-r04-01> show dot1x interface
802.1X Information:
Interface    Role           State           MAC address     User
ge-0/0/0.0   Authenticator  Authenticated   00:04:F2:8B:69:D1  0004f28b69d1
ge-0/0/0.0   Authenticator  Authenticated   00:E0:4C:68:00:FE  user2

```

2. Verify that Cisco ISE has applied Data VLAN 100 to port ge-0/0/0:

```

root@ex2300-r04-01> show dot1x interface detail
ge-0/0/0.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 1 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Mac Radius Authentication Protocol: EAP-MD5
  Reauthentication: Enabled
  Reauthentication interval: 3600 seconds
  Supplicant timeout: 10 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 3
  Guest VLAN member: blackhole
  Number of connected supplicants: 2
    Supplicant: 0004f28b69d1, 00:04:F2:8B:69:D1
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
      Authenticated VLAN: blackhole
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3370 seconds
      Session Accounting Interim Interval: 1800 seconds
      Accounting Update due in 1570 seconds
      Eapol-Block: Not In Effect
    Supplicant: user2, 00:E0:4C:68:00:FE
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Radius
      Authenticated VLAN: data
      Dynamic Filter: deny_all
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3460 seconds
      Session Accounting Interim Interval: 1800 seconds
      Accounting Update due in 1660 seconds
      Eapol-Block: Not In Effect

```

```

root@ex2300-r04-01> show ethernet-switching interface ge-0/0/0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                        LH - MAC limit hit, DN - interface down,
                        MMAS - Mac-move action shutdown, AS - Autostate-exclude enabled,
                        SCTL - shutdown by Storm-control, MI - MAC+IP limit hit)

Logical interface      Vlan      TAG  MAC  MAC+IP  STP      Logical      Tagging
interface             members   TAG  limit limit state   interface flags
ge-0/0/0.0
                      blackhole  666  16384 0        Forwarding
                      data        100  16384 0        Forwarding
                      voice      500  16384 0        Forwarding

```

3. View the Cisco ISE logs. Choose **Operations > Live Logs**.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles
x				user1	x Endpoint ID	Endpoint Prof	Authentication Policy	Authorization Policy	Authorization Profiles
Aug 28, 2018 12:32:57.302 PM			0	user1	00:E0:4C:68:00:FE	Unknown	Default >> Dot1X	Default >> VLAN 100 for dot1x users connect...	Juniper_Data_VLAN_100
Aug 28, 2018 12:02:57.273 PM				user1	00:E0:4C:68:00:FE	Unknown	Default >> Dot1X	Default >> VLAN 100 for dot1x users connect...	Juniper_Data_VLAN_100

4. Choose Operations > Live Sessions

Initiated	Updated	Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Server	Auth Met...	Authentication Protocol	Authentication Policy	Authorization Policy
x				Endpoint ID	Identity	IP Address	Endpoint Profile	Server	Auth Method	Authentication Protocol	Authentication Policy	Authorization Policy
Aug 28, 2018 11:39:49.922 AM	Aug 28, 2018 11:39:50.508 AM	Started	Show CoA Actions	00:04:F2:8B:69:D1	00:04:F2:8B:69:D1		Polycom-Device	nw-cisco-b...	mab	EAP-MD5	Default >> MAB	Default >> VLAN 900 for Poly...

Verify User 2

1. Change credentials in Windows to user2.
2. Verify that user2 is authenticated.

```

root@ex2300-r04-01> show dot1x interface ge-0/0/0
802.1X Information:
Interface   Role           State           MAC address     User
ge-0/0/0.0  Authenticator  Authenticated   00:04:F2:8B:69:D1  0004f28b69d1
ge-0/0/0.0  Authenticator  Authenticated   00:E0:4C:68:00:FE  user1

```

3. Verify that Cisco ISE has applied Data VLAN 100, and also applied the locally configured firewall filter/ACL called deny_all.

