ExtremeCloud IQ - Site Engine and ExtremeControl – Cisco Switch Integration Guide

Abstract: This document details the utilization of a Cisco switch as an edge enforcement point in ExtremeControl using two enforcement methods, Downloadable ACLs (also known as Per-User ACLs) and Dynamic ACLs.

Part Number: 9037336-00 Rev AA

Published: January 2022

Extreme Networks, Inc.
6480 Via Del Oro
San Jose, California 95119
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000
www.extremenetworks.com

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see:
https://www.extremenetworks.com/Company/legal/trademarks/

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
https://www.extremenetworks.com/support/policies/open-source-declaration/

Contents

Acronyms

Term or Acronym	Definition
AAA	Authentication, Authorization, Accounting
ACL	Access Control List
NAC	Network Access Control
NAS	Network Access Server
VSA	Vendor Specific Attribute

Test Environment

Testing was performed on the following software and hardware models and versions. Newer versions should work similarly, although the commands might be different.

- ExtremeCloud IQ - Site Engine version 21.04.10.99
- ExtremeControl for ExtremeCloud IQ – Site Engine version 21.04.10.99
- Cisco C3750G-24TS-1U version 12.2(55)SE12

Overview

Five functions are required to fully integrate a Cisco switch into ExtremeControl.

1. Visibility – To gain end system visibility at the edge of the network, a method of authentication is required. For Cisco switches, both MAC and 802.1X authentication methods are supported.

2. IP Resolution – An additional component of visibility is to associate the correct IP address with each end system. Multiple mechanisms are utilized to resolve the IP address of an end system connecting to the network, including some methods specific to Cisco switching.

3. Re-authentication – When a device is connected to the network, a method to re-authenticate the device is necessary to allow roles to be dynamically changed for these end systems as they are pushed through the ExtremeControl authorization process.

4. Authorization – A method to enforce access restrictions is required to permit or deny access to network services (for example, HTTP or DNS). For Cisco switching, dynamically assigned ACLs are utilized to swap user roles and are considered a best practice. The use of VLANs is also an option, however, that is outside the scope of this document. This document describes two approaches for ACLs that are dynamically assigned per user session:

    a. Downloadable ACLs (also referred to as Per-User ACLs): A downloadable ACL is an ACL that is created and stored in the RADIUS Server, which is in this scenario ExtremeControl. The Network Access Server device (NAS), which in this case is the Cisco switch, does not save any pre-configured ACLs in the running configuration. Downloadable ACLs are installed on the switch upon successful authentication as part of RADIUS Access-Accept message. A downloadable ACL action can assign different ACLs per authenticated session.

    b. Dynamic ACLs: A dynamic ACL is an ACL that is pre-configured and stored in the NAS device (Cisco switch). Upon successful authentication, the RADIUS Server (ExtremeControl) sends the name of the pre-configured ACL as part of RADIUS Access-Accept message. A dynamic ACL action can assign different ACLs per authenticated session.

5. Web Redirection – When a captive portal is used as part of the ExtremeControl solution, a mechanism to redirect the client Web traffic to the Access Control Engine is required. For Cisco switches, a Vendor Specific Attribute (VSA) is utilized to redirect the client Web traffic.

Switch Configuration

The first section covers configuring the Cisco switch to be monitored by ExtremeCloud IQ - Site Engine and integrating ExtremeControl as a RADIUS server. All configurations are performed using CLI, and it is assumed that serial console access to the switch is available. Alternatively, some of the configuration can be automated via scripting in ExtremeCloud IQ - Site Engine, which is covered at the end of this section. The switch configuration is broken down into five parts:

- SNMP Configuration
- RADIUS Configuration
- Web-Redirect Configuration
- ACL Configuration
- Authentication Configuration

SNMP Configuration

For ExtremeControl to manage the Cisco switch, both SNMP read and write capabilities must be configured. It is highly recommended that the Cisco switch be configured to use SNMPv3 if possible. SNMPv3 has many advantages over v1 and v2 including security of communication and performance. To configure SNMP v3 on a Cisco switch, enter the following commands.

```
snmp-server group V3Group v3 auth read V3Read write V3Write
snmp-server user snmpuser V3Group v3 auth md5 snmpauthcred priv des
snmpprivcred
snmp-server view V3Read iso included
snmp-server view V3Write iso included
```

RADIUS Configuration

The Cisco switch must authenticate against ExtremeControl. For this authentication process to occur, the Access Control Engine needs to be configured as a RADIUS server within the switch configuration. Multiple command sets must be configured on the switch to complete the RADIUS configuration. First, you create the ‘aaa’ rules. These rules need to be carefully evaluated when being applied as it is quite easy to deny existing Telnet, SSH, or serial console access to the switch. As a best practice be sure to note if any of these commands already exist within the switch configuration and if so, adjust the new commands accordingly. If no ‘aaa’ commands are present, the following commands will need to be added. The last command creates a local account (admin) to administer the switch.

```
aaa new-model
aaa authentication login default local
aaa authentication enable default enable none

username admin privilege 15 password 0 MyPassword123
```

The following commands should be utilized to add the Access Control Engine as a RADIUS server. Note that the RADIUS shared secret will always be '*ETS_TAG_SHARED_SECRET*' in Access Control unless it is explicitly changed. The test username is used to verify that an Access Control Engine is alive and available. This account does not need to exist; the switch is just looking for a response from the server.

```
username test-radius privilege 0 password 0 BadPass123

radius-server host <EAC Engine IP> auth-port 1812 acct-port 1813 test
username test-radius key ETS_TAG_SHARED_SECRET

radius-server dead-criteria time 30 tries 3
radius-server vsa send accounting
radius-server vsa send authentication
ip radius source-interface vlan <VLAN Number>
```

After defining the Access Control Engine, add it to a group that can be used in the 'aaa' configuration. If multiple Access Control Engines are configured, add each one to the same group.

```
aaa group server radius EAC
 server <EAC Engine IP> auth-port 1812 acct-port 1813
```

Add the 'aaa' rules for the switch to authenticate devices against the Access Control Engine.

```
aaa authentication dot1x default group EAC
aaa authorization network default group EAC
aaa accounting dot1x default start-stop group EAC
aaa accounting update periodic 5
aaa session-id common
```

Adding the following commands enables RFC 3576 support. This is not required for Access Control but can be useful if problems arise with re-authentication. If using RFC 3576, an NTP server is recommended as the messages are time sensitive.

```
ntp server <NTP Server IP>

aaa server radius dynamic-author
  client <EAC Engine IP> server-key ETS_TAG_SHARED_SECRET
  auth-type any
```

The following global commands are used to assist in authentication recovery, tracking of devices, and logging.

```
ip device tracking
epm logging
authentication critical recovery delay 1000
authentication mac-move permit
dot1x critical eapol
```

Web-Redirect Configuration

Cisco uses a special ACL to redirect client web traffic to a captive portal. This ACL is written so that all traffic that matches a permit statement in the ACL will be redirected. Therefore, a deny statement matching the Access Control Engine IP address needs to be added so that redirected Web traffic does not get stuck in a redirect loop. A redirect ACL should be similar to the example below.

```
ip access-list extended Unregistered
 deny ip any host 10.8.255.106
 permit tcp any any eq www
 permit tcp any any eq 443
```

In addition to the ACL configuration, the HTTP server on the switch needs to be enabled in order to redirect traffic to a web server. The following commands can be used.

```
ip http server
ip http secure-server
```

ACL Configuration

ACL Configuration on the switch is only required if the "Dynamic ACL" method is used and ExtremeControl is only returning the name of the ACL as RADIUS Access-Accept message. Skip this part of the Cisco configuration if the Downloadable ACL method will be used.

For the Dynamic ACL method to work, ACLs must be preconfigured on the switch to allow Access Control to return a single RADIUS attribute that represents the assigned access for the end system. An example list of ACLs is below. Note that the ACL names (such as EnterpriseUser and GuestAccess) cannot contain spaces.

```
ip access-list extended Administrator
 permit ip any any
ip access-list extended EnterpriseUser
 permit ip any any
ip access-list extended GuestAccess
 permit ip any any
ip access-list extended Quarantine
 deny ip any host 10.8.255.106
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended Unregistered
 deny ip any host 10.8.255.106
 permit tcp any any eq www
 permit tcp any any eq 443
```

NOTE

Per Cisco's documentation: "For any ACL configured for multiple-host mode, the source portion of statement must be any. (For example, permit icmp any host 10.10.1.1.)". This is also true for multi-auth mode. If this ACL usage guidance is not followed, authorization will fail.

Authentication Configuration

Each Ethernet interface that is going to have an end system connected to it should have authentication enabled to allow visibility within ExtremeControl. Note, the commands below assume that 802.1X and MAC Authentication are both utilized on the edge switch ports. If 802.1X is not required, it can be removed from the command list. Additionally, these commands need to be merged with the existing commands on each interface. Lastly, the 'interface range' command can be used to simultaneously modify multiple interfaces.

```
interface GigabitEthernet 1/0/10
  switchport mode access
  switchport access vlan 3

  !Allows traffic before authentication is completed.
  authentication open

  !Useful for Printers and devices that send traffic infrequently.
  authentication control-direction in

  !Allow multiple devices to authenticate to a single port.
  authentication host-mode multi-auth

  !Re-authenticate periodically
  authentication periodic

  !Listen to session-timeout information from EAC.
  authentication timer reauthenticate server

  !If 802.1X fails, use MAC Authentication
  authentication event fail action next-method

  !If EAC fails, open access to the access vlan used above
  authentication event server dead action authorize vlan 3

  !When EAC comes back online, re-authenticate
  authentication event server alive action reinitialize

  !Use 802.1X first if available, then MAC Authentication Bypass
  authentication order dot1x mab
  authentication priority dot1x mab

  !If a device moves from one port to another, replace the existing session
  authentication violation replace

  !Enable MAC Authentication Bypass and 802.1X
  mab
  dot1x pae authenticator

  !Set 802.1X Timeout to 10 seconds. This can be adjusted if 802.1X timeout
is taking too long. If 802.1X is used in the network though, be careful of
```

```
making it too low.
  dot1x timeout tx-period 10

  !Set port as an edge port for Spanning Tree.
  spanning-tree portfast

  !Enable Authentication on this port
  authentication port-control auto
```

After entering all of these commands, an interface should look similar to this:

```
interface GigabitEthernet1/0/10
 switchport access vlan 3
 switchport mode access
 authentication control-direction in
 authentication event fail action next-method
 authentication event server dead action authorize vlan 3
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication violation replace
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
end
```

If 802.1X authentication is being utilized, then 802.1X must be enabled globally on the switch:

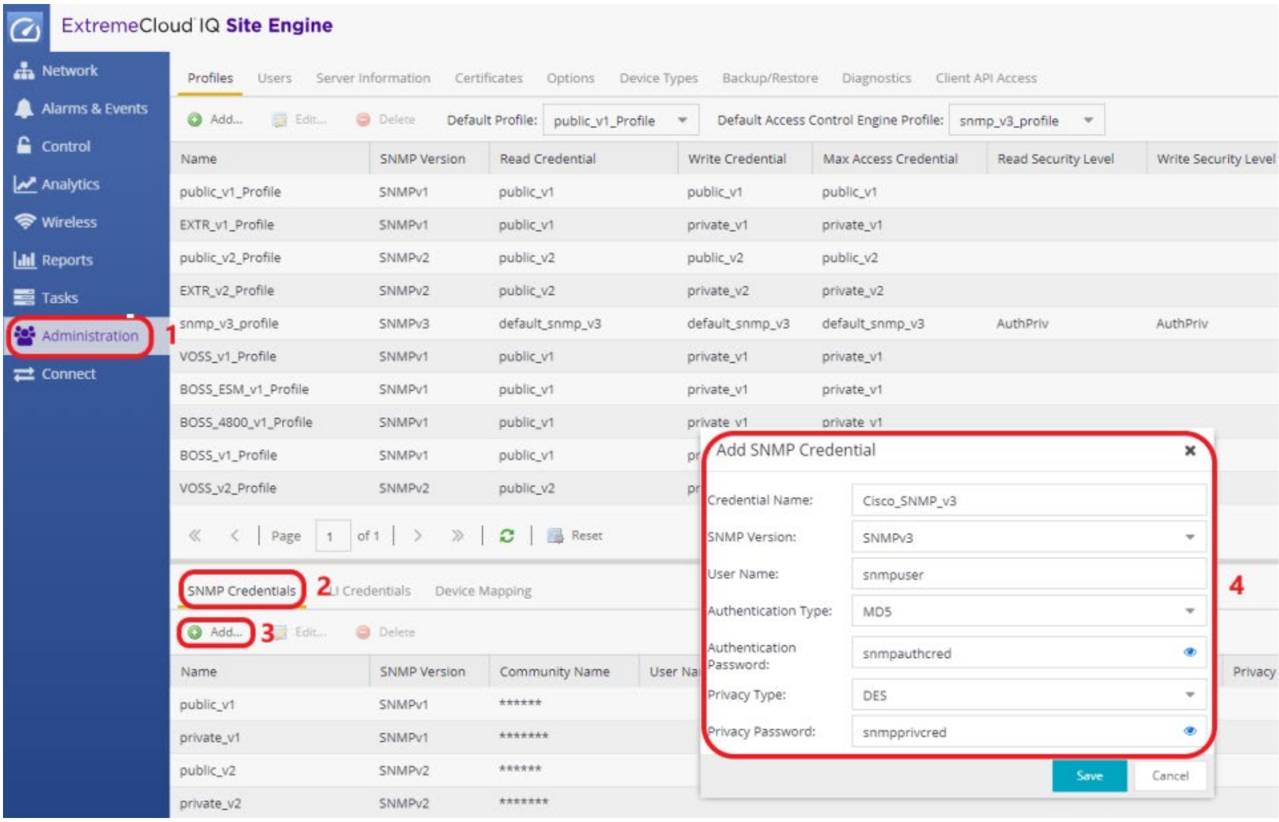
```
dot1x system-auth-control
```

ExtremeCloud IQ - Site Engine and ExtremeControl Configuration for Cisco Switches

Cisco Switch Discovery in ExtremeCloud IQ - Site Engine

In order to manage Cisco switches in ExtremeCloud IQ - Site Engine, the switch needs to be discovered and added to the ExtremeCloud IQ - Site Engine database. For this purpose, SNMP and CLI Credentials should be created and added to a Device Profile which will then be used during the discovery process.

As depicted in Figure 1, navigate to **Administration** and follow the steps to create SNMP and CLI credentials for the Cisco switch. Make sure to configure the same SNMP user name, authentication and privacy types and passwords that are configured on the switch.



Default Profile: public_v1_Profile

Default Access Control Engine Profile: snmp_v3_profile

Name	SNMP Version	Read Credential	Write Credential	Max Access Credential	Read Security Level	Write Security Level
public_v1_Profile	SNMPv1	public_v1	public_v1	public_v1		
EXTR_v1_Profile	SNMPv1	public_v1	private_v1	private_v1		
public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2		
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2		
snmp_v3_profile	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv
VOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1		
BOSS_ESM_v1_Profile	SNMPv1	public_v1	private_v1	private_v1		
BOSS_4800_v1_Profile	SNMPv1	public_v1	private_v1	private_v1		
BOSS_v1_Profile	SNMPv1	public_v1	pr			
VOSS_v2_Profile	SNMPv2	public_v2	pr			

Name	SNMP Version	Community Name	User Na	Privacy
public_v1	SNMPv1	******		
private_v1	SNMPv1	*******		
public_v2	SNMPv2	******		
private_v2	SNMPv2	*******		

Add SNMP Credential

Credential Name: Cisco_SNMP_v3

SNMP Version: SNMPv3

User Name: snmpuser

Authentication Type: MD5

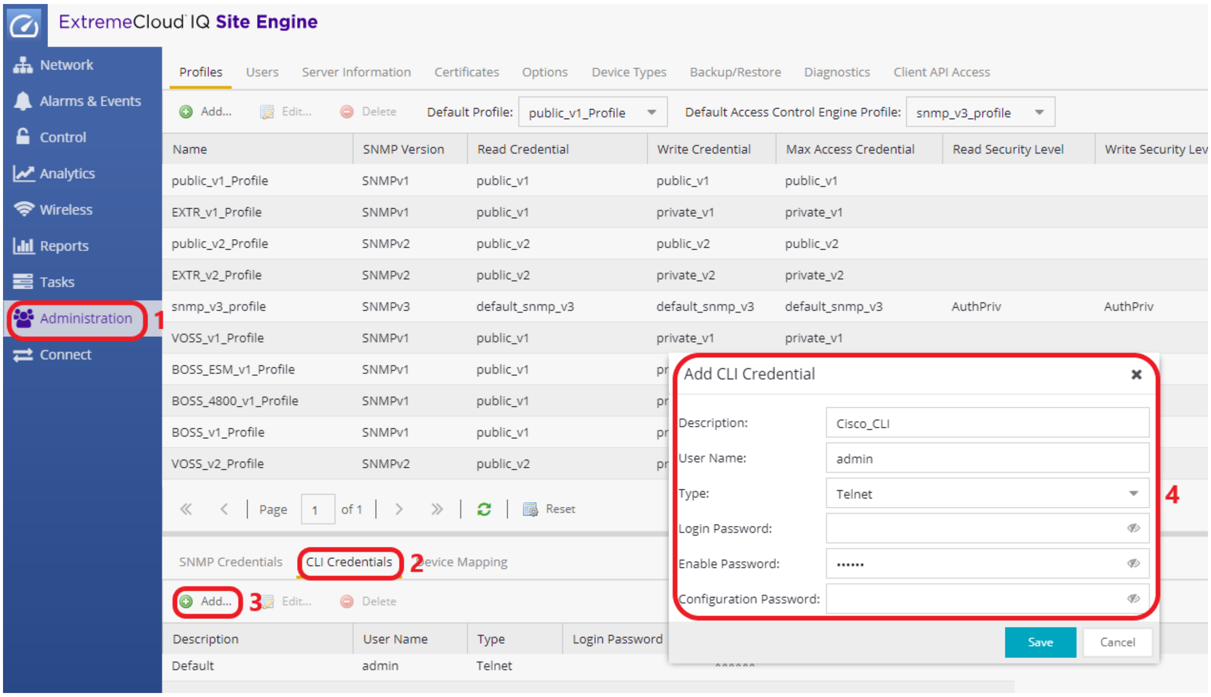
Authentication Password: snmpauthcred

Privacy Type: DES

Privacy Password: snmpprivcred

Figure 1 – How to configure SNMP credentials for a Cisco switch in ExtremeCloud IQ - Site Engine

A CLI credential is needed to access the CLI terminal of the device directly from ExtremeCloud IQ - Site Engine or to run a script/workflow that will interact with the device through the CLI. Note that a CLI credential is not required for ExtremeControl integration.



Default Profile: public_v1_Profile

Default Access Control Engine Profile: snmp_v3_profile

Name	SNMP Version	Read Credential	Write Credential	Max Access Credential	Read Security Level	Write Security Lev
public_v1_Profile	SNMPv1	public_v1	public_v1	public_v1		
EXTR_v1_Profile	SNMPv1	public_v1	private_v1	private_v1		
public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2		
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2		
snmp_v3_profile	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv
VOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1		
BOSS_ESM_v1_Profile	SNMPv1	public_v1	pr			
BOSS_4800_v1_Profile	SNMPv1	public_v1	pr			
BOSS_v1_Profile	SNMPv1	public_v1	pr			
VOSS_v2_Profile	SNMPv2	public_v2	pr			

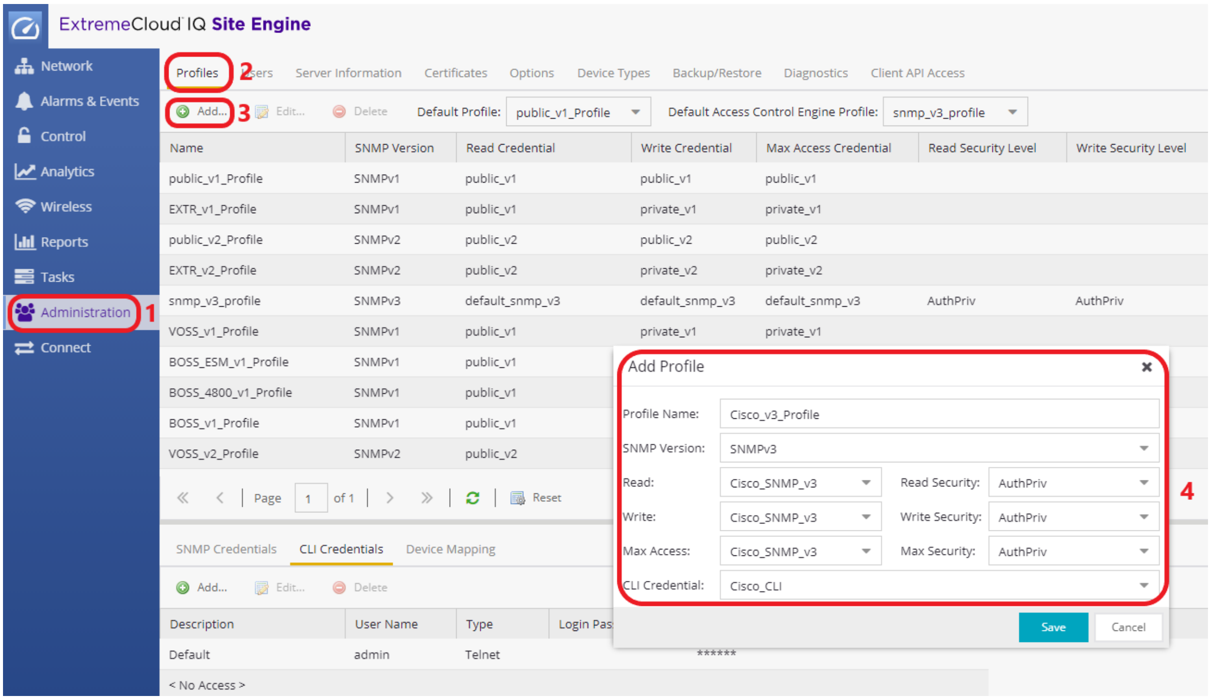
Description	User Name	Type	Login Password
Default	admin	Telnet	******

Add CLI Credential

Description:	Cisco_CLI
User Name:	admin
Type:	Telnet
Login Password:	
Enable Password:	••••••
Configuration Password:	

Figure 2 – How to configure CLI credentials for a Cisco switch in ExtremeCloud IQ - Site Engine

When both SNMP and CLI credentials have been set up, add a new Device Profile and bind the credentials to the profile as shown in Figure 3.



Default Profile: public_v1_Profile

Default Access Control Engine Profile: snmp_v3_profile

Name	SNMP Version	Read Credential	Write Credential	Max Access Credential	Read Security Level	Write Security Level
public_v1_Profile	SNMPv1	public_v1	public_v1	public_v1		
EXTR_v1_Profile	SNMPv1	public_v1	private_v1	private_v1		
public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2		
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2		
snmp_v3_profile	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv
VOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1		
BOSS_ESM_v1_Profile	SNMPv1	public_v1				
BOSS_4800_v1_Profile	SNMPv1	public_v1				
BOSS_v1_Profile	SNMPv1	public_v1				
VOSS_v2_Profile	SNMPv2	public_v2				

Description	User Name	Type	Login Pas
Default	admin	Telnet	******
< No Access >			

Add Profile

Profile Name:	Cisco_v3_Profile		
SNMP Version:	SNMPv3		
Read:	Cisco_SNMP_v3	Read Security:	AuthPriv
Write:	Cisco_SNMP_v3	Write Security:	AuthPriv
Max Access:	Cisco_SNMP_v3	Max Security:	AuthPriv
CLI Credential:	Cisco_CLI		

Figure 3 – How to create a Device Profile for a Cisco switch in ExtremeCloud IQ - Site Engine

After the Device Profile is set up, navigate to the **Network** menu from the left pane of ExtremeCloud IQ - Site Engine and select the **Devices** tab. Select the relevant Site for the Cisco switch to be added in and then right click on that Site and select "**Add Devices**".

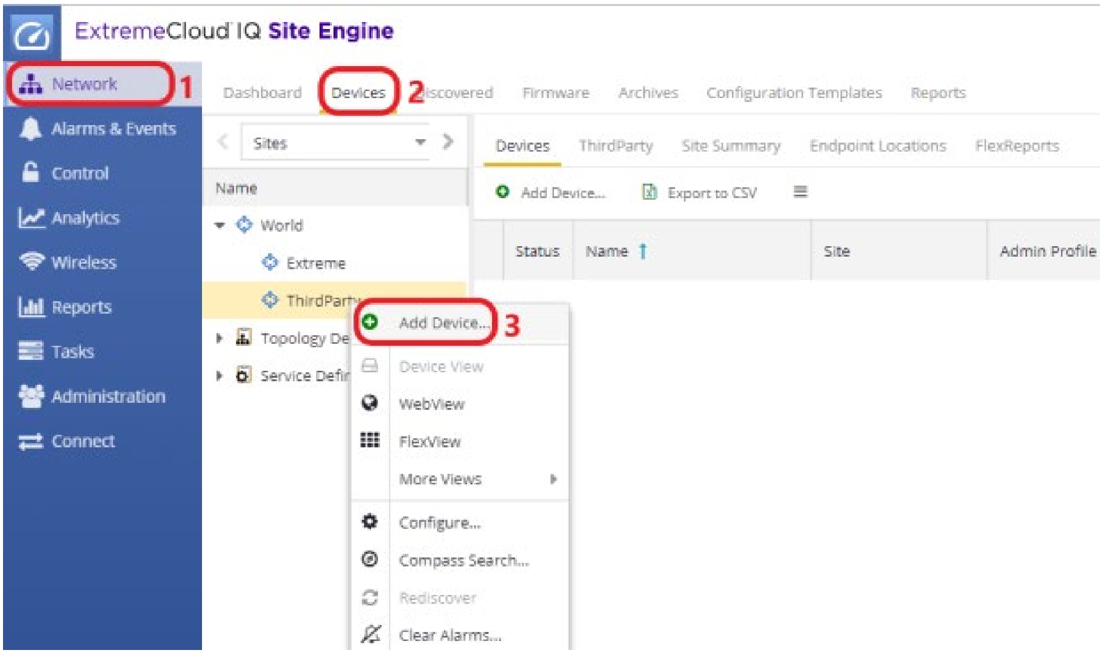
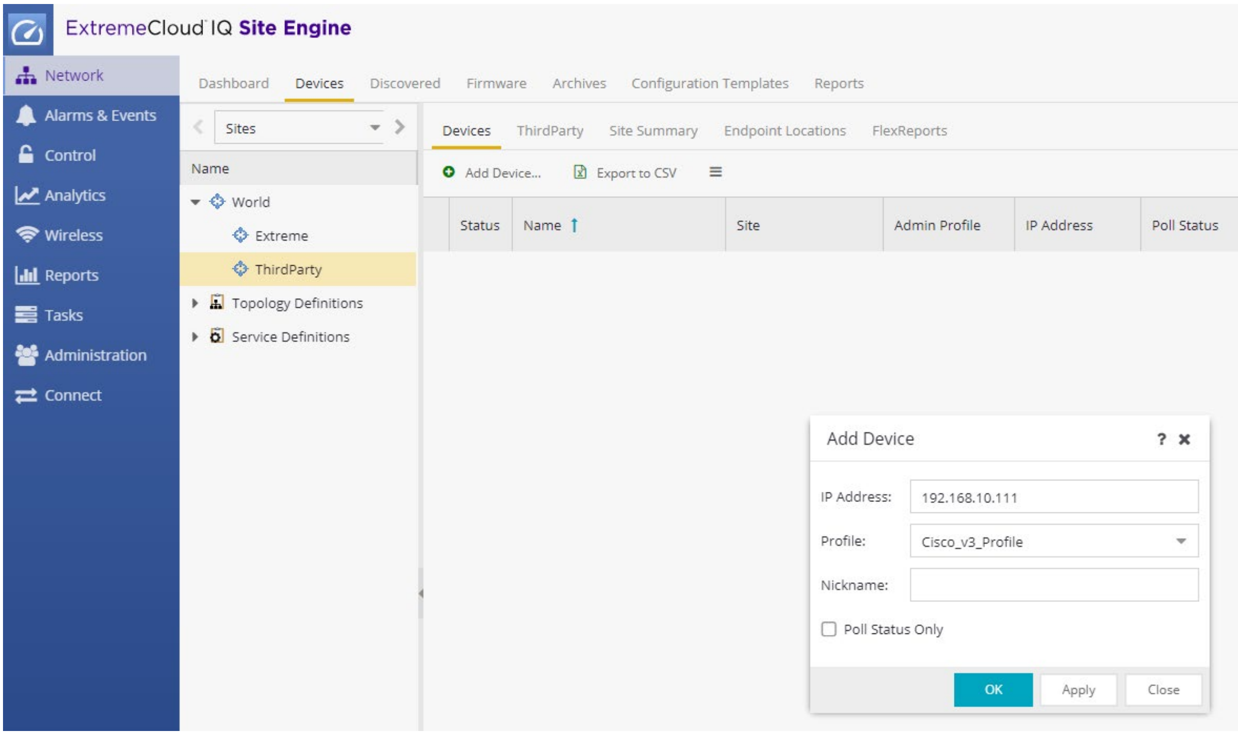


Figure 4 – How to manually onboard a Cisco switch in ExtremeCloud IQ - Site Engine - 1



IP Address: 192.168.10.111

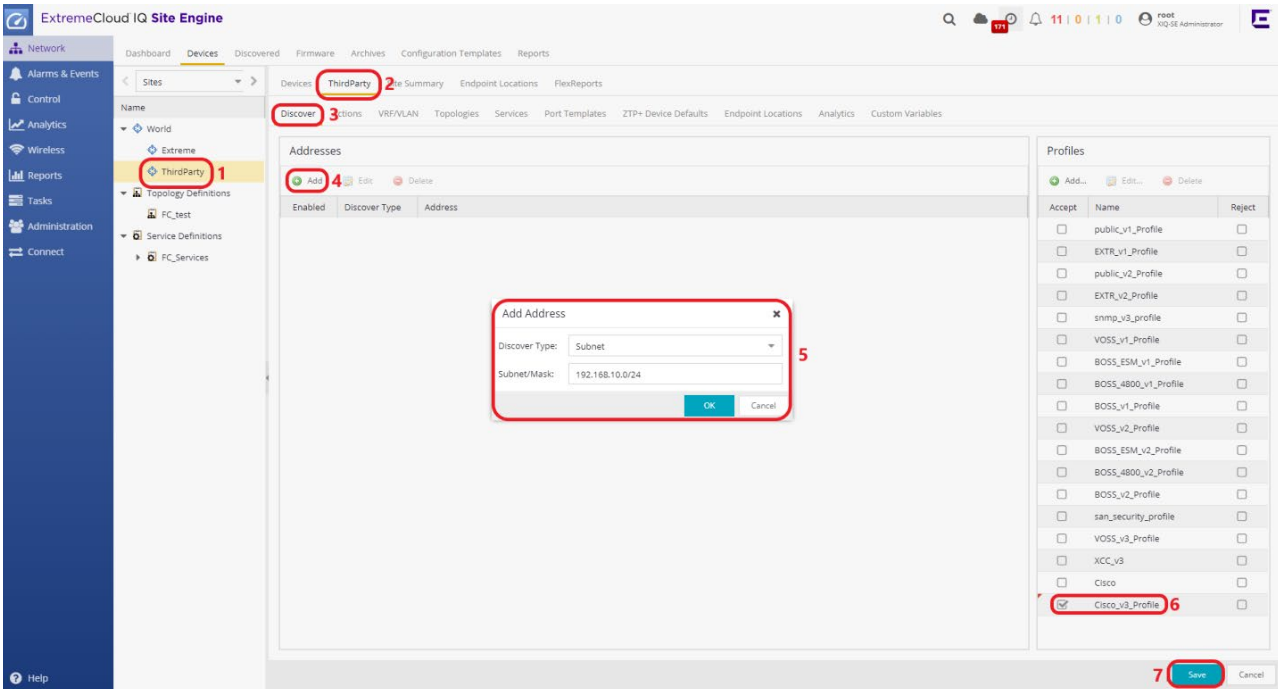
Profile: Cisco_v3_Profile

Nickname:

☐ Poll Status Only

Figure 5 – How to manually onboard a Cisco switch in ExtremeCloud IQ - Site Engine - 2

Alternatively, if multiple switches need to be onboarded, a more convenient method is to use the “Discover” operation under the Site as illustrated in Figure 6. The discover type can be a subnet, a seed address, or an address range.



Add Address

Discover Type: Subnet

Subnet/Mask: 192.168.10.0/24

OK Cancel

Accept	Name	Reject
☐	public_v1_Profile	☐
☐	EXTR_v1_Profile	☐
☐	public_v2_Profile	☐
☐	EXTR_v2_Profile	☐
☐	snmp_v3_profile	☐
☐	VOSS_v1_Profile	☐
☐	BOSS_ESM_v1_Profile	☐
☐	BOSS_4800_v1_Profile	☐
☐	BOSS_v1_Profile	☐
☐	VOSS_v2_Profile	☐
☐	BOSS_ESM_v2_Profile	☐
☐	BOSS_4800_v2_Profile	☐
☐	BOSS_v2_Profile	☐
☐	san_security_profile	☐
☐	VOSS_v3_Profile	☐
☐	XCC_v3	☐
☐	Cisco	☐
☑	Cisco_v3_Profile	☐

Figure 6 – How to discover multiple switches in ExtremeCloud IQ - Site Engine

ExtremeControl Configuration using Dynamic ACLs

Overview

This section covers the configuration of ExtremeControl to use the Cisco switch as an edge enforcement point using the Dynamic ACL method together with Guest Registration. Skip this section if Downloadable ACL (Per-User ACL) method is preferred.

Step 1: Add the Cisco Switch to Access Control

Because the Cisco switch was already onboarded to ExtremeCloud IQ - Site Engine in the previous section, the next step is to add the switch to the Access Control and configure Access Control with appropriate RADIUS attributes.

Open ExtremeCloud IQ - Site Engine and navigate to the **Control** section and then select the **Access Control** tab. Next, select the **Switches** sub-tab and the **Add** button to add the Cisco switch as shown in Figure 7 and Figure 8.

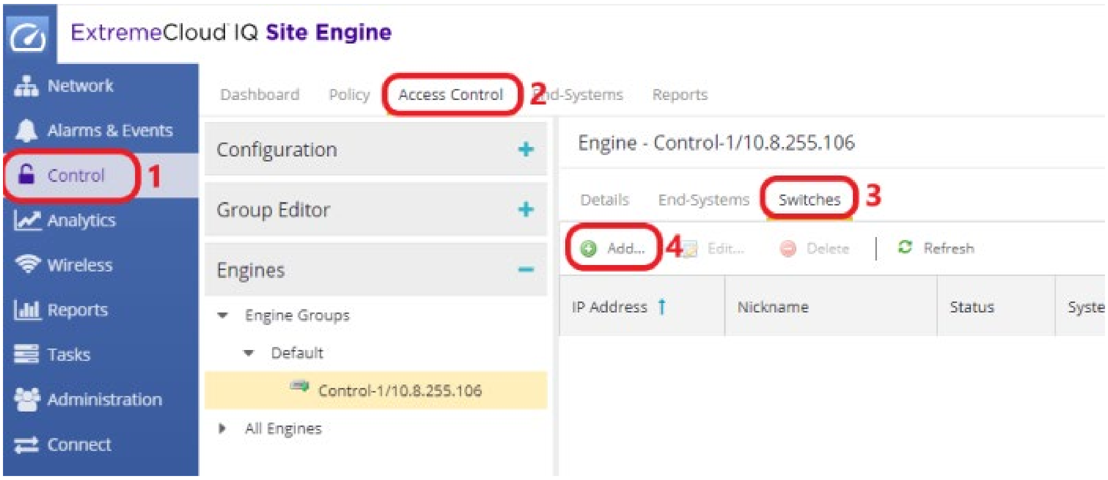
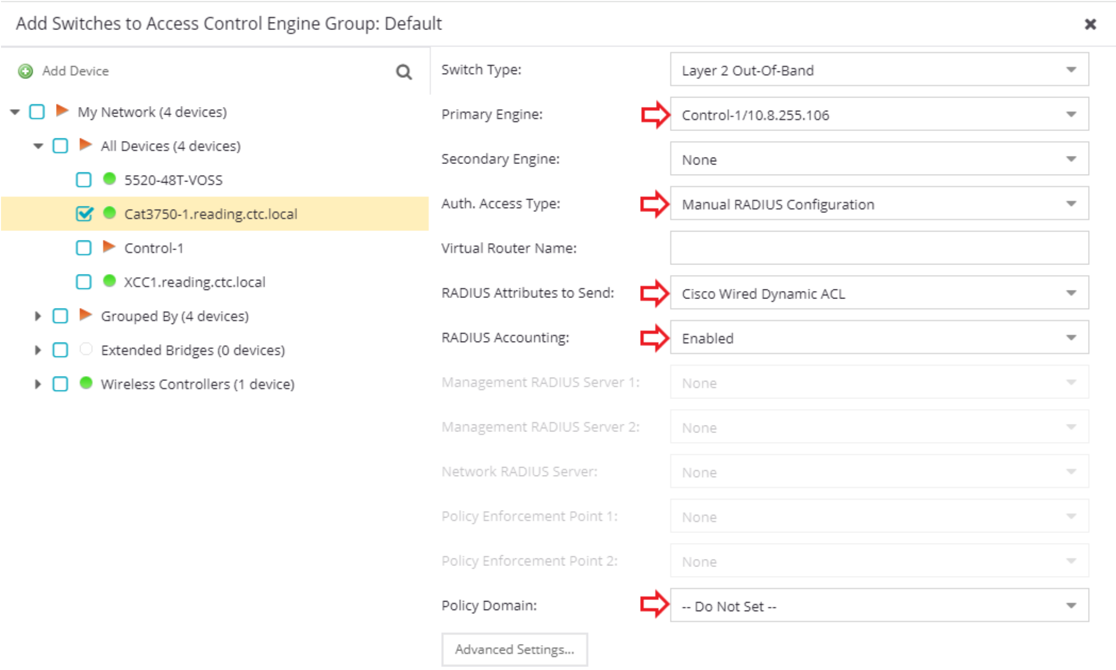


Figure 7 – How to add a Cisco switch to Access Control – 1

Because the Cisco device is already in the ExtremeCloud IQ - Site Engine database, expand the “My Network” pane, find the Cisco switch, and select the checkbox. By default, some settings are determined based on the type of device that is added. However, a few settings need to be set manually. These settings are:

Primary Engine: Primary Access Control Engine to be used
RADIUS Attributes to Send: Cisco Wired Dynamic ACL
RADIUS Accounting: Enabled
Policy Domain: Do Not Set



Add Switches to Access Control Engine Group: Default

Add Device

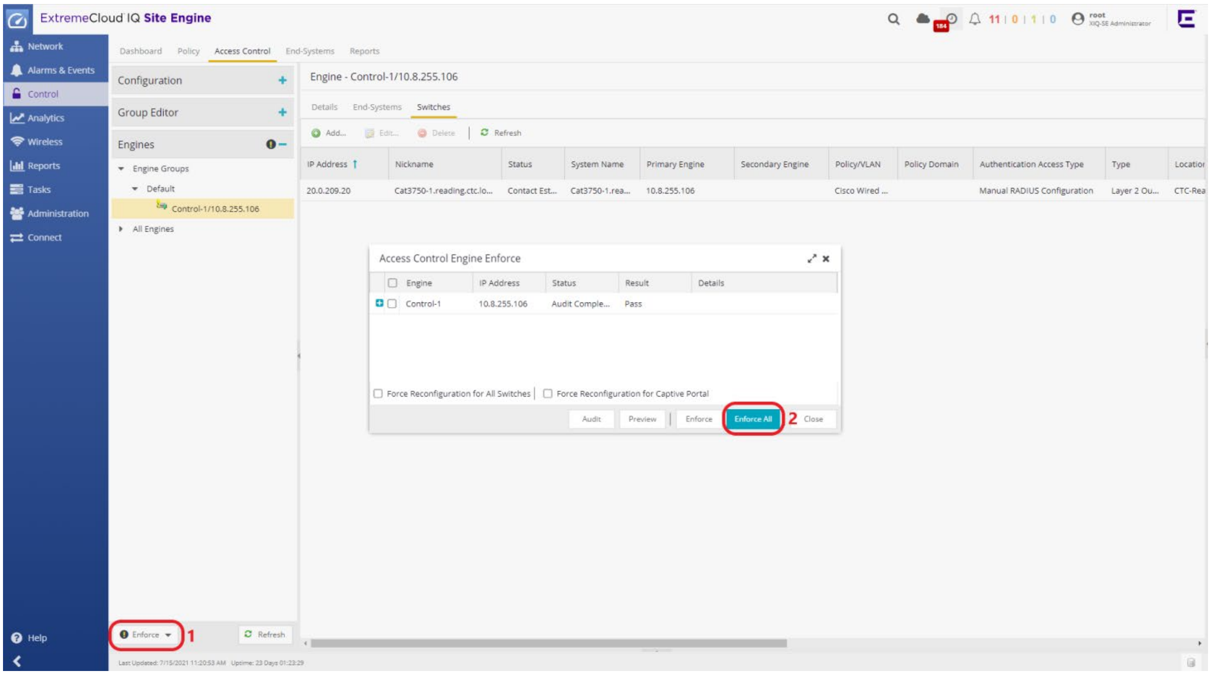
- □ My Network (4 devices)
  - □ All Devices (4 devices)
    - □ 5520-48T-VOSS
    - ☑ Cat3750-1.reading.ctc.local
    - □ Control-1
    - □ XCC1.reading.ctc.local
  - □ Grouped By (4 devices)
  - □ Extended Bridges (0 devices)
  - □ Wireless Controllers (1 device)

Switch Type:	Layer 2 Out-Of-Band
Primary Engine:	Control-1/10.8.255.106
Secondary Engine:	None
Auth. Access Type:	Manual RADIUS Configuration
Virtual Router Name:	
RADIUS Attributes to Send:	Cisco Wired Dynamic ACL
RADIUS Accounting:	Enabled
Management RADIUS Server 1:	None
Management RADIUS Server 2:	None
Network RADIUS Server:	None
Policy Enforcement Point 1:	None
Policy Enforcement Point 2:	None
Policy Domain:	-- Do Not Set --

Advanced Settings...

Figure 8 – How to add a Cisco switch to Access Control – 2

When the switch is added, **Enforce** the configurations.



Engine - Control-1/10.8.255.106

IP Address	Nickname	Status	System Name	Primary Engine	Secondary Engine	Policy/VLAN	Policy Domain	Authentication Access Type	Type	Locatio
20.0.209.20	Cat3750-1.reading.ctc.lo...	Contact Est...	Cat3750-1.rea...	10.8.255.106		Cisco Wired ...		Manual RADIUS Configuration	Layer 2 Ou...	CTC-Rea

Access Control Engine Enforce

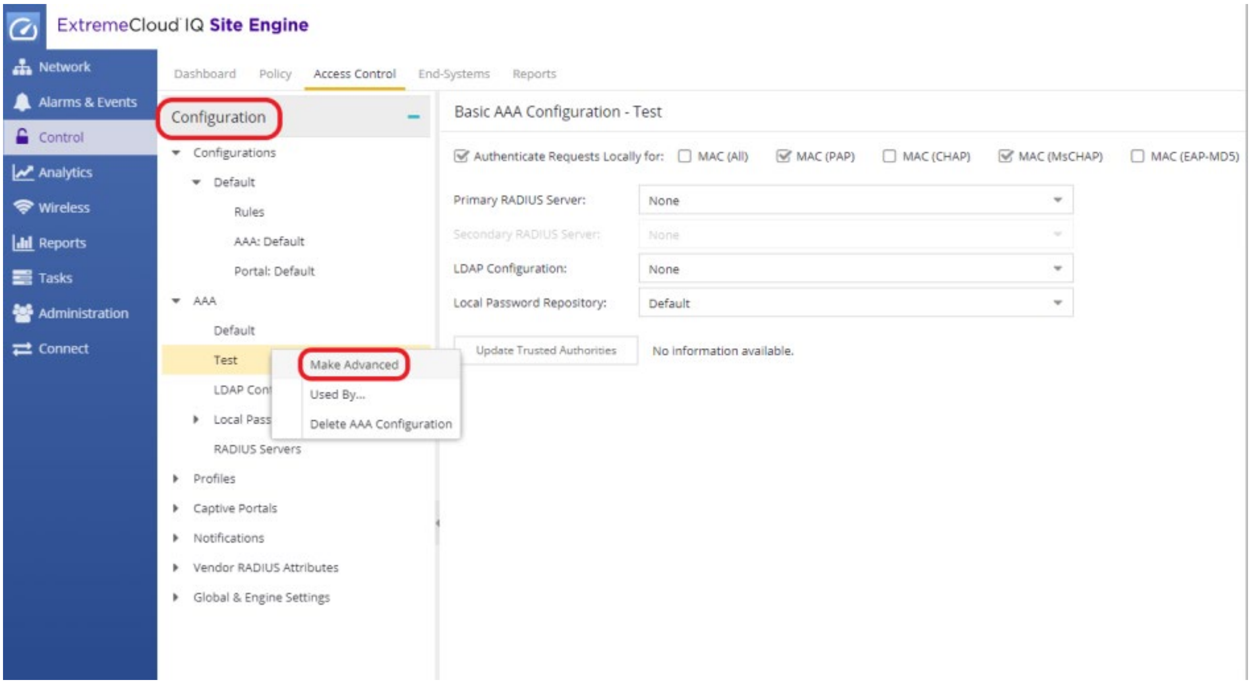
Engine	IP Address	Status	Result	Details
Control-1	10.8.255.106	Audit Comple...	Pass	

☐ Force Reconfiguration for All Switches ☐ Force Reconfiguration for Captive Portal

Last Updated: 7/15/2021 11:20:53 AM Uptime: 23 Days 01:23:29

Step 2: Configure AAA with Local Authentication Method

To ensure the switch receives a RADIUS Reject message when testing availability of the Access Control Engine, the AAA configuration needs to be adjusted. Select the **Configuration** section, expand **AAA** in the Configuration tree, and right-click the **Default** AAA configuration. Select **Make Advanced**.