```

root@ex2300-r04-01> show dot1x interface detail
ge-0/0/0.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 1 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Mac Radius Authentication Protocol: EAP-MD5
  Reauthentication: Enabled
  Reauthentication interval: 3600 seconds
  Supplicant timeout: 10 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 3
  Guest VLAN member: blackhole
  Number of connected supplicants: 2
    Supplicant: 0004f28b69d1, 00:04:F2:8B:69:D1
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
      Authenticated VLAN: blackhole
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3370 seconds
      Session Accounting Interim Interval: 1800 seconds
      Accounting Update due in 1570 seconds
      Eapol-Block: Not In Effect
    Supplicant: user2, 00:E0:4C:68:00:FE
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Radius
      Authenticated VLAN: data
      Dynamic Filter: deny_all
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3460 seconds
      Session Accounting Interim Interval: 1800 seconds
      Accounting Update due in 1660 seconds
      Eapol-Block: Not In Effect

```

4. Verify that the firewall filter is active for the supplicant.

```

root@ex2300-r04-01> show dot1x interface detail
ge-0/0/0.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Multiple
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 1 seconds
Mac Radius: Enabled
Mac Radius Restrict: Disabled
Mac Radius Authentication Protocol: EAP-MD5
Reauthentication: Enabled
Reauthentication interval: 3600 seconds
Supplicant timeout: 10 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 3
Guest VLAN member: blackhole
Number of connected supplicants: 2
  Supplicant: 0004f28b69d1, 00:04:F2:8B:69:D1
    Operational state: Authenticated
    Backend Authentication state: Idle
    Authentication method: Mac Radius
    Authenticated VLAN: blackhole
    Session Reauth interval: 3600 seconds
    Reauthentication due in 3589 seconds
    Session Accounting Interim Interval: 1800 seconds
    Accounting Update due in 1789 seconds
    Eapol-Block: Not In Effect
  Supplicant: user1, 00:E0:4C:68:00:FE
    Operational state: Authenticated
    Backend Authentication state: Idle
    Authentication method: Radius
    Authenticated VLAN: data
    Session Reauth interval: 3600 seconds
    Reauthentication due in 1124 seconds
    Session Accounting Interim Interval: 1800 seconds
    Accounting Update due in 1124 seconds
    Eapol-Block: Not In Effect

```

5. View the Cisco ISE logs. Choose **Operations -> Live Logs**. Note the different authorization policy applied for user2, Data VLAN 100 + ACL deny_all.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	
x				user2	x	Endpoint ID	Endpoint Prof	Authentication Policy	Authorization Policy	Authorization Profiles
Aug 28, 2018 01:14:13.281 PM			0	user2	00:E0:4C:68:00:FE	Unknown	Default >> Dot1X	Default >> VLAN 100 with ACL for dot1x users ...	Junipe_Data_VLAN_100_ACL	
Aug 28, 2018 01:14:13.245 PM				user2	00:E0:4C:68:00:FE	Unknown	Default >> Dot1X	Default >> VLAN 100 with ACL for dot1x users ...	Junipe_Data_VLAN_100_ACL	

6. Choose **Operations > Live Sessions**.

	Initiated	Updated	Session Status	Action	Endpoint ID	Identity	Endpoint Profile	Server	Auth Met...	Authentication Protocol	Authentication Policy	Authorization Policy	Authorization Profiles
x						user1	x						
	Aug 28, 2018 01:03:10.039 PM	Aug 28, 2018 01:03:10.139 PM	Started	Show CoA Actions	00:E0:4C:68:00:FE	user1	Unknown	ne-disc-h...	MSCHAPV2	PEAP (EAP-MSCHAPV2)	Default >> Dot1X	Default >> VLAN 100 for dot1...	Juniper_Data_VLAN_100

Verify User 3

1. Change credentials in Windows to user3.
2. Verify that user3 is authenticated.

```
root@ex2300-r04-01> show dot1x interface
802.1X Information:
Interface      Role           State           MAC address      User
ge-0/0/0.0    Authenticator  Authenticated   00:04:F2:8B:69:D1  0004f28b69d1
ge-0/0/0.0    Authenticator  Authenticated   00:E0:4C:68:00:FE  user3
```

3. Verify that Cisco ISE has applied Data VLAN 100, and also applied a dynamic/downloadable firewall filter/ACL to the supplicant.