Basic AAA Configuration - Test

☑ Authenticate Requests Locally for: ☐ MAC (All) ☑ MAC (PAP) ☐ MAC (CHAP) ☑ MAC (MsCHAP) ☐ MAC (EAP-MD5)

Primary RADIUS Server: None

Secondary RADIUS Server: None

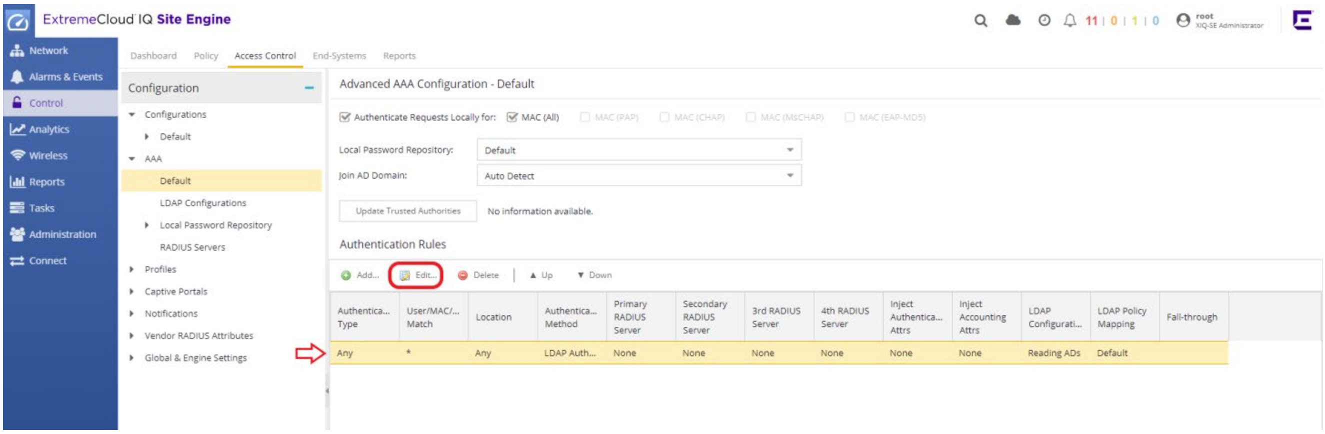
LDAP Configuration: None

Local Password Repository: Default

No information available.

Figure 10 – AAA Configuration - 1

Select the “**Any**” Authentication Rule and then the **Edit** button.



Advanced AAA Configuration - Default

☑ Authenticate Requests Locally for: ☑ MAC (All) □ MAC (PAP) □ MAC (CHAP) □ MAC (MsCHAP) □ MAC (EAP-MD5)

Local Password Repository: Default

Join AD Domain: Auto Detect

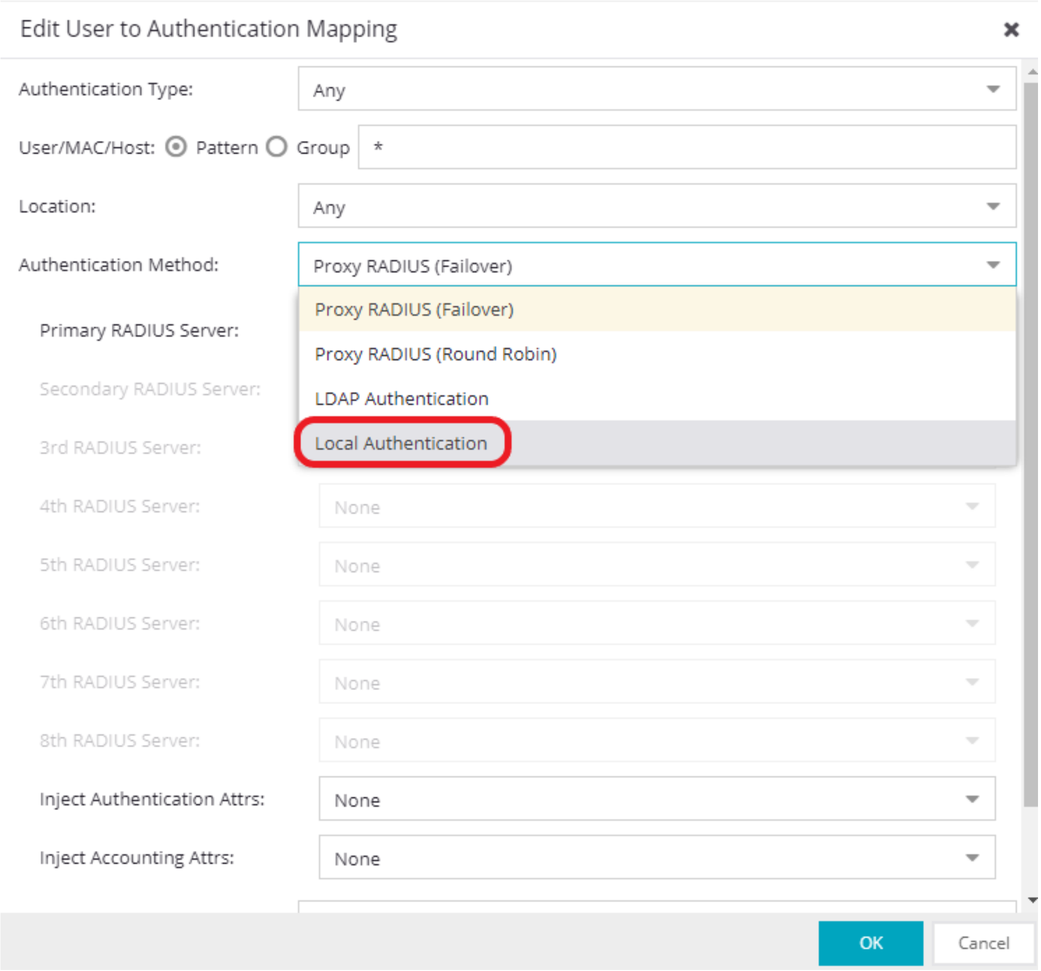
No information available.

Authentication Rules

Authentica... Type	User/MAC/... Match	Location	Authentica... Method	Primary RADIUS Server	Secondary RADIUS Server	3rd RADIUS Server	4th RADIUS Server	Inject Authentica... Attrs	Inject Accounting Attrs	LDAP Configurati...	LDAP Policy Mapping	Fall-through
Any	*	Any	LDAP Auth...	None	None	None	None	None	None	Reading ADs	Default	

Figure 11 – AAA Configuration - 2

In this section, Local Authentication will be used. LDAP or Proxy RADIUS Authentication can also be selected. In the “**Edit User to Authentication Mapping**” window, change the **Authentication Method** to **Local Authentication** and then select the **OK** button.



Authentication Type: Any

User/MAC/Host: ● Pattern ○ Group *

Location: Any

Authentication Method: Proxy RADIUS (Failover)

Primary RADIUS Server:

Secondary RADIUS Server:

3rd RADIUS Server:

4th RADIUS Server: None

5th RADIUS Server: None

6th RADIUS Server: None

7th RADIUS Server: None

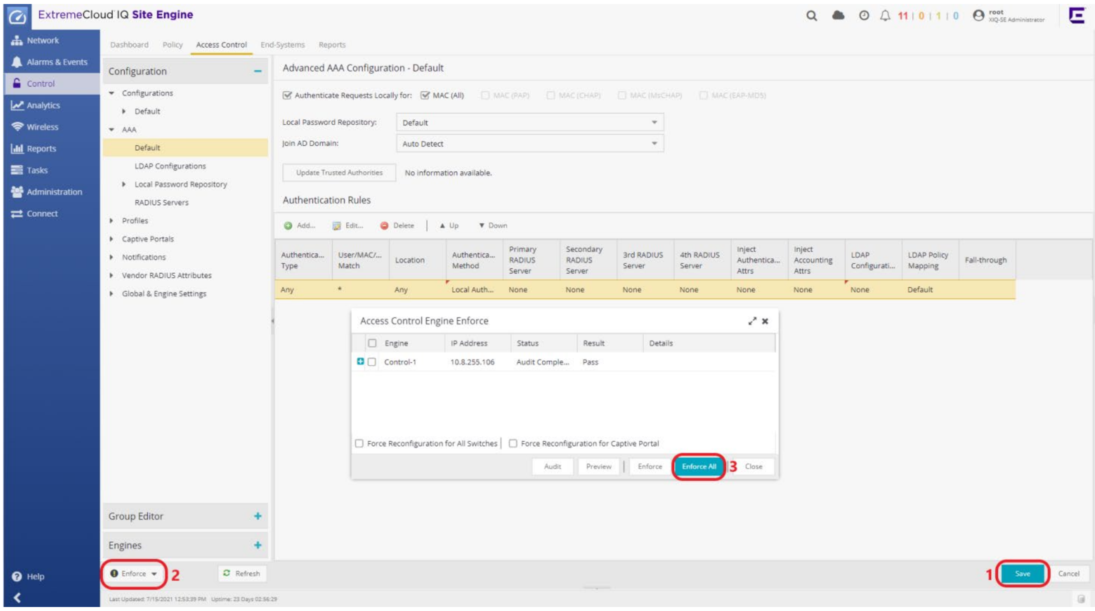
8th RADIUS Server: None

Inject Authentication Attrs: None

Inject Accounting Attrs: None

Figure 12 – AAA Configuration – Local Authentication Setting

Save the Configuration and **Enforce** again as shown in Figure 13.



Advanced AAA Configuration - Default

☑ Authenticate Requests Locally for: ☑ MAC (All) ☐ MAC (PAP) ☐ MAC (CHAP) ☐ MAC (MsCHAP) ☐ MAC (EAP-MD5)

Local Password Repository: Default

Join AD Domain: Auto Detect

Update Trusted Authorities No information available.

Authentication Rules

Authentica... Type	User/MAC/... Match	Location	Authentica... Method	Primary RADIUS Server	Secondary RADIUS Server	3rd RADIUS Server	4th RADIUS Server	Inject Authentica... Attrs	Inject Accounting Attrs	LDAP Configurati...	LDAP Policy Mapping	Fall-through
Any	*	Any	Local Auth...	None	None	None	None	None	None	None	Default	

Access Control Engine Enforce

☐ Engine	IP Address	Status	Result	Details
☐ Control-1	10.8.255.106	Audit Comple...	Pass	

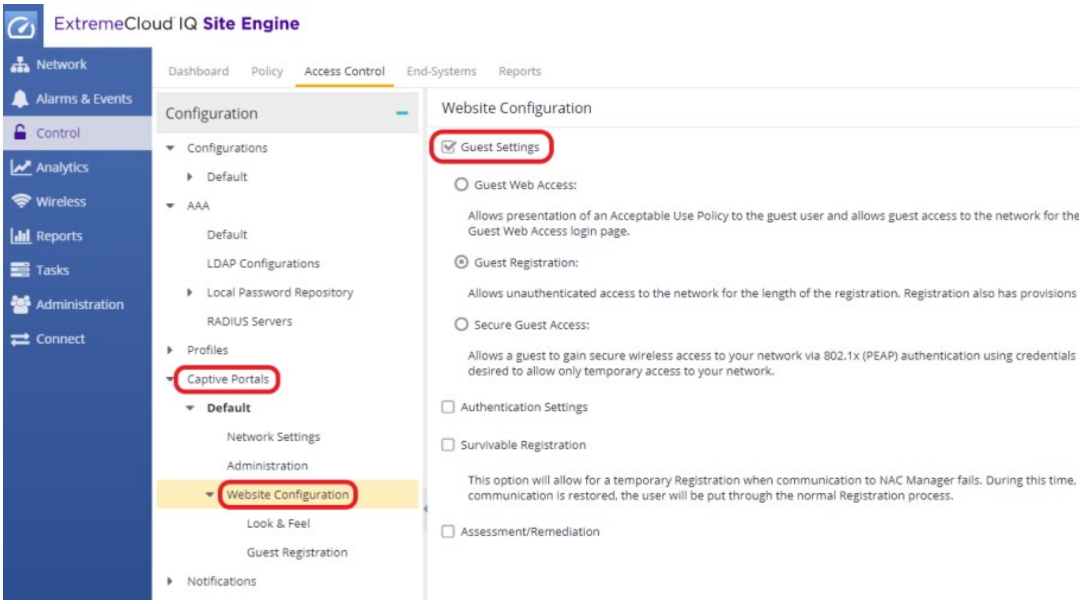
☐ Force Reconfiguration for All Switches | ☐ Force Reconfiguration for Captive Portal

Last Updated: 7/15/2021 12:53:39 PM Uptime: 23 Days 02:56:29

Figure 13 – How to enforce the configuration in ExtremeControl

Step 3: Configure the Rules and ACLs to Assign

After the switch is added to Access Control, the rules need to be adjusted to return the correct RADIUS VSAs for the Cisco switch. Assuming that Guest Registration is already configured on the system, a default set of rules already exists. If Guest Registration is not enabled, it can be enabled by expanding **Captive Portals** and the **Default** configuration. Select **Website Configuration** and select the checkbox for **Guest Registration**. Then be sure to **Save** and **Enforce** the configuration.



Website Configuration

☑ Guest Settings

○ Guest Web Access:

Allows presentation of an Acceptable Use Policy to the guest user and allows guest access to the network for the Guest Web Access login page.

● Guest Registration:

Allows unauthenticated access to the network for the length of the registration. Registration also has provisions

○ Secure Guest Access:

Allows a guest to gain secure wireless access to your network via 802.1x (PEAP) authentication using credentials desired to allow only temporary access to your network.

☐ Authentication Settings

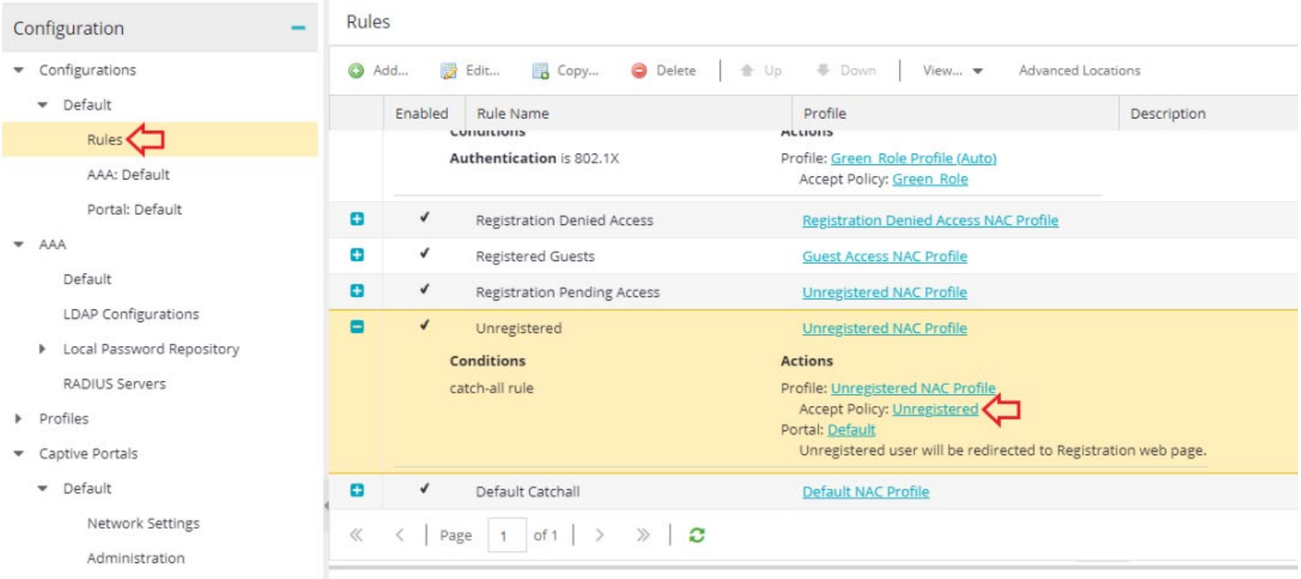
☐ Survivable Registration

This option will allow for a temporary Registration when communication to NAC Manager fails. During this time, communication is restored, the user will be put through the normal Registration process.

☐ Assessment/Remediation

Figure 14 – How to enable Guest Registration from ExtremeControl

Expand the **Default** configuration menu under **Configurations** to access the Rules engine. Scroll to the bottom where the **Unregistered** rule exists. Note that this is the "**catch-all rule**" when registration is enabled. Select the Accept Policy of **Unregistered**.



Configuration

- Configurations
  - Default
    - Rules
    - AAA: Default
    - Portal: Default
- AAA
  - Default
  - LDAP Configurations
  - Local Password Repository
  - RADIUS Servers
- Profiles
- Captive Portals
  - Default
    - Network Settings
    - Administration

Rules

	Enabled	Rule Name	Profile	Description
		Conditions **Authentication** is 802.1X	Actions Profile: Green_Role Profile (Auto) Accept Policy: Green_Role	
⊞	✓	Registration Denied Access	Registration Denied Access NAC Profile	
⊞	✓	Registered Guests	Guest Access NAC Profile	
⊞	✓	Registration Pending Access	Unregistered NAC Profile	
⊟	✓	Unregistered	Unregistered NAC Profile	
		Conditions catch-all rule	**Actions** Profile: Unregistered NAC Profile Accept Policy: Unregistered Portal: Default Unregistered user will be redirected to Registration web page.	
⊞	✓	Default Catchall	Default NAC Profile	

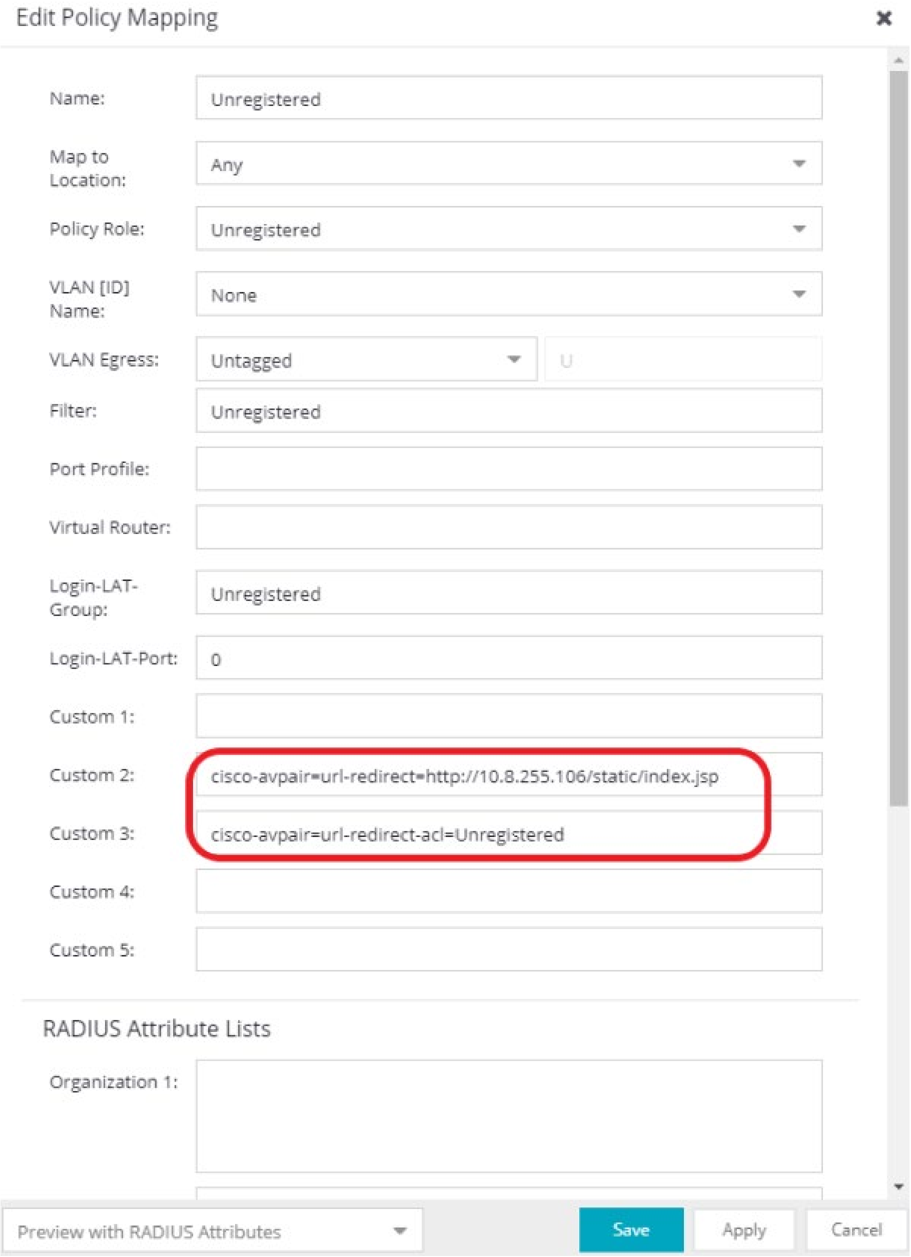
Figure 15 – Selecting the Accept Policy "Unregistered" in ExtremeControl

In the resulting **Edit Policy Mapping** window, the RADIUS VSAs need to be specified. The Custom 2, Custom 3, and Custom 4 fields are used for all VSAs being sent back to the switch. For a role that is using Web redirect, Custom 2 and Custom 3 need to be filled in with the following values:

Custom 2: cisco-avpair=url-redirect=http://<EAC Engine IP>/static/index.jsp

Custom 3: cisco-avpair=url-redirect-acl=Unregistered

The **Custom 2** field specifies the URL to redirect the web traffic to. This can also be HTTPS if it is enabled. The **Custom 3** column defines which ACL to use with the redirection. Based on the previous configuration, this is the Unregistered ACL. See Figure 16.