```
root@ex2300-r04-01> show dot1x interface detail
ge-0/0/0.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Multiple
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 1 seconds
Mac Radius: Enabled
Mac Radius Restrict: Disabled
Mac Radius Authentication Protocol: EAP-MD5
Reauthentication: Enabled
Reauthentication interval: 3600 seconds
Supplicant timeout: 10 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 3
Guest VLAN member: blackhole
Number of connected supplicants: 2
  Supplicant: 0004f28b69d1, 00:04:F2:8B:69:D1
    Operational state: Authenticated
    Backend Authentication state: Idle
    Authentication method: Mac Radius
    Authenticated VLAN: blackhole
    Session Reauth interval: 3600 seconds
    Reauthentication due in 3536 seconds
    Session Accounting Interim Interval: 1800 seconds
    Accounting Update due in 1736 seconds
    Eapol-Block: Not In Effect
  Supplicant: user3, 00:E0:4C:68:00:FE
    Operational state: Authenticated
    Backend Authentication state: Idle
    Authentication method: Radius
    Authenticated VLAN: data
    Dynamic Filter: match destination-ip 1.1.1.1/32 action deny, match destination-ip 2.2.2.2/32 action deny, match destination-ip 0.0.0.0/0 action allow
    Session Reauth interval: 3600 seconds
    Reauthentication due in 3553 seconds
    Session Accounting Interim Interval: 1800 seconds
    Accounting Update due in 1753 seconds
    Eapol-Block: Not In Effect
```

4. Verify that the firewall filter is active for the supplicant. The terms should be in this order:
 - t0 is the first term
 - t1 is the second term
 - T term without a t-name is the last term to allow all traffic

```
root@ex2300-r04-01> show dot1x firewall
Filter name: dot1x_ge-0/0/0
Counters:
Name                                     Bytes      Packets
dot1x_ge-0/0/0_00e04c6800fe            71522      210
dot1x_ge-0/0/0_00e04c6800fe_t0           0           0
dot1x_ge-0/0/0_00e04c6800fe_t1           0           0
```


5. View the Cisco ISE logs. Choose **Operations > Live Logs**. Note the different authorization policy applied for user2, Data VLAN 100 + dACL.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	
x				user3	x	Endpoint ID	Endpoint Prof	Authentication Policy	Authorization Policy	Authorization Profiles
Aug 28, 2018 01:55:18.300 PM			0	user3	00:E0:4C:68:00:FE	Unknown	Default >> Dot1X	Default >> VLAN 100 with dACL for dot1x user...	Juniper_Data_VLAN_100_dACL	
Aug 28, 2018 01:55:18.226 PM				user3	00:E0:4C:68:00:FE	Unknown	Default >> Dot1X	Default >> VLAN 100 with dACL for dot1x user...	Juniper_Data_VLAN_100_dACL	

6. Choose **Operations > Live Sessions**.

Initiated	Updated	Session Status	Action	Endpoint ID	Identity	Endpoint Profile	Server	Auth Met...	Authentication Protocol	Authentication Policy	Authorization Policy	Authorization Profiles
x				Endpoint ID	user3	x	Endpoint Profile	Server	Auth Method	Authentication Protocol	Authentication Policy	Authorization Profiles
Aug 28, 2018 01:55:18.226 PM	Aug 28, 2018 01:55:18.300 PM	Started	Show CoA Actions	00:E0:4C:68:00:FE	user3	Unknown	new-disco-18...	MSCHAPV2	PEAP (EAP-MSCHAPV2)	Default >> Dot1X	Default >> VLAN 100 with dACL ...	Juniper_Data_VLAN_100_dACL

7. Verify that user3 is authenticated.