Edit Policy Mapping

Name:	Unregistered
Map to Location:	Any
Policy Role:	Unregistered
VLAN [ID] Name:	None
VLAN Egress:	Untagged
Filter:	Unregistered
Port Profile:	
Virtual Router:	
Login-LAT-Group:	Unregistered
Login-LAT-Port:	0
Custom 1:	
Custom 2:	cisco-avpair=url-redirect=http://10.8.255.106/static/index.jsp
Custom 3:	cisco-avpair=url-redirect-acl=Unregistered
Custom 4:	
Custom 5:	

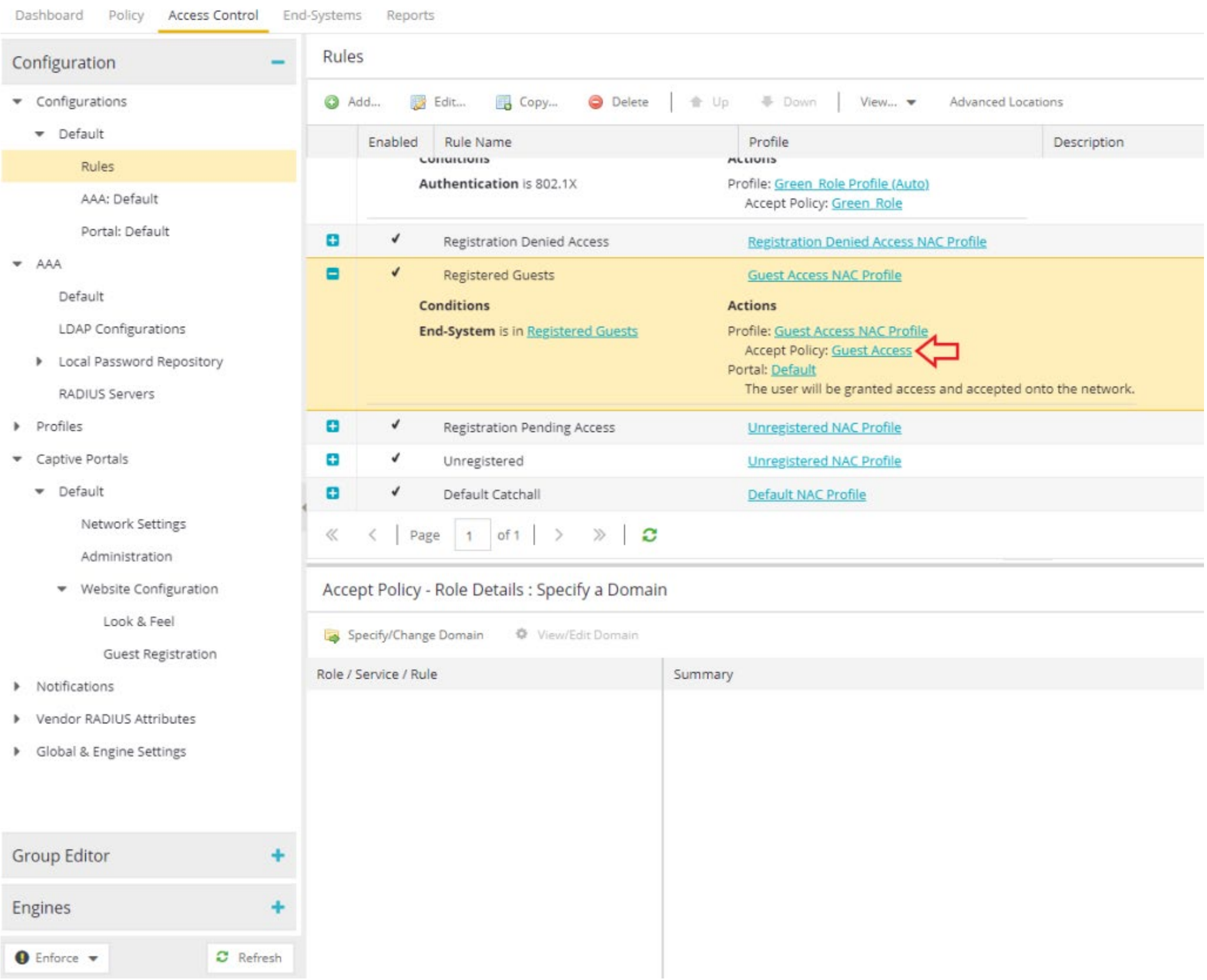
RADIUS Attribute Lists

Organization 1:

Figure 16 – How to modify the "Unregistered" Policy Mapping for Cisco VSAs

NOTES
If the Custom fields are not displayed, ensure the switch was added to Access Control with the correct **RADIUS Attributes to Send**. The Custom 4 field is not used when Web redirect is being performed. This is because it is configured to pass back a Filter-ID which the Cisco switch does not need when using Web redirect.

Next, select the **Guest Access** Accept Policy and set the ACL to be utilized when Guest Registration is complete.



Enabled	Rule Name	Profile	Description
✓	Registration Denied Access	Registration Denied Access NAC Profile	
✓	Registered Guests	Guest Access NAC Profile	
✓	Registration Pending Access	Unregistered NAC Profile	
✓	Unregistered	Unregistered NAC Profile	
✓	Default Catchall	Default NAC Profile	

Conditions
Authentication is 802.1X

Actions
Profile: Green_Role Profile (Auto)
Accept Policy: Green_Role

Conditions
End-System is in Registered Guests

Actions
Profile: Guest Access NAC Profile
Accept Policy: Guest Access
Portal: Default
The user will be granted access and accepted onto the network.

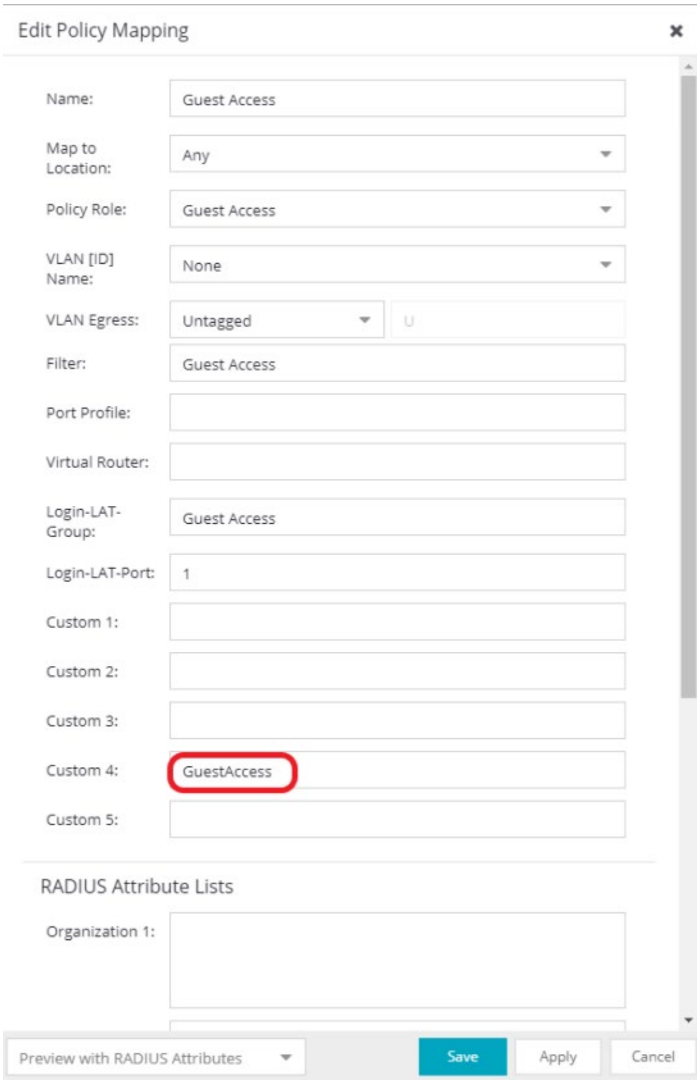
Accept Policy - Role Details : Specify a Domain

Role / Service / Rule	Summary

Figure 17 – Selecting Accept Policy “Guest Access” in ExtremeControl

In the **Edit Policy Mapping** window, the field that needs to be edited is the **Custom 4** field. This is because web redirection is not going to be used for Guest Access. Instead, just an ACL name will be returned. Therefore, in this field enter only the name of the ACL (for example, GuestAccess). Combined with the RADIUS settings selected for the switch, the return attribute for the switch will be formatted as "**Filter-Id=%CUSTOM4%.in**". For example, if GuestAccess is the ACL being returned, the attribute that can be seen on the wire is "**Filter-Id=GuestAccess.in**".

Caution
Note that spaces are not supported on Cisco ACL names. Therefore the name of the ACL configured must not contain spaces.



Edit Policy Mapping

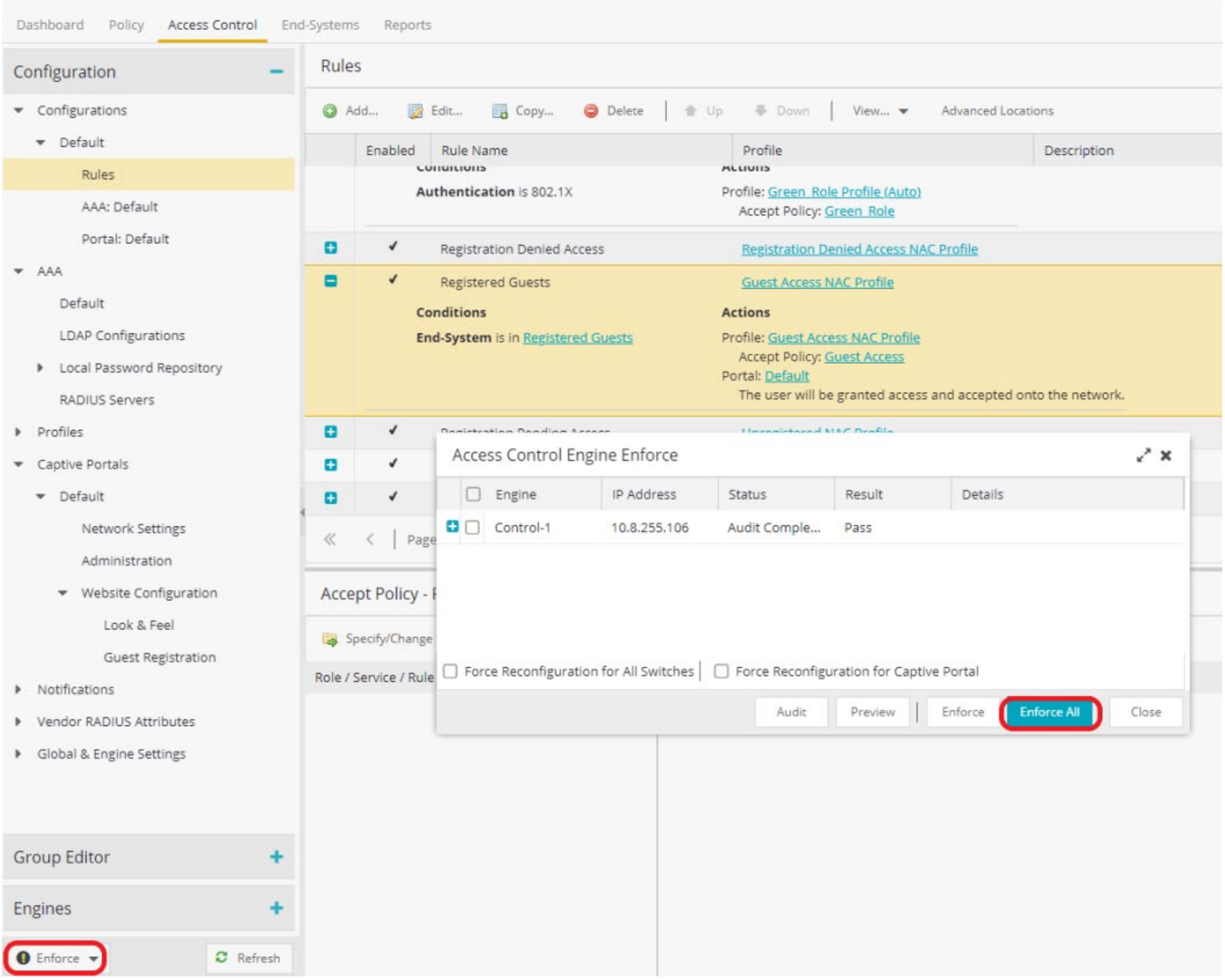
Name: Guest Access
Map to Location: Any
Policy Role: Guest Access
VLAN [ID] Name: None
VLAN Egress: Untagged
Filter: Guest Access
Port Profile:
Virtual Router:
Login-LAT-Group: Guest Access
Login-LAT-Port: 1
Custom 1:
Custom 2:
Custom 3:
Custom 4: GuestAccess
Custom 5:

RADIUS Attribute Lists

Organization 1:

Figure 18 – How to modify "GuestAccess" Policy Mapping to return "Filter-ID" attribute

Repeat this process for any additional ACLs (roles) that need to be assigned through the Rules Engine. Some additional ACL examples include an Administrator, EnterpriseUser, and Quarantine (commonly used with the Web redirect function). After these settings are configured, **Enforce** the configuration to the Access Control Engine.



Enabled	Rule Name	Profile	Description
	Conditions **Authentication** is 802.1X	**Actions** Profile: Green_Role Profile (Auto) Accept Policy: Green_Role	
✓	Registration Denied Access	Registration Denied Access NAC Profile	
✓	Registered Guests	Guest Access NAC Profile	
	Conditions **End-System** is in Registered Guests	**Actions** Profile: Guest Access NAC Profile Accept Policy: Guest Access Portal: Default The user will be granted access and accepted onto the network.	
✓	Registration Pending Access	Unregistered NAC Profile	
✓			
✓			

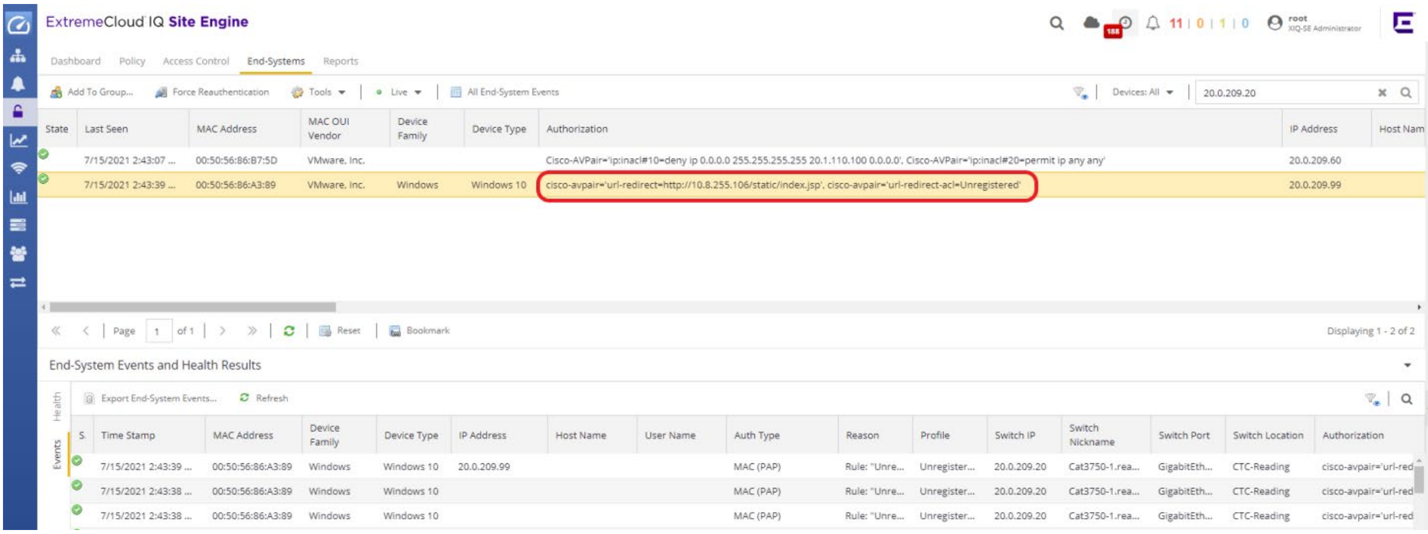
□ Engine	IP Address	Status	Result	Details
□ Control-1	10.8.255.106	Audit Comple...	Pass	

Figure 19 – Enforcing the settings in ExtremeControl

Step 4: Verify - Client Testing

Connect a wired client to the Cisco switch port where authentication is configured according to the steps explained in the previous “Authentication Configuration” section.

When a new user without an IEEE 802.1X supplicant configured on the end-system connects to the Cisco switch port with both MAB and 802.1X authentication configured, the “Unregistered” Rule will be applied and the “Unregistered” Policy which has the Custom 2 and Custom 3 attributes (see Figure 16) configured for Web Redirection will be sent to Cisco switch. The operation can be validated by checking the End System table as shown in Figure 20.



20.0.209.20

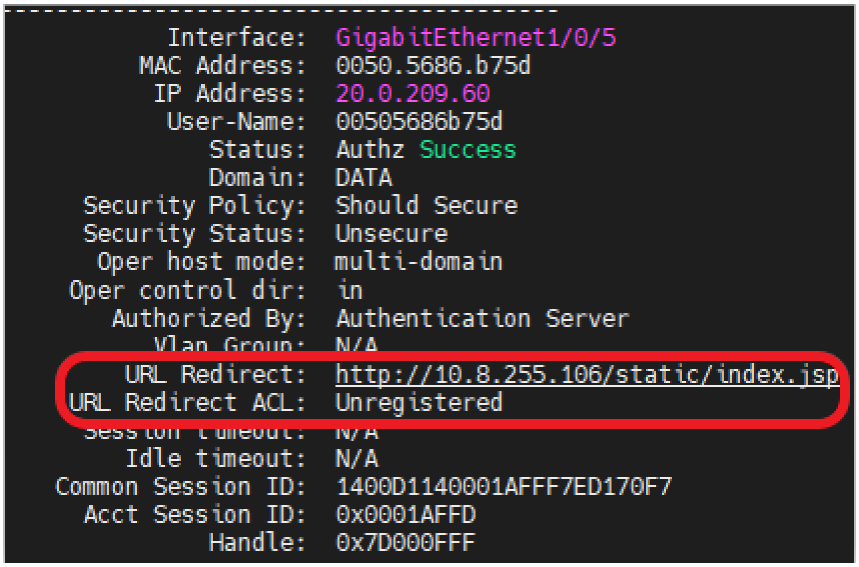
State	Last Seen	MAC Address	MAC OUI Vendor	Device Family	Device Type	Authorization	IP Address	Host Nam
✓	7/15/2021 2:43:07 ...	00:50:56:86:B7:5D	VMware, Inc.			Cisco-AVPair='ip:inacl#10=deny ip 0.0.0.0 255.255.255.255 20.1.110.100 0.0.0.0', Cisco-AVPair='ip:inacl#20=permit ip any any'	20.0.209.60	
✓	7/15/2021 2:43:39 ...	00:50:56:86:A3:89	VMware, Inc.	Windows	Windows 10	cisco-avpair='url-redirect=http://10.8.255.106/static/index.jsp', cisco-avpair='url-redirect-acl=Unregistered'	20.0.209.99	

End-System Events and Health Results

S.	Time Stamp	MAC Address	Device Family	Device Type	IP Address	Host Name	User Name	Auth Type	Reason	Profile	Switch IP	Switch Nickname	Switch Port	Switch Location	Authorization
✓	7/15/2021 2:43:39 ...	00:50:56:86:A3:89	Windows	Windows 10	20.0.209.99			MAC (PAP)	Rule: "Unre...	Unregister...	20.0.209.20	Cat3750-1.rea...	GigabitEth...	CTC-Reading	cisco-avpair='url-red
✓	7/15/2021 2:43:38 ...	00:50:56:86:A3:89	Windows	Windows 10				MAC (PAP)	Rule: "Unre...	Unregister...	20.0.209.20	Cat3750-1.rea...	GigabitEth...	CTC-Reading	cisco-avpair='url-red
✓	7/15/2021 2:43:38 ...	00:50:56:86:A3:89	Windows	Windows 10				MAC (PAP)	Rule: "Unre...	Unregister...	20.0.209.20	Cat3750-1.rea...	GigabitEth...	CTC-Reading	cisco-avpair='url-red

Figure 20 – ExtremeControl End-Systems Table showing Web redirect VSAs

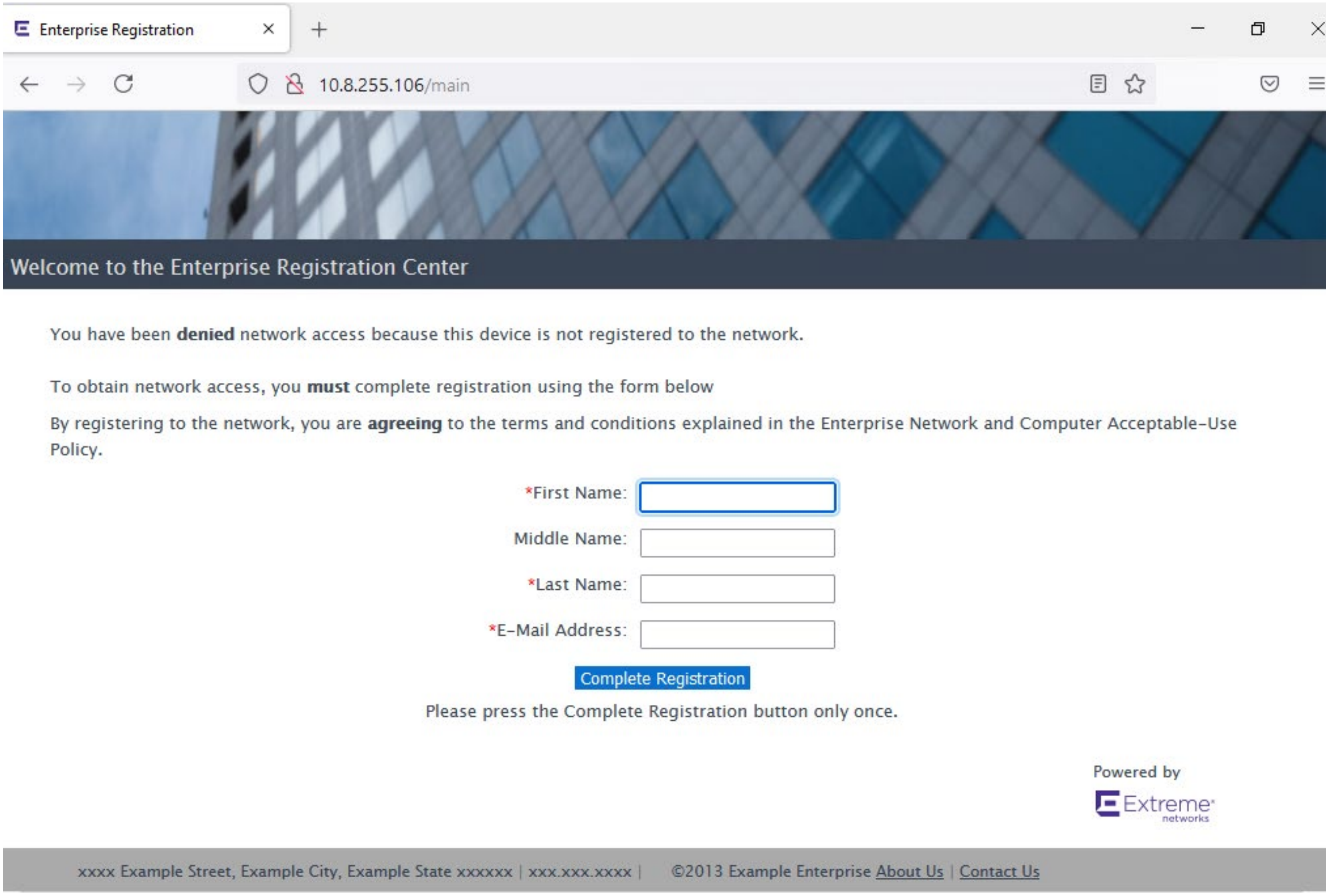
Another validation can be performed on the switch, by checking the *‘show authentication sessions interface <interface id>’* CLI command output as in Figure 21.



```
----------------------------------------
            Interface:  GigabitEthernet1/0/5
          MAC Address:  0050.5686.b75d
           IP Address:  20.0.209.60
            User-Name:  00505686b75d
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  in
        Authorized By:  Authentication Server
           Vlan Group:  N/A
         URL Redirect:  http://10.8.255.106/static/index.jsp
     URL Redirect ACL:  Unregistered
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  1400D1140001AFFF7ED170F7
      Acct Session ID:  0x0001AFFD
               Handle:  0x7D000FFF
```

Figure 21 – Validating Cisco Web Redirect VSAs from the Cisco CLI

After the Cisco switch receives the URL Redirect from ExtremeControl as a result of RADIUS Access-Accept, the end-system will be redirected to the IP address of the Access Control Engine whenever an HTTP/HTTPS request is made, and the Guest Registration page will welcome the user as seen in Figure 22.



Welcome to the Enterprise Registration Center

You have been **denied** network access because this device is not registered to the network.

To obtain network access, you **must** complete registration using the form below

By registering to the network, you are **agreeing** to the terms and conditions explained in the Enterprise Network and Computer Acceptable-Use Policy.

*First Name:

Middle Name:

*Last Name:

*E-Mail Address:

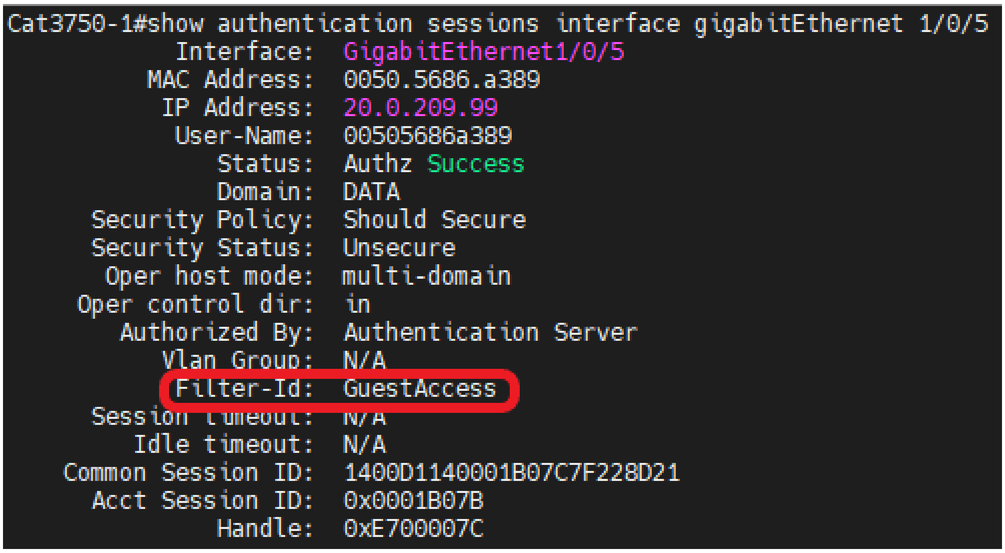
Please press the Complete Registration button only once.

Powered by

xxxx Example Street, Example City, Example State xxxxxx | xxx.xxx.xxxx | ©2013 Example Enterprise About Us | Contact Us

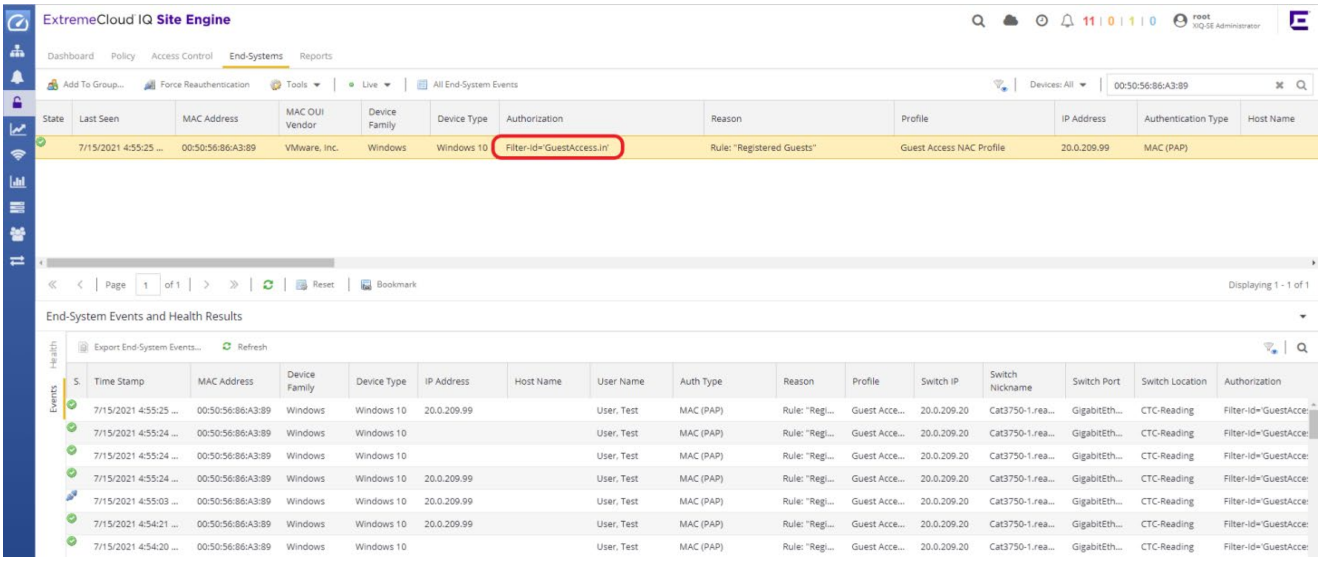
Figure 22 – Extreme Control - Guest Registration Default Landing Page

After the registration form is filled out and submitted by selecting “Complete Registration”, one can validate whether the correct Filter-ID is sent, and the ACL named “GuestAccess” is applied to the end-system.



```
Cat3750-1#show authentication sessions interface gigabitEthernet 1/0/5
            Interface:  GigabitEthernet1/0/5
          MAC Address:  0050.5686.a389
           IP Address:  20.0.209.99
            User-Name:  00505686a389
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  in
        Authorized By:  Authentication Server
           Vlan Group:  N/A
            Filter-Id:  GuestAccess
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  1400D1140001B07C7F228D21
      Acct Session ID:  0x0001B07B
               Handle:  0xE700007C
```

Figure 23 – Validating the Filter-ID from the Cisco CLI



00:50:56:86:A3:89

State	Last Seen	MAC Address	MAC OUI Vendor	Device Family	Device Type	Authorization	Reason	Profile	IP Address	Authentication Type	Host Name
✓	7/15/2021 4:55:25 ...	00:50:56:86:A3:89	VMware, Inc.	Windows	Windows 10	Filter-Id='GuestAccess.in'	Rule: "Registered Guests"	Guest Access NAC Profile	20.0.209.99	MAC (PAP)	

End-System Events and Health Results

S.	Time Stamp	MAC Address	Device Family	Device Type	IP Address	Host Name	User Name	Auth Type	Reason	Profile	Switch IP	Switch Nickname	Switch Port	Switch Location	Authorization
✓	7/15/2021 4:55:25 ...	00:50:56:86:A3:89	Windows	Windows 10	20.0.209.99		User, Test	MAC (PAP)	Rule: "Regi...	Guest Acce...	20.0.209.20	Cat3750-1.rea...	GigabitEth...	CTC-Reading	Filter-Id='GuestAcce
✓	7/15/2021 4:55:24 ...	00:50:56:86:A3:89	Windows	Windows 10			User, Test	MAC (PAP)	Rule: "Regi...	Guest Acce...	20.0.209.20	Cat3750-1.rea...	GigabitEth...	CTC-Reading	Filter-Id='GuestAcce
✓	7/15/2021 4:55:24 ...	00:50:56:86:A3:89	Windows	Windows 10			User, Test	MAC (PAP)	Rule: "Regi...	Guest Acce...	20.0.209.20	Cat3750-1.rea...	GigabitEth...	CTC-Reading	Filter-Id='GuestAcce
✓	7/15/2021 4:55:24 ...	00:50:56:86:A3:89	Windows	Windows 10	20.0.209.99		User, Test	MAC (PAP)	Rule: "Regi...	Guest Acce...	20.0.209.20	Cat3750-1.rea...	GigabitEth...	CTC-Reading	Filter-Id='GuestAcce
	7/15/2021 4:55:03 ...	00:50:56:86:A3:89	Windows	Windows 10	20.0.209.99		User, Test	MAC (PAP)	Rule: "Regi...	Guest Acce...	20.0.209.20	Cat3750-1.rea...	GigabitEth...	CTC-Reading	Filter-Id='GuestAcce
✓	7/15/2021 4:54:21 ...	00:50:56:86:A3:89	Windows	Windows 10	20.0.209.99		User, Test	MAC (PAP)	Rule: "Regi...	Guest Acce...	20.0.209.20	Cat3750-1.rea...	GigabitEth...	CTC-Reading	Filter-Id='GuestAcce
✓	7/15/2021 4:54:20 ...	00:50:56:86:A3:89	Windows	Windows 10			User, Test	MAC (PAP)	Rule: "Regi...	Guest Acce...	20.0.209.20	Cat3750-1.rea...	GigabitEth...	CTC-Reading	Filter-Id='GuestAcce

Figure 24 – ExtremeControl End-System table after successful Guest Registration

ExtremeControl Configuration using Downloadable ACLs

Overview

This section covers the configuration of ExtremeControl to use the Cisco switch as an edge enforcement point using the Downloadable ACL method.

Policy and Downloadable ACLs

The Policy tab of ExtremeControl provides a single pane of glass to configure access permissions for roles that can be assigned via Access Control. A feature enhancement starting with Extreme Management Center version 8.1 and also included in ExtremeCloud IQ - Site Engine version 21.04.10.99 extends this functionality to Cisco switches through the use of Downloadable ACLs.

The new feature takes advantage of the ability to write ACLs as part of the RADIUS Accept message that is returned to the switch during client authentication. The traditional method of policy enforcement with ExtremeWireless and ExtremeSwitching is to write the policy rules and roles via SNMP so that they exist locally on the device. This new method does not write to the switch itself; rather, the policy rules and roles are saved in the local database on the Access Control Engine. Therefore, when an enforce is done, any policy-capable Extreme device will have policy pushed via SNMP, while any Cisco or HPE switch will have the policy converted automatically to a Downloadable ACL (or Per-User ACL) that is saved in the database.

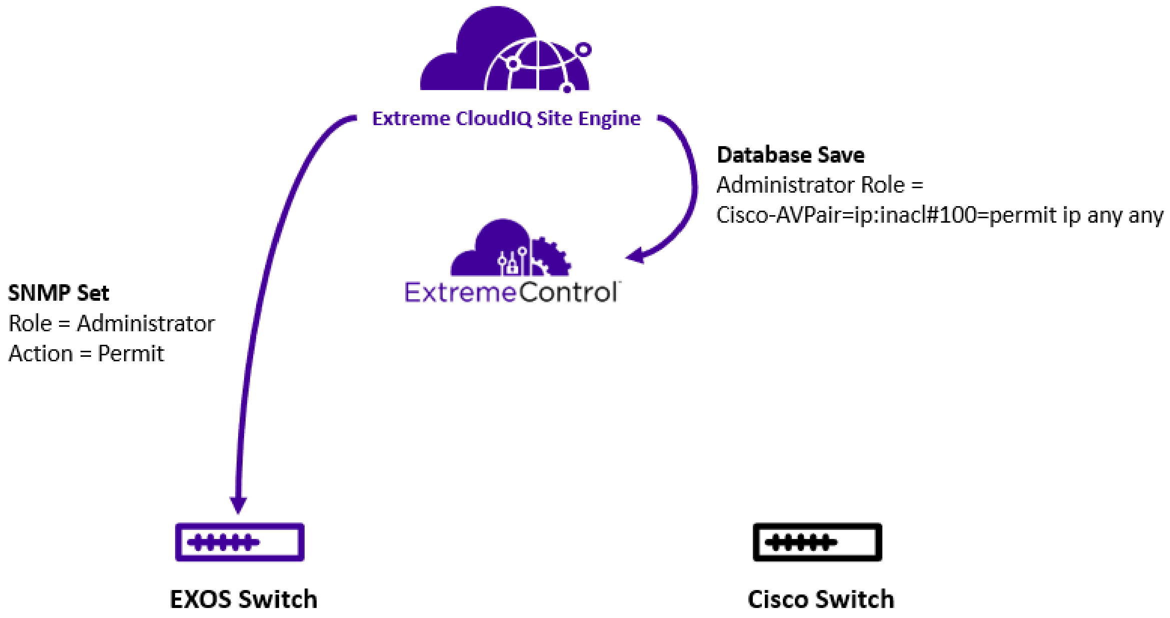
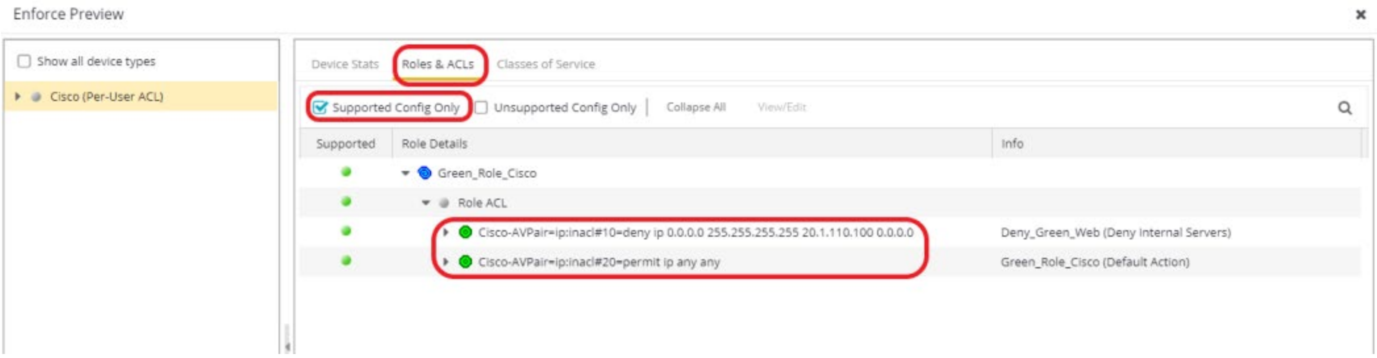


Figure 25 – Policy enforcement with EXOS and Cisco switches

Upon enforcement of the policy domain, the exact ACLs to be assigned can be reviewed in the Enforce Preview screen as shown in Figure 26.



Enforce Preview

☐ Show all device types

Cisco (Per-User ACL)

Supported	Role Details	Info
●	Green_Role_Cisco	
●	Role ACL	
●	Cisco-AVPair=ip:inacl#10=deny ip 0.0.0.0 255.255.255.255 20.1.110.100 0.0.0.0	Deny_Green_Web (Deny Internal Servers)
●	Cisco-AVPair=ip:inacl#20=permit ip any any	Green_Role_Cisco (Default Action)

Figure 26 – How to visualize Cisco Per-User ACLs during policy enforcement

NOTE

The Role ACLs tab will appear in the UI only after a Cisco switch has been added to the policy domain.

After a device authenticates to Access Control and Downloadable ACLs are configured to be returned to the authenticated session, the appropriate RADIUS Attributes are included that specify the ACLs to assign the end system.

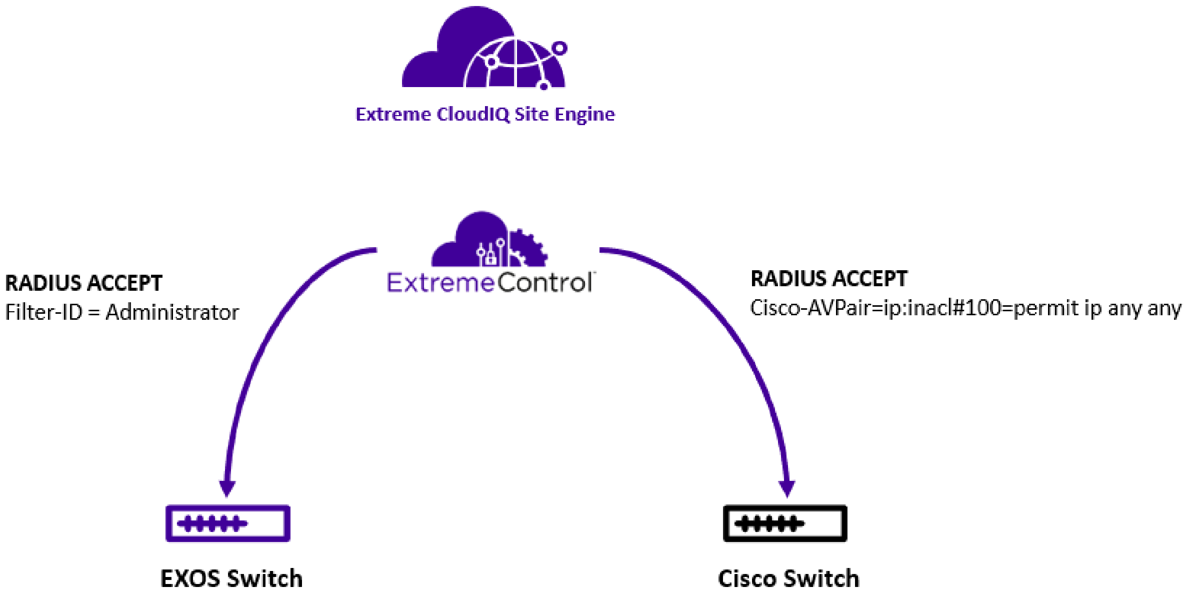
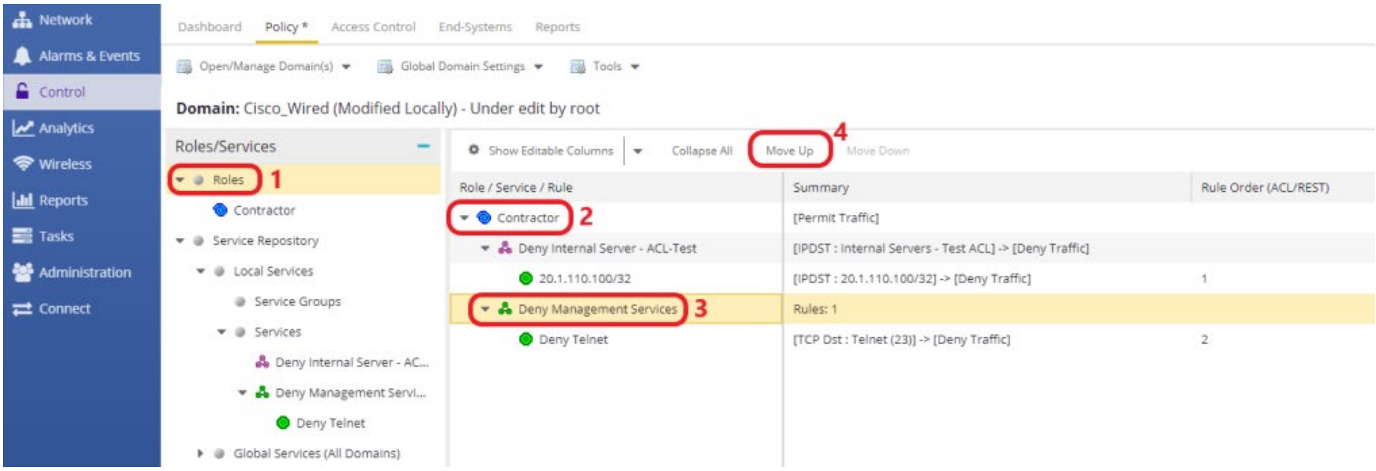

Extreme CloudIQ Site Engine
ExtremeControl
RADIUS ACCEPT
Filter-ID = Administrator
RADIUS ACCEPT
Cisco-AVPair=ip:inacl#100=permit ip any any
EXOS Switch
Cisco Switch

Figure 27 – Policy assignment (authorization) with EXOS and Cisco switches

Rule Ordering

When converting policy rules to Downloadable ACLs, ExtremeCloud IQ - Site Engine makes some intelligent decisions to set a precedence of the ordering. However, the ordering that is derived might not be the desired outcome. In this case, the ordering of the Downloadable ACLs can be rearranged during assignment. This is accomplished by following the steps as shown in Figure 28, using the “Move Up” or “Move Down” options to arrange the rules as desired.

> **NOTE**
>
> The Rule Ordering view will appear in the UI only after a Cisco switch has been added to the policy domain.



Domain: Cisco_Wired (Modified Locally) - Under edit by root

Role / Service / Rule	Summary	Rule Order (ACL/REST)
Contractor	[Permit Traffic]	
Deny Internal Server - ACL-Test	[IPDST : Internal Servers - Test ACL] -> [Deny Traffic]	
20.1.110.100/32	[IPDST : 20.1.110.100/32] -> [Deny Traffic]	1
Deny Management Services	Rules: 1	
Deny Telnet	[TCP Dst : Telnet (23)] -> [Deny Traffic]	2

Figure 28 – How to order ACL Rules within a Policy Domain

Policy Support

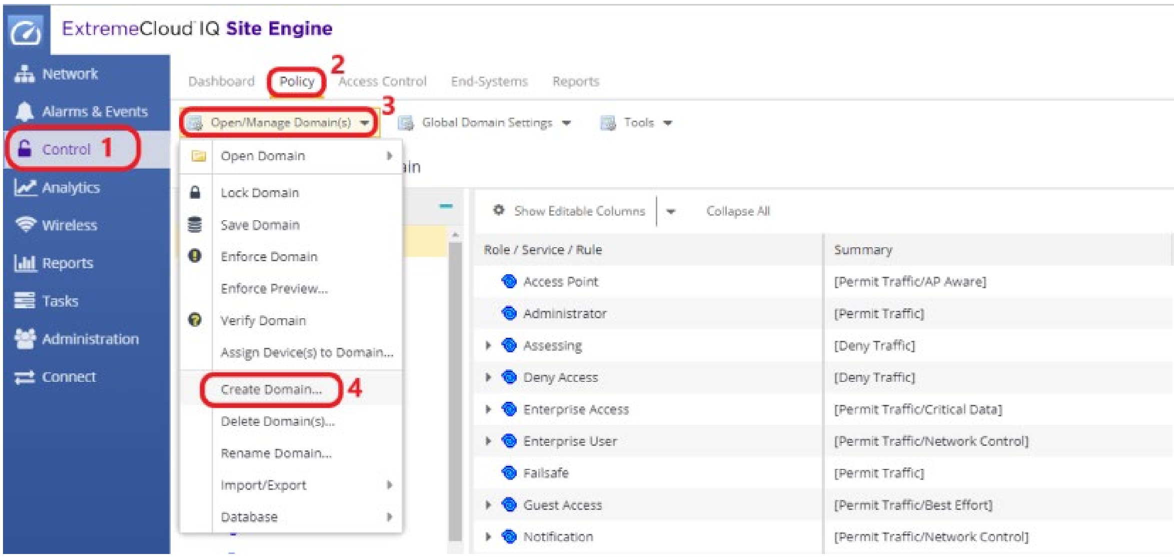
Because Extreme Policy has many features that can be used in addition to traditional ACL support, there will be certain feature sets within Policy that cannot be converted to Downloadable ACLs. The following policy types are supported based on the hardware and software capabilities of Cisco.