```
root@ex2300-r04-01> show dot1x interface
802.1X Information:
Interface      Role           State           MAC address     User
ge-0/0/0.0    Authenticator  Authenticated   00:04:F2:8B:69:D1  0004f28b69d1
ge-0/0/0.0    Authenticator  Authenticated   00:E0:4C:68:00:FE  user3
```

8. View the Cisco ISE log. Choose **Operations > Live Sessions > Show CoA Actions > Session termination** for user3.

9. Click **Show CoA Actions** and session termination.

Initiated	Updated	Session Status	Action	Endpoint ID	Identity
x				Endpoint ID	Identity
Sep 04, 2018 08:35:40.755 AM	Sep 04, 2018 08:35:40.779 AM	Started	Show CoA Actions	00:04:F2:8B:69:D1	00:04:F2:8B:69:D1
Sep 04, 2018 07:43:40.649 AM	Sep 04, 2018 08:12:49.580 AM	Started	Show CoA Actions		

Actions

- Session termination with port bounce
- Session termination

10. Verify that the user3 session is terminated.

```
root@ex2300-r04-01> show dot1x firewall
Filter name: dot1x_ge-0/0/0
Counters:
Name                                     Bytes           Packets
counter1__dot1x_ge-0/0/0_00e04c6800fe-deny_all-t1  15305           138
```


Verify CoA Session Disconnect with Port Bounce

1. Verify that the IP Phone is authenticated. (0004f228b69d1)

```
root@ex2300-r04-01> show dot1x interface
802.1X Information:
Interface      Role          State          MAC address    User
ge-0/0/0.0    Authenticator Authenticated   00:04:F2:8B:69:D1 0004f28b69d1
ge-0/0/0.0    Authenticator Authenticated   00:E0:4C:68:00:FE user3
```

2. View the Cisco ISE log. Choose **Operations > Live Sessions > Show CoA Actions > Session termination** for IP Phone.

3. Click **Show CoA Actions** then choose **Session termination with port bounce**.

Initiated	Updated	Session Status	Action	Endpoint ID	Identity
x					
Sep 04, 2018 08:40:08.400 AM	Sep 04, 2018 08:40:08.458 AM	Started	Show CoA Actions		
Sep 04, 2018 08:35:40.755 AM	Sep 04, 2018 08:35:40.779 AM	Started	Show CoA Actions	00:04:F2:8B:69:D1	00:04:F2:8B:69:D1

4. Run the command **show dot1x interface** and notice that all sessions are now terminated because the port was bounced.

```
root@ex2300-r04-01> show dot1x interface
802.1X Information:
Interface      Role          State          MAC address    User
ge-0/0/0.0    Authenticator Connecting
```

```
root@ex2300-r04-01> show dot1x statistics
Interface: ge-0/0/0.0
TxReqId = 4099 TxReq = 1528 TxTotal = 5627
RxStart = 5 RxLogoff = 0 RxRespId = 179 RxResp = 1526
CoA-Request = 1 CoA-Ack = 1 CoA-Nak = 0
RxInvalid = 0 RxLenErr = 0 RxTotal = 1710
LastRxVersion = 1 LastRxSrcMac = 00:04:f2:8b:69:d1
PortBounceReqRx = 1
```

```

root@ex2300-r04-01> show interfaces ge-0/0/0
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 648, SNMP ifIndex: 513
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Link-mode: Full-duplex, Speed: Auto,
  Loopback: Disabled, Source filtering: Disabled, Flow control: Disabled, Auto-negotiation
  Auto-MDIX: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 58:00:bb:9a:72:ac, Hardware address: 58:00:bb:9a:72:ac
  Last flapped   : 2018-09-04 10:48:42 CEST (00:00:14 ago)
  Input rate     : 4144 bps (2 pps)
  Output rate    : 3392 bps (2 pps)
  Active alarms  : None
  Active defects : None
  PCS statistics
    Bit errors           0
    Errored blocks       0
  Ethernet FEC statistics
    FEC Corrected Errors 0
    FEC Uncorrected Errors 0
    FEC Corrected Errors Rate 0
    FEC Uncorrected Errors Rate 0
  PRBS Statistics : Disabled
  Interface transmit statistics: Disabled

```