- IP Address Source, Destination, and Bilateral traffic
- TCP Source, Destination, and Bilateral traffic
- UDP Source, Destination, and Bilateral traffic
- ICMP

Step 1: Create a Policy Domain for the Cisco Switch

Unlike the Dynamic ACL approach, the first step one needs to consider is to create a Policy Domain for Cisco switches. This Policy Domain will be used when adding the switch to Access Control and for creating Roles, Services and Rules.

Navigate to **Control** and then **Policy** and follow the steps illustrated in Figure 29 to create a new Policy Domain.

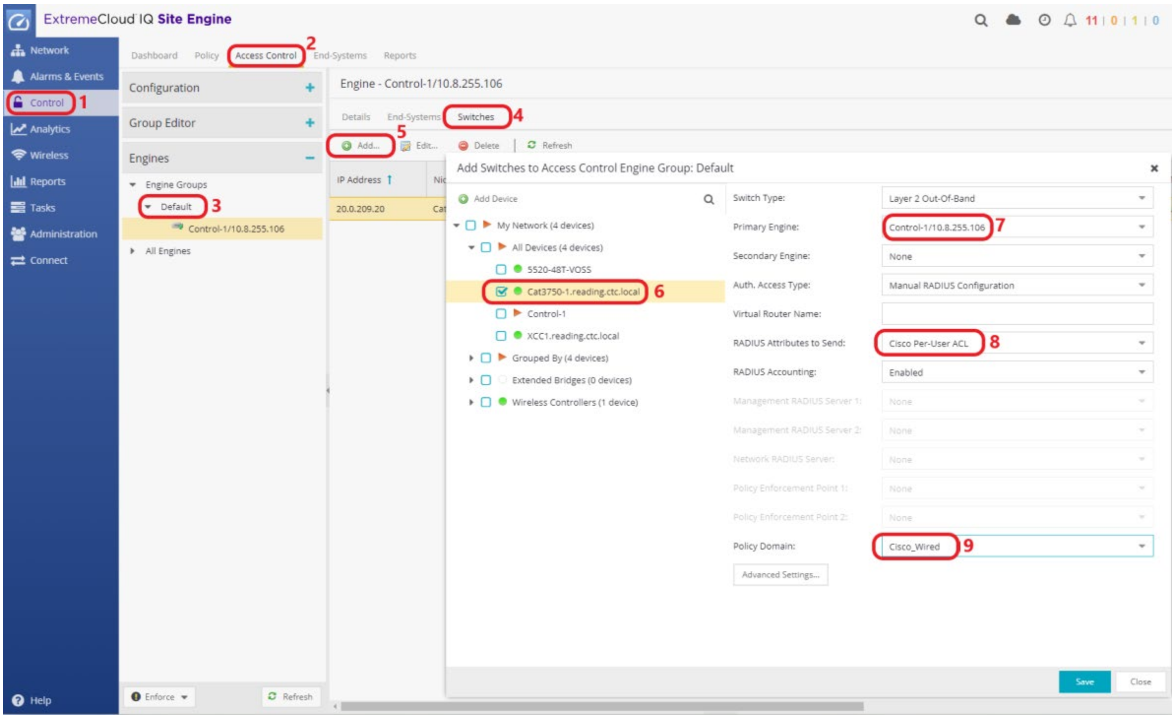


Role / Service / Rule	Summary
Access Point	[Permit Traffic/AP Aware]
Administrator	[Permit Traffic]
Assessing	[Deny Traffic]
Deny Access	[Deny Traffic]
Enterprise Access	[Permit Traffic/Critical Data]
Enterprise User	[Permit Traffic/Network Control]
Failsafe	[Permit Traffic]
Guest Access	[Permit Traffic/Best Effort]
Notification	[Permit Traffic/Network Control]

Figure 29 – How to create a new Policy Domain

Step 2a: Add the Cisco Switch to Access Control

Navigate to the **Control** menu within ExtremeCloud IQ - Site Engine and select the **Access Control** tab. Under **Engines**, select the **Default** group and then the **Switches** tab. Select the **Add** button to assign the Cisco switch to the Access Control Engine group. Select the drop-down option for the **RADIUS Attributes to Send** field and select **Cisco Per-User ACL**. Finally, select the Policy Domain that was created in Step 1. See Figure 30.



Engine - Control-1/10.8.255.106

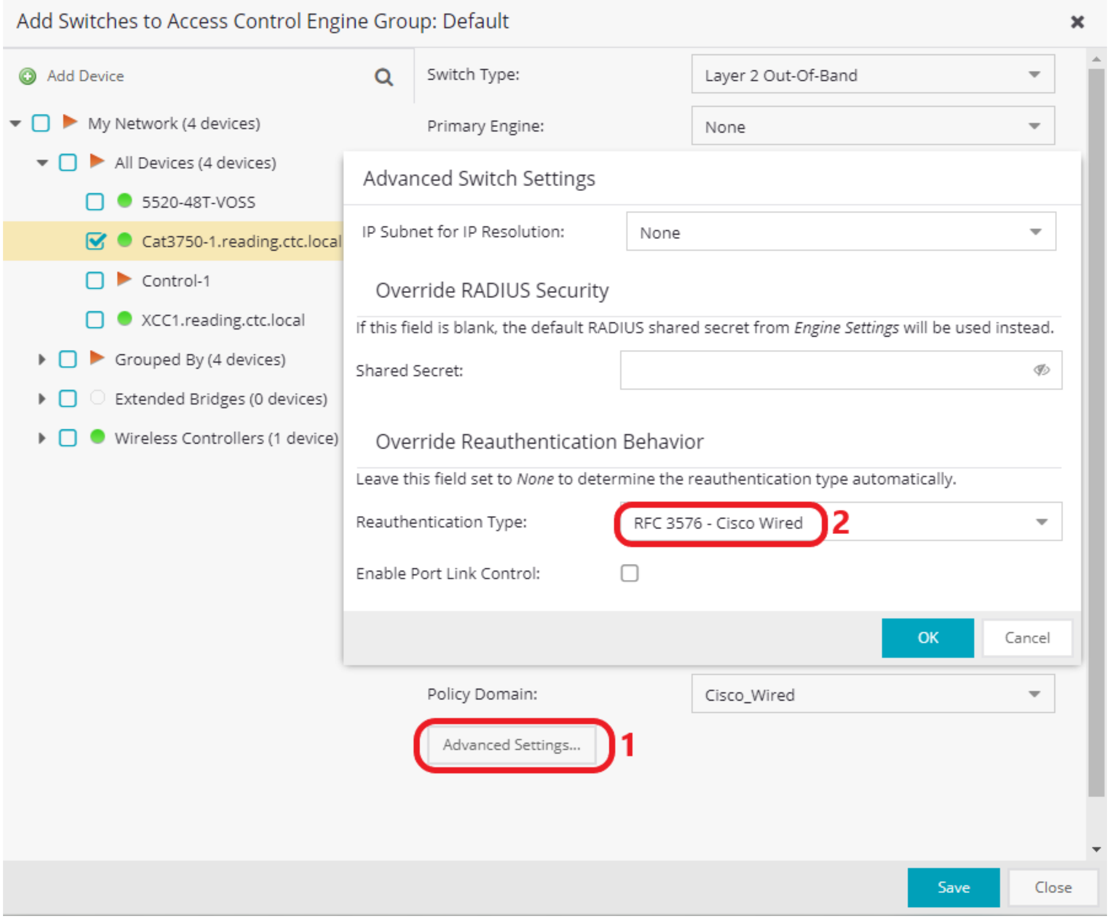
Add Switches to Access Control Engine Group: Default

- □ My Network (4 devices)
  - □ All Devices (4 devices)
    - □ 5520-48T-VOSS
    - ☑ Cat3750-1.reading.ctc.local 6
    - □ Control-1
    - □ XCC1.reading.ctc.local
  - □ Grouped By (4 devices)
  - □ Extended Bridges (0 devices)
  - □ Wireless Controllers (1 device)

Switch Type: Layer 2 Out-Of-Band
Primary Engine: Control-1/10.8.255.106 7
Secondary Engine: None
Auth. Access Type: Manual RADIUS Configuration
Virtual Router Name:
RADIUS Attributes to Send: Cisco Per-User ACL 8
RADIUS Accounting: Enabled
Management RADIUS Server 1: None
Management RADIUS Server 2: None
Network RADIUS Server: None
Policy Enforcement Point 1: None
Policy Enforcement Point 2: None
Policy Domain: Cisco_Wired 9
Advanced Settings...

Figure 30 – How to add a Cisco switch to Access Control

Select the **Advanced Settings** button and change the Reauthentication type to **RFC 3576 – Cisco Wired** as depicted in Figure 31. **Enforce** the Access Control configuration when prompted.



Add Switches to Access Control Engine Group: Default

Add Device

- My Network (4 devices)
  - All Devices (4 devices)
    - □ 5520-48T-VOSS
    - ☑ Cat3750-1.reading.ctc.local
    - □ Control-1
    - □ XCC1.reading.ctc.local
  - Grouped By (4 devices)
  - Extended Bridges (0 devices)
  - Wireless Controllers (1 device)

Switch Type: Layer 2 Out-Of-Band

Primary Engine: None

Advanced Switch Settings

IP Subnet for IP Resolution: None

Override RADIUS Security

If this field is blank, the default RADIUS shared secret from *Engine Settings* will be used instead.

Shared Secret:

Override Reauthentication Behavior

Leave this field set to *None* to determine the reauthentication type automatically.

Reauthentication Type: RFC 3576 - Cisco Wired

Enable Port Link Control: □

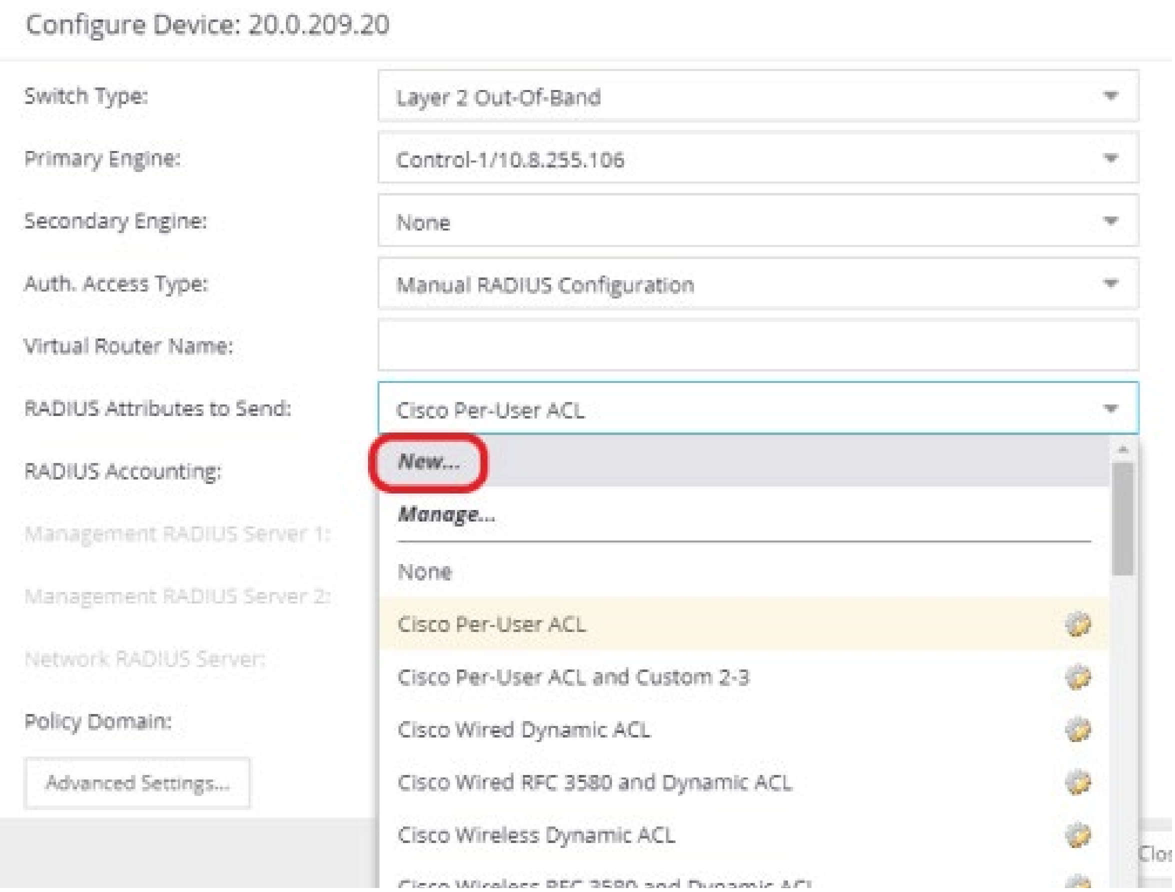
Policy Domain: Cisco_Wired

Figure 31 – How to configure reauthentication settings for a Cisco switch

If there is a need to assign additional Cisco VSAs (Vendor Specific Attributes) for cases such as IP Phones or redirecting users Web traffic to a portal, then it is recommended to create a custom “RADIUS Attribute” by adding Custom 2 and Custom 3 fields for the required Cisco VSAs. See Step 2b if this is the case in your deployment and create a custom Radius Attribute, otherwise skip to Step 3.

Step 2b: Optional – Create a New RADIUS Attribute Configuration to Include Additional Cisco VSAs

To create a new Radius Attribute configuration, expand "RADIUS Attributes to Send" and select New as shown in Figure 32.



Configure Device: 20.0.209.20

Switch Type: Layer 2 Out-Of-Band

Primary Engine: Control-1/10.8.255.106

Secondary Engine: None

Auth. Access Type: Manual RADIUS Configuration

Virtual Router Name:

RADIUS Attributes to Send: Cisco Per-User ACL

RADIUS Accounting:

Management RADIUS Server 1:

Management RADIUS Server 2:

Network RADIUS Server:

Policy Domain:

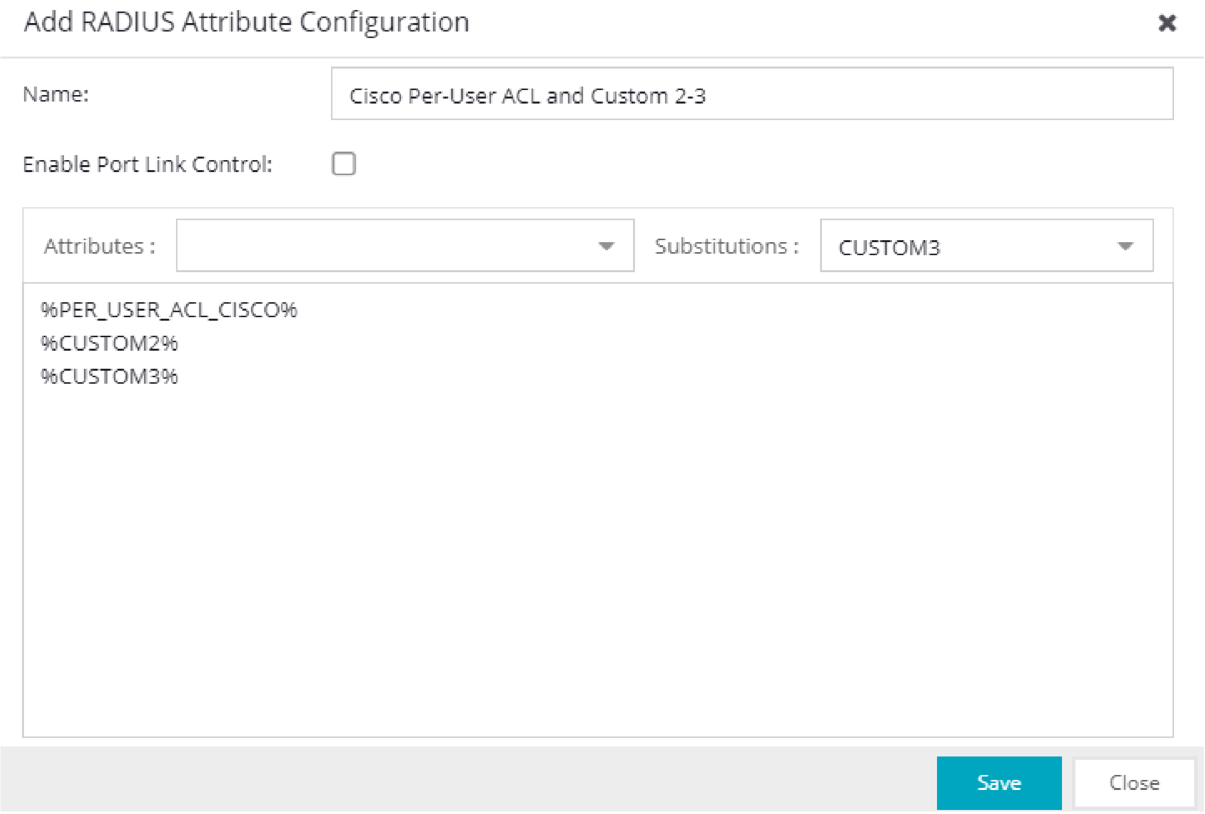
New...
Manage...
None
Cisco Per-User ACL
Cisco Per-User ACL and Custom 2-3
Cisco Wired Dynamic ACL
Cisco Wired RFC 3580 and Dynamic ACL
Cisco Wireless Dynamic ACL
Cisco Wireless RFC 3580 and Dynamic ACL
Advanced Settings...
Clos

Figure 32 – How to create a new RADIUS attribute in ExtremeControl

In the **Add RADIUS Attribute Configuration** window, the RADIUS attributes and variables can be assigned to the switch. These attributes are then communicated to the switch via RADIUS Accept packets. The **Substitutions** are variables that are calculated by Access Control at the time of authentication.

Set the **Name** for the configuration to the value **Cisco Per-User ACL and Custom 2-3**. Select the drop-down menu on the **Substitutions** field and individually choose the options **Per-User ACL Cisco**, **Custom 2**, and **Custom 3**.

The Custom 2 and Custom 3 substitutions are used when additional Cisco Vendor Specific Attributes (VSAs) need to be sent. For instance, with IP Phones, a VSA is required to assign the phone VLAN on a Cisco switch. Alternatively, to redirect a user's Web traffic to a portal, a separate combination of Cisco VSAs is required. Ensure that each attribute appears on a separate line within the configuration window.


Add RADIUS Attribute Configuration

Name: Cisco Per-User ACL and Custom 2-3

Enable Port Link Control: □

Attributes :

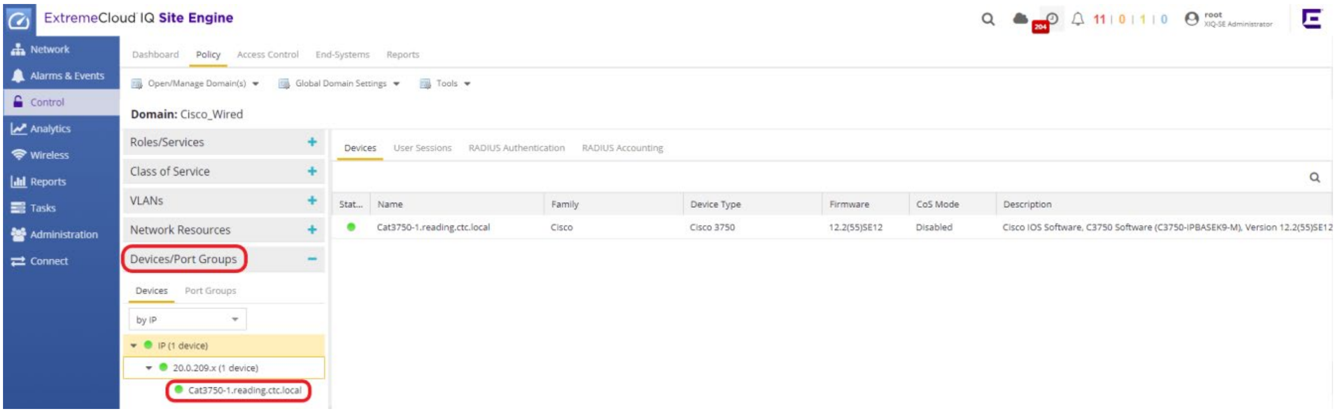
Substitutions : CUSTOM3

```
%PER_USER_ACL_CISCO%
%CUSTOM2%
%CUSTOM3%
```

Figure 33 – Custom RADIUS attributes that include additional Cisco VSAs

Step 3: Create a Layer 3 Network Resource

Select the **Policy** tab and then open the **Cisco_Wired** Policy Domain that was previously created. Select the **Devices/Port Groups** menu and ensure that the Cisco switch has been added to the domain.



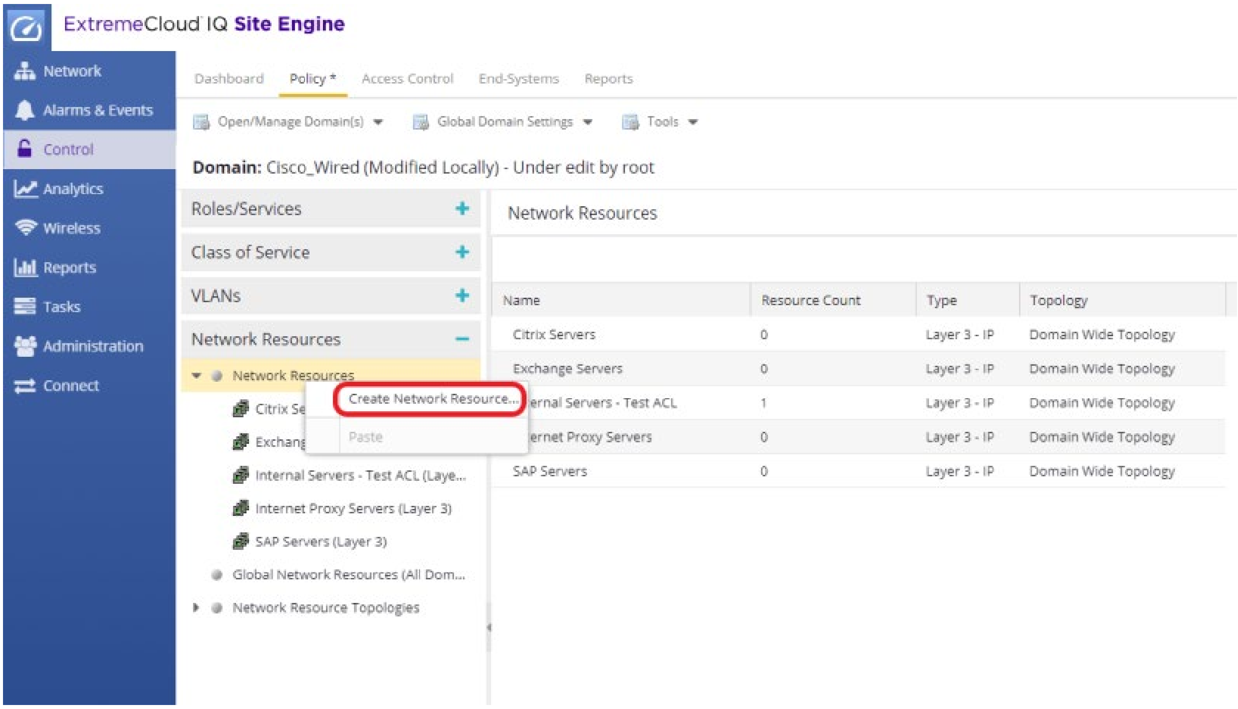
Domain: Cisco_Wired

Stat...	Name	Family	Device Type	Firmware	CoS Mode	Description
●	Cat3750-1.reading.ctc.local	Cisco	Cisco 3750	12.2(55)SE12	Disabled	Cisco IOS Software, C3750 Software (C3750-IPBASEK9-M), Version 12.2(55)SE12

Figure 34 – How to verify that a Cisco switch is added to Policy Domain

The next step involves creating a new **Network Resource** which can then be used to store a list of internal server IP addresses. This Network Resource can then be used within an automated service assigned to a role.

Select the **Network Resource** panel, right-click **Network Resources** in the tree, and then select **Create Network Resource**. In the **Create** pop-up window, set the **Name** field to the value of **Internal Servers – Test-ACL**.



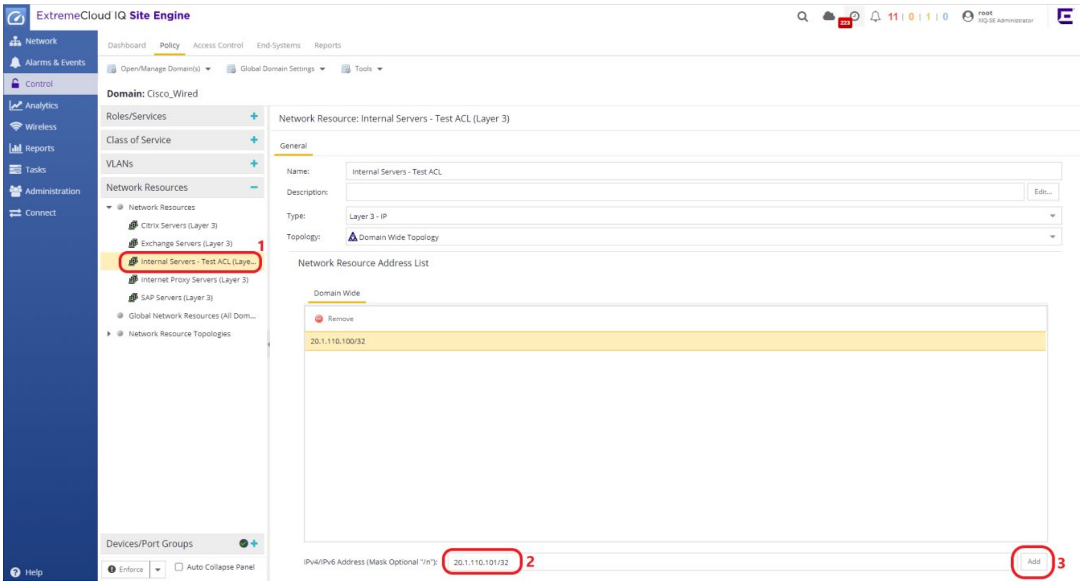
Domain: Cisco_Wired (Modified Locally) - Under edit by root

Network Resources

Name	Resource Count	Type	Topology
Citrix Servers	0	Layer 3 - IP	Domain Wide Topology
Exchange Servers	0	Layer 3 - IP	Domain Wide Topology
ernal Servers - Test ACL	1	Layer 3 - IP	Domain Wide Topology
ernet Proxy Servers	0	Layer 3 - IP	Domain Wide Topology
SAP Servers	0	Layer 3 - IP	Domain Wide Topology

Figure 35 – How to create a new Network Resource

In the **General** tab, enter the IP address of an internal resource to which access will be denied and select the **Add** button to complete the process.



Domain: Cisco_Wired

Network Resource: Internal Servers - Test ACL (Layer 3)

Name: Internal Servers - Test ACL

Description:

Type: Layer 3 - IP

Topology: Domain Wide Topology

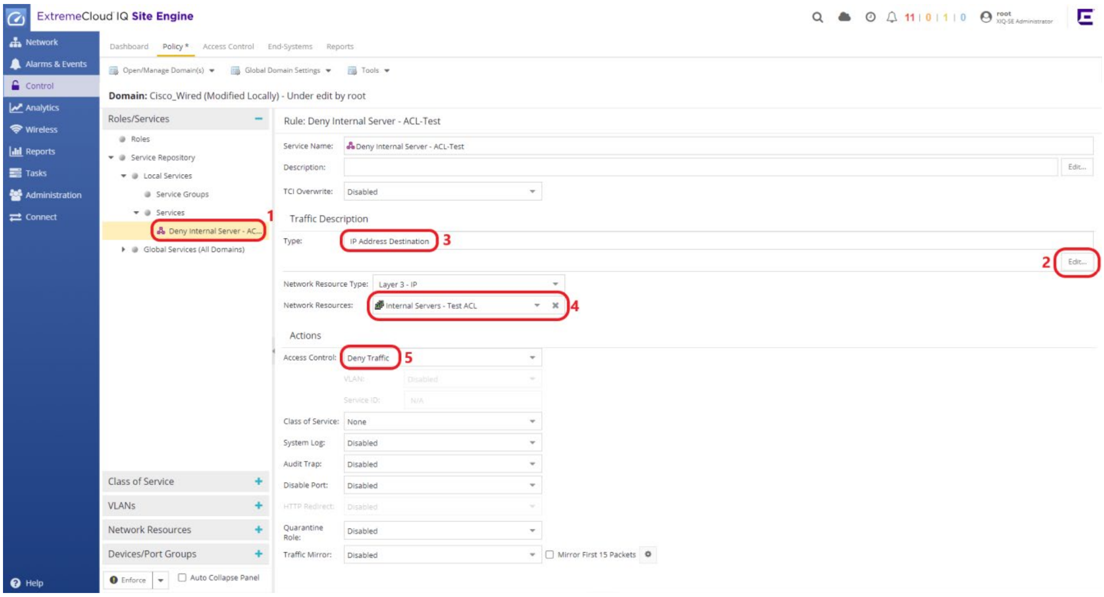
20.1.110.100/32

IPv4/IPv6 Address (Mask Optional "/n"): 20.1.110.101/32

Figure 36 – How to add IP addresses/subnets to a Layer 3 Network Resource

Next, select the **Roles/Services** panel, scroll down to **Services** in the tree, and then right- click the **Services** item. Select the pop-up menu option **Create Automated Service**. Set the name field to **Deny Internal Server – ACL-Test** and select the **OK** button. Select the **Edit** button in the **Traffic Description** section and select **IP Address Destination** as the option.

For the **Network Resource Type,** select **Layer 3 – IP** and for the **Network Resources** select the previously created **Internal Servers – Test-ACL** resource. Finally, select **Deny Traffic** as the **Access Control** option under **Actions**. Figure 37 illustrates this process step by step.



Domain: Cisco_Wired (Modified Locally) - Under edit by root

Rule: Deny Internal Server - ACL-Test

Service Name: Deny Internal Server - ACL-Test

Description:

TCI Overwrite: Disabled

Type: IP Address Destination

Network Resource Type: Layer 3 - IP

Network Resources: Internal Servers - Test ACL

Access Control: Deny Traffic

VLAN: Disabled

Service ID: N/A

Class of Service: None

System Log: Disabled

Audit Trap: Disabled

Disable Port: Disabled

HTTP Redirect: Disabled

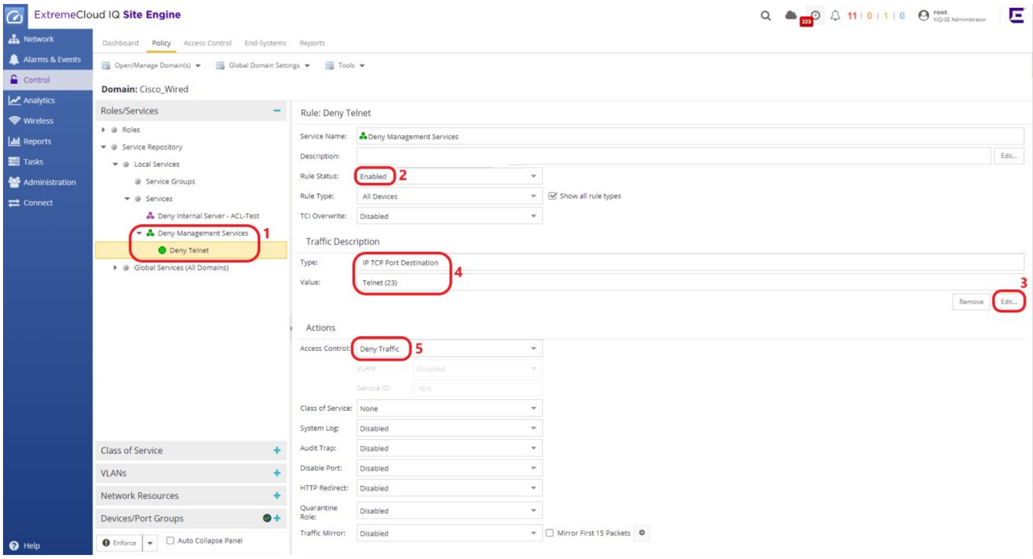
Quarantine Role: Disabled

Traffic Mirror: Disabled □ Mirror First 15 Packets

Figure 37 – How to create an Automated Service and attach Network Resources

Step 4: Create a Layer 4 Network Service

To create a Layer 4 Network service, right-click on the **Services** menu and select **Create Service** instead of **Create Automated Service**. Create a new service named **Deny Management Services**. Set the **Rule Status** to **Enabled**, set the **Traffic Description** to **IP TCP Port Destination** with a **Value** of **Telnet (23),** and set **Access Control** to **Deny Traffic**.



Domain: Cisco_Wired

Rule: Deny Telnet

Service Name: Deny Management Services
Description:
Rule Status: Enabled
Rule Type: All Devices ☑ Show all rule types
TCI Overwrite: Disabled

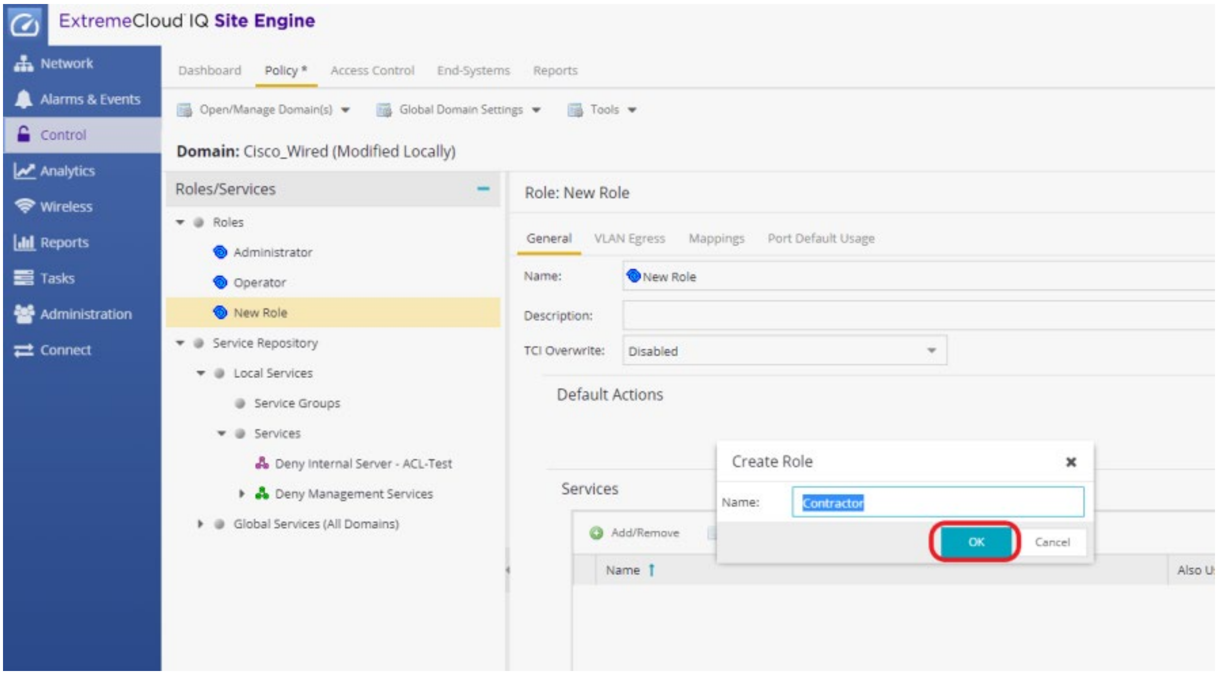
Traffic Description
Type: IP TCP Port Destination
Value: Telnet (23)

Actions
Access Control: Deny Traffic
VLAN: Disabled
Service ID: N/A
Class of Service: None
System Log: Disabled
Audit Trap: Disabled
Disable Port: Disabled
HTTP Redirect: Disabled
Quarantine Role: Disabled
Traffic Mirror: Disabled □ Mirror First 15 Packets

Figure 38 – How to create a Layer-4 Network Service

Step 5: Assign Services to a Role

Right-click on the **Roles** menu, create a new role called **Contractor,** and select the **OK** button to complete the process.



Domain: Cisco_Wired (Modified Locally)

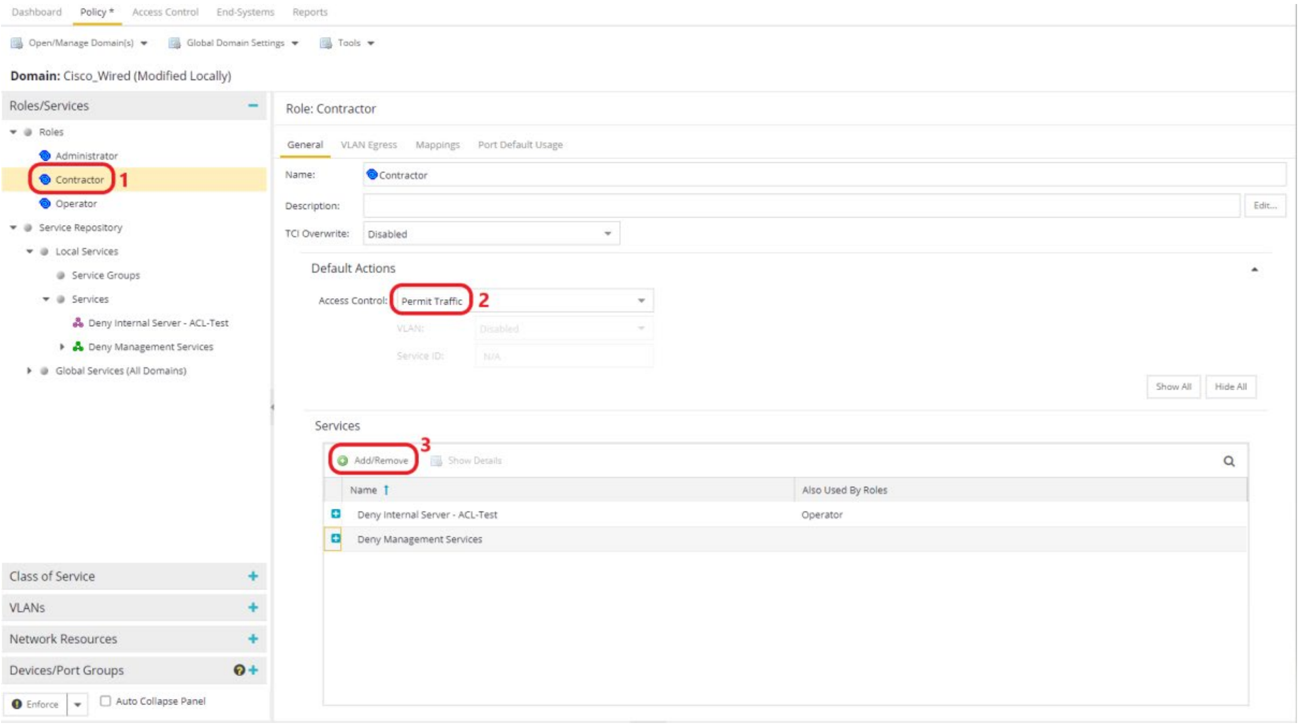
Role: New Role

Name: New Role
Description:
TCI Overwrite: Disabled

Create Role
Name: Contractor

Figure 39 – How to create a new role in a policy

Select the newly created role and set the **Default Action** for **Access Control** to **Permit Traffic**. Then select the **Add/Remove** button from the **Services** section and add the two previously created services.



Domain: Cisco_Wired (Modified Locally)

Role: Contractor

Name: Contractor

Description:

TCI Overwrite: Disabled

Access Control: Permit Traffic

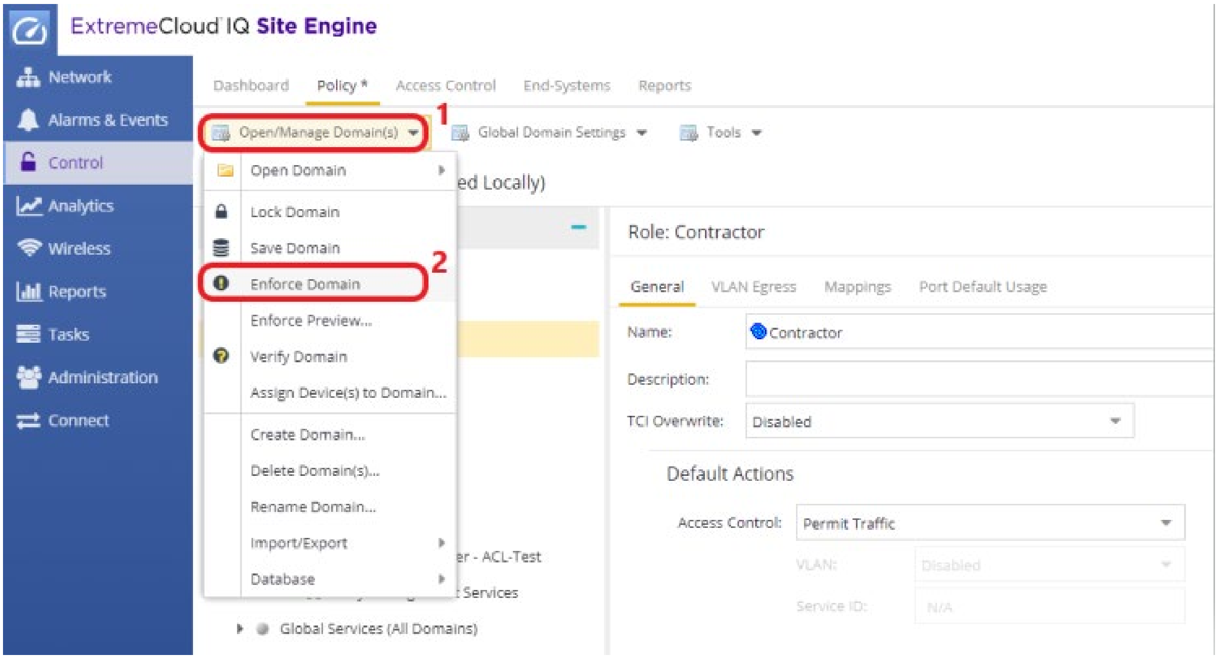
VLAN: Disabled

Service ID: N/A

Name	Also Used By Roles
Deny Internal Server - ACL-Test	Operator
Deny Management Services	

Figure 40 – How to add services to roles in a policy

Now that the configuration changes for the Contractor role are complete, select the **Open/Manage Domain(s)** menu and then choose the **Enforce Domain** option. The **Enforce Preview** window opens.



Role: Contractor

Name: Contractor

Description:

TCI Overwrite: Disabled

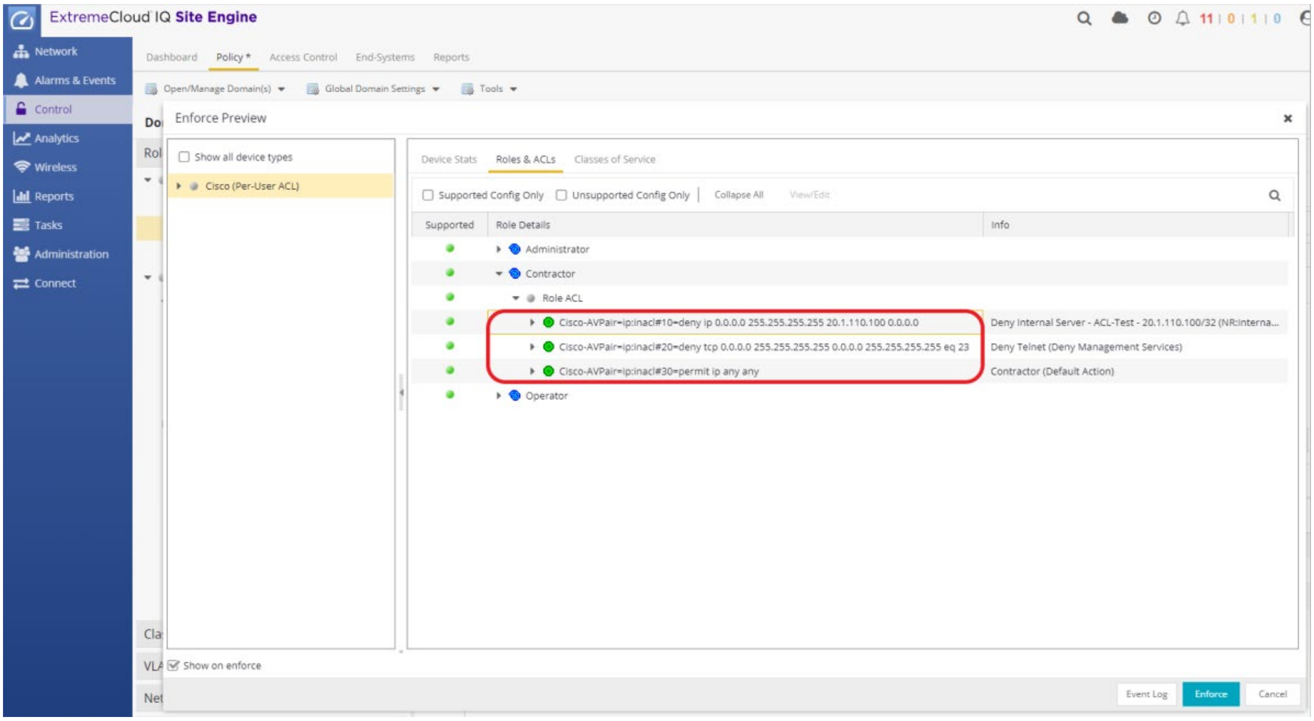
Access Control: Permit Traffic

VLAN: Disabled

Service ID: N/A

Figure 41 – How to enforce a Policy Domain

In the Enforce Preview window, select the Role/ACLs tab followed by the Supported Config Only checkbox. Expand both the TestRole role and the sub-item called Role ACL. Note that the Per-User ACLs contain the Cisco VSAs that are sent to the switch in the RADIUS Accept message. Select the Enforce button to continue.

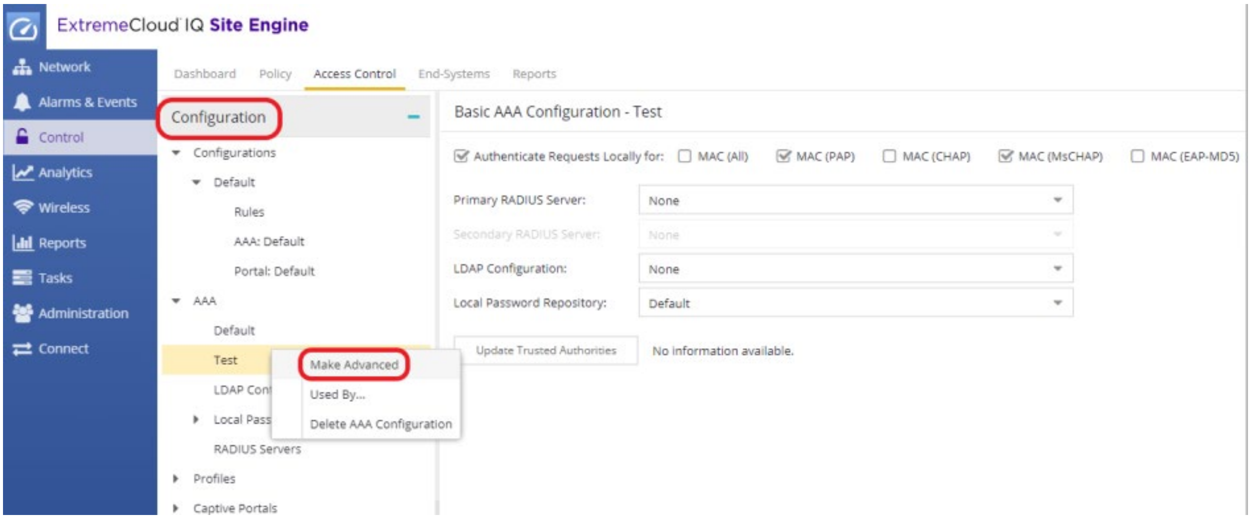


Supported	Role Details	Info
●	Administrator	
●	Contractor	
●	Role ACL	
●	Cisco-AVPair=ip:inacl#10=deny ip 0.0.0.0 255.255.255.255 20.1.110.100 0.0.0.0	Deny Internal Server - ACL-Test - 20.1.110.100/32 (NR:Interna...
●	Cisco-AVPair=ip:inacl#20=deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 23	Deny Telnet (Deny Management Services)
●	Cisco-AVPair=ip:inacl#30=permit ip any any	Contractor (Default Action)
●	Operator	

Figure 42 – Enforce Preview Screen

Step 6: Configure AAA with LDAP Authentication Method

To ensure that the switch receives a RADIUS Reject message when testing availability of the Access Control Engine, the AAA configuration needs to be adjusted. Select the Configuration section, expand AAA in the Configuration tree, and right-click the Default AAA configuration. Select Make Advanced. If the AAA Configuration is already in Advanced Mode, skip this step.



Basic AAA Configuration - Test

☑ Authenticate Requests Locally for: □ MAC (All) ☑ MAC (PAP) □ MAC (CHAP) ☑ MAC (MsCHAP) □ MAC (EAP-MD5)

Primary RADIUS Server: None

Secondary RADIUS Server: None

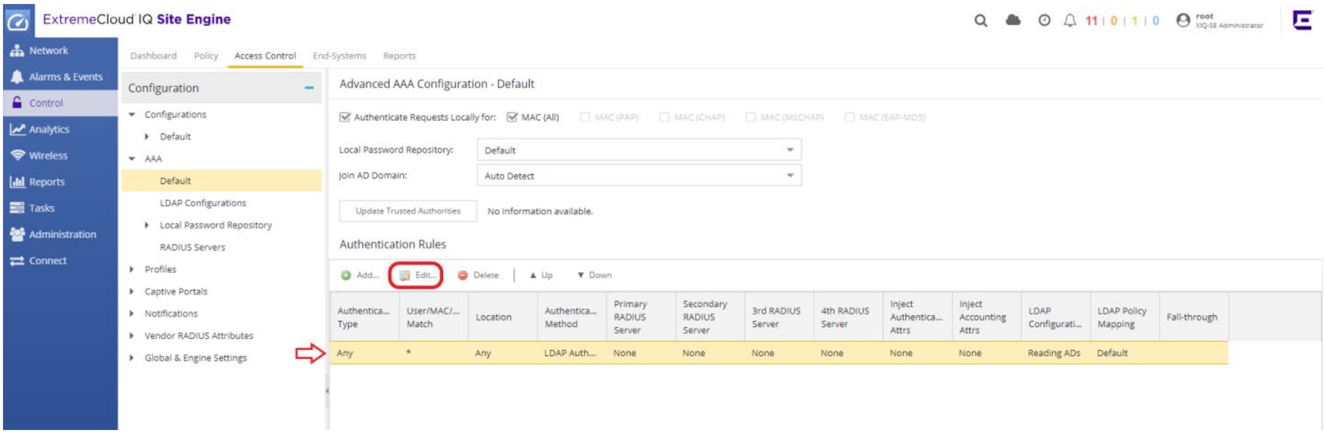
LDAP Configuration: None

Local Password Repository: Default

No information available.

Figure 43 – AAA Configuration - 1

Select the “**Any**” Authentication Rule and then the **Edit** button.



Advanced AAA Configuration - Default

☑ Authenticate Requests Locally for: ☑ MAC (All) □ MAC (PAP) □ MAC (CHAP) □ MAC (MsCHAP) □ MAC (EAP-MD5)

Local Password Repository: Default

Join AD Domain: Auto Detect

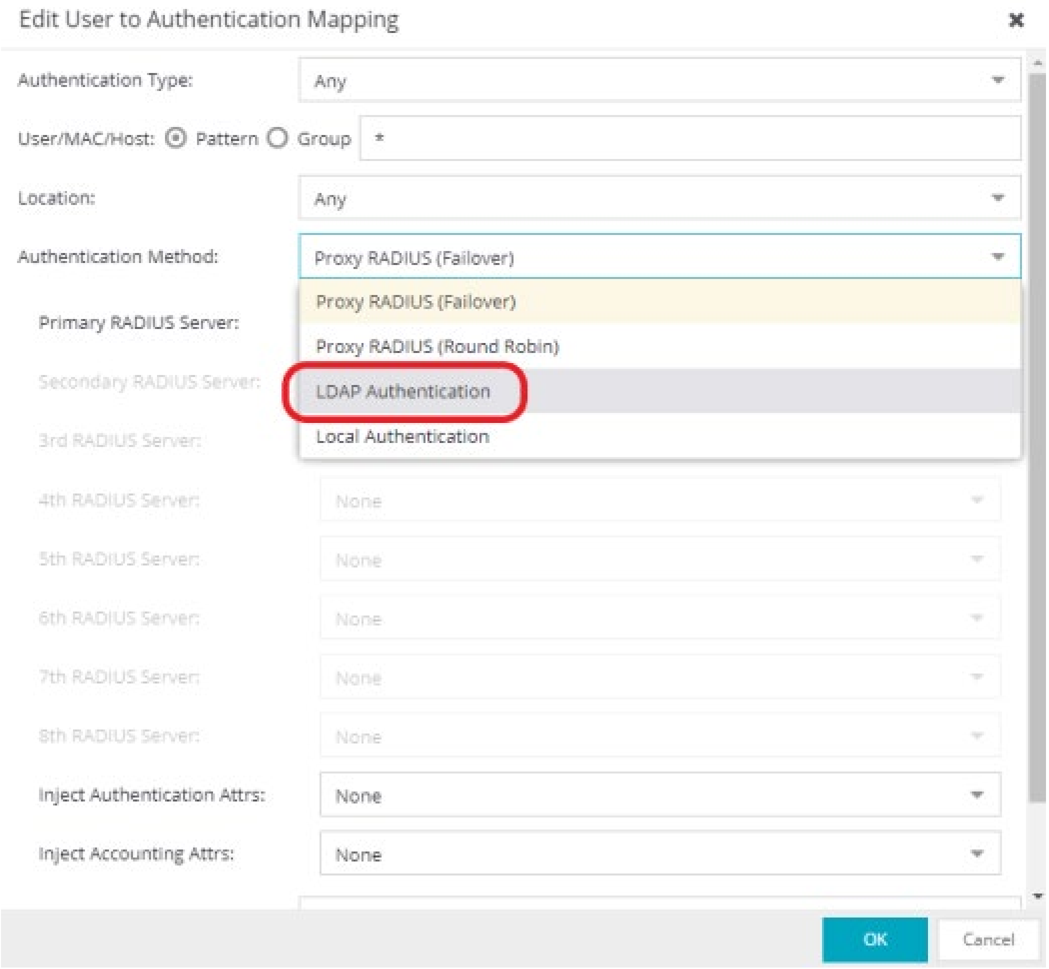
No information available.

Authentication Rules

Authentica... Type	User/MAC/... Match	Location	Authentica... Method	Primary RADIUS Server	Secondary RADIUS Server	3rd RADIUS Server	4th RADIUS Server	Inject Authentica... Attrs	Inject Accounting Attrs	LDAP Configurati...	LDAP Policy Mapping	Fall-through
Any	*	Any	LDAP Auth...	None	None	None	None	None	None	Reading ADs	Default	

Figure 44 – AAA Configuration - 2

In this section, LDAP Authentication will be used. In the “**Edit User to Authentication Mapping**” window, change the **Authentication Method** to **LDAP Authentication** and then select the **OK** button.



Edit User to Authentication Mapping

Authentication Type: Any

User/MAC/Host: ● Pattern ○ Group *

Location: Any

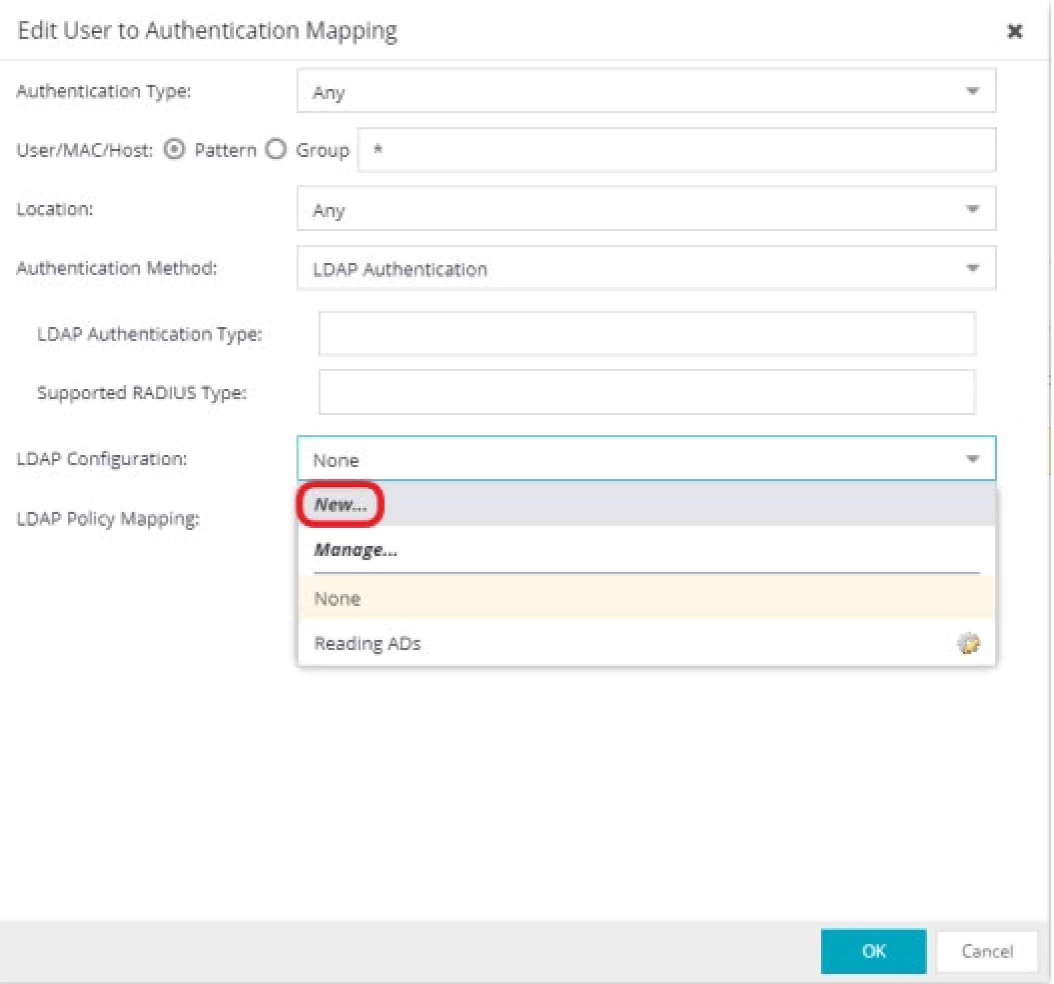
Authentication Method: Proxy RADIUS (Failover)

Inject Authentication Attrs: None

Inject Accounting Attrs: None

Figure 45 – AAA Configuration – LDAP Authentication Setting

After selecting **LDAP Authentication**, a new LDAP configuration needs to be created which will allow ExtremeControl to communicate with Active Directory. Select the drop-down menu in **LDAP Configuration** and then select **New** as shown in Figure 46.



Edit User to Authentication Mapping

Authentication Type: Any

User/MAC/Host: ● Pattern ○ Group *

Location: Any

Authentication Method: LDAP Authentication

LDAP Authentication Type:

Supported RADIUS Type:

LDAP Configuration: None

LDAP Policy Mapping:

Figure 46 – AAA Configuration – Add LDAP Configuration – 1

Follow the steps illustrated in Figure 47 to populate LDAP configuration fields.

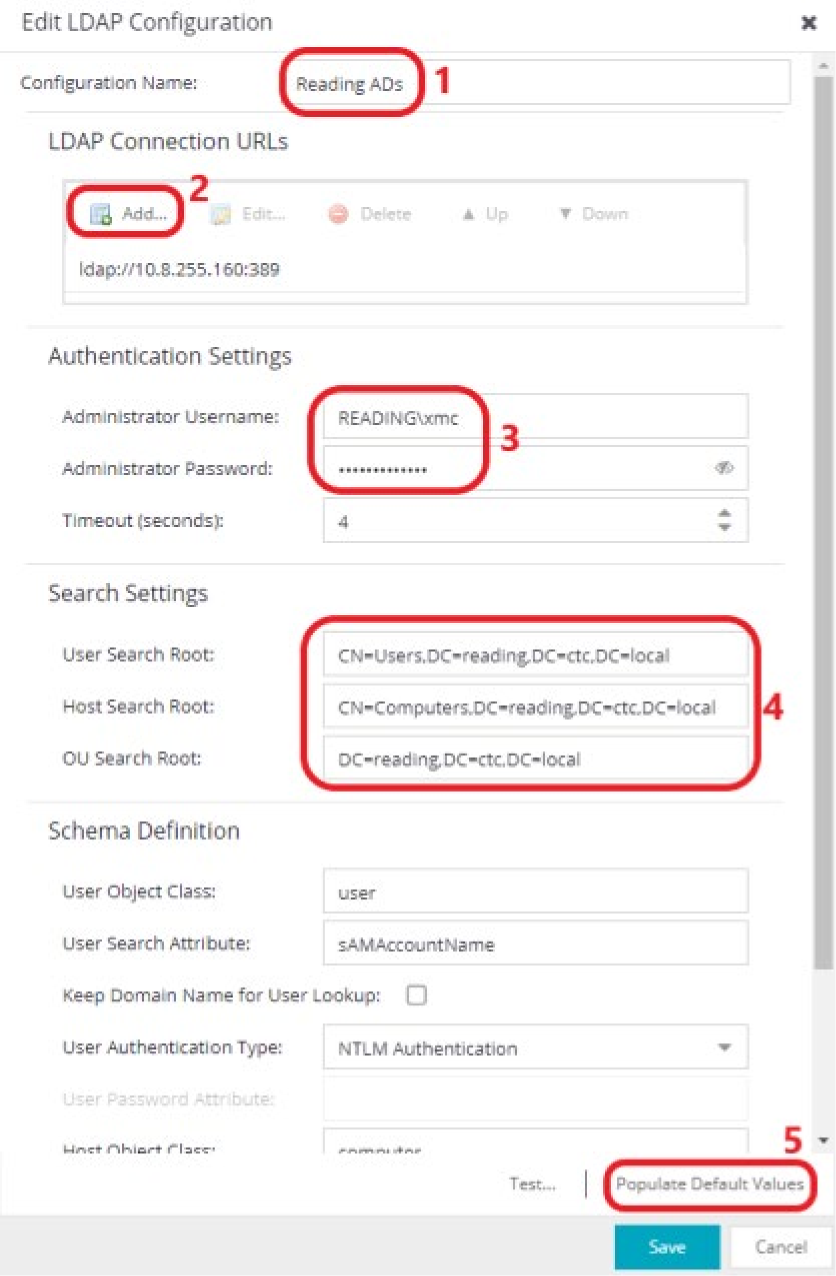
1- Configuration Name: Give a name to the LDAP Configuration

2- LDAP Connection URL: Select the **Add** button and provide the IP address of the LDAP server(s). The URL format must be the following: ldap://a.b.c.d:389 or ldaps://a.b.c.d:636. More than one LDAP Server is recommended for high availability.

3- Administrator Username and Password: *DOMAIN\Username* of LDAP user to perform LDAP lookups and password of username.

4- Search settings: To create the search roots, the FQDN of the domain needs to be broken into separate DC= statements, comma delimited. Add CN=Users and CN=Computers at the beginning of User and Computer search roots respectively.

5- Populate Default Values: At the bottom right click the **Populate Default Values** button, select **Active Directory User Defaults**, and select **Save**.



Edit LDAP Configuration

Configuration Name: Reading ADs

LDAP Connection URLs

ldap://10.8.255.160:389

Authentication Settings

Administrator Username: READING\xmc

Administrator Password: ••••••••••••••

Timeout (seconds): 4

Search Settings

User Search Root: CN=Users,DC=reading,DC=ctc,DC=local

Host Search Root: CN=Computers,DC=reading,DC=ctc,DC=local

OU Search Root: DC=reading,DC=ctc,DC=local

Schema Definition

User Object Class: user

User Search Attribute: sAMAccountName

Keep Domain Name for User Lookup: □

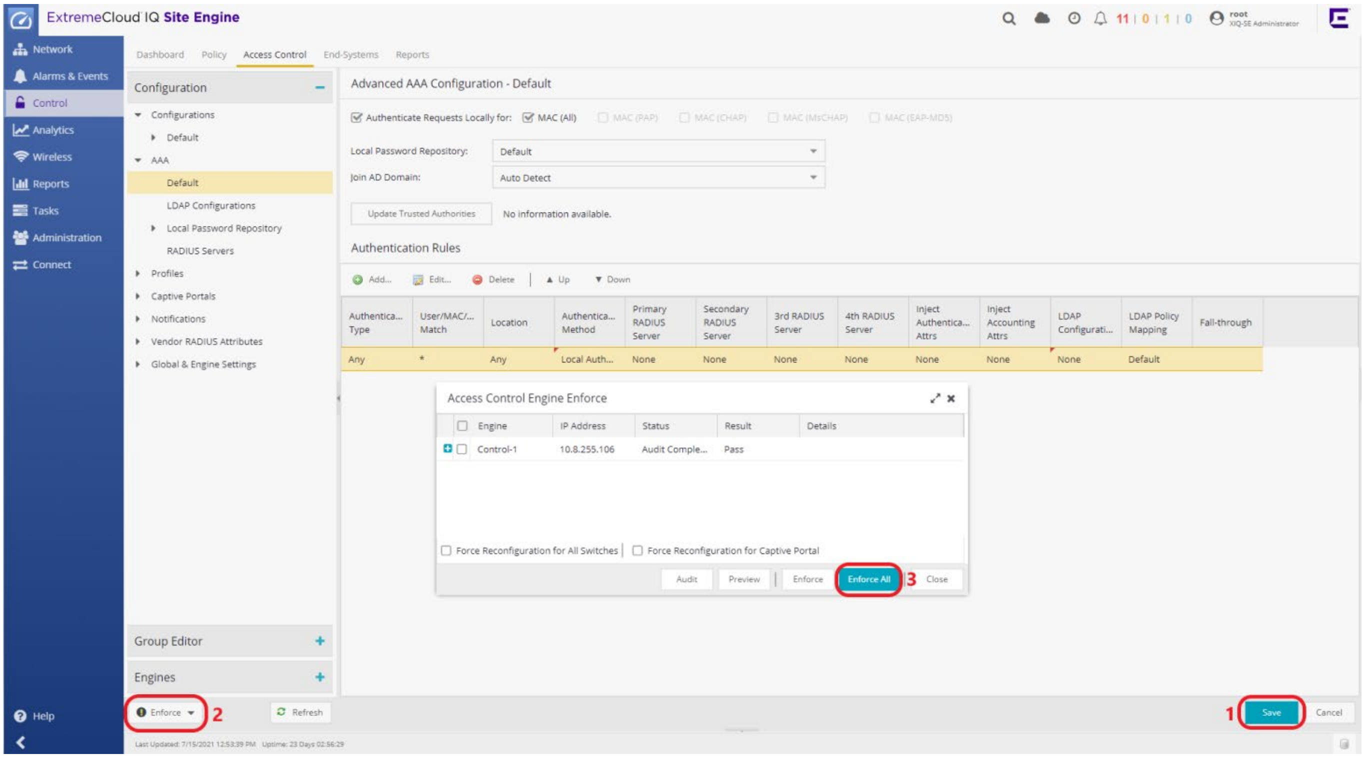
User Authentication Type: NTLM Authentication

User Password Attribute:

Host Object Class: computer

Figure 47 – AAA Configuration – Add LDAP Configuration – 2

Save the Configuration and **Enforce** again as shown in Figure 48.



Advanced AAA Configuration - Default

☑ Authenticate Requests Locally for: ☑ MAC (All) □ MAC (PAP) □ MAC (CHAP) □ MAC (MsCHAP) □ MAC (EAP-MD5)

Local Password Repository: Default

Join AD Domain: Auto Detect

No information available.

Authentication Rules

Authentica... Type	User/MAC/... Match	Location	Authentica... Method	Primary RADIUS Server	Secondary RADIUS Server	3rd RADIUS Server	4th RADIUS Server	Inject Authentica... Attrs	Inject Accounting Attrs	LDAP Configurati...	LDAP Policy Mapping	Fall-through
Any	*	Any	Local Auth...	None	None	None	None	None	None	None	Default	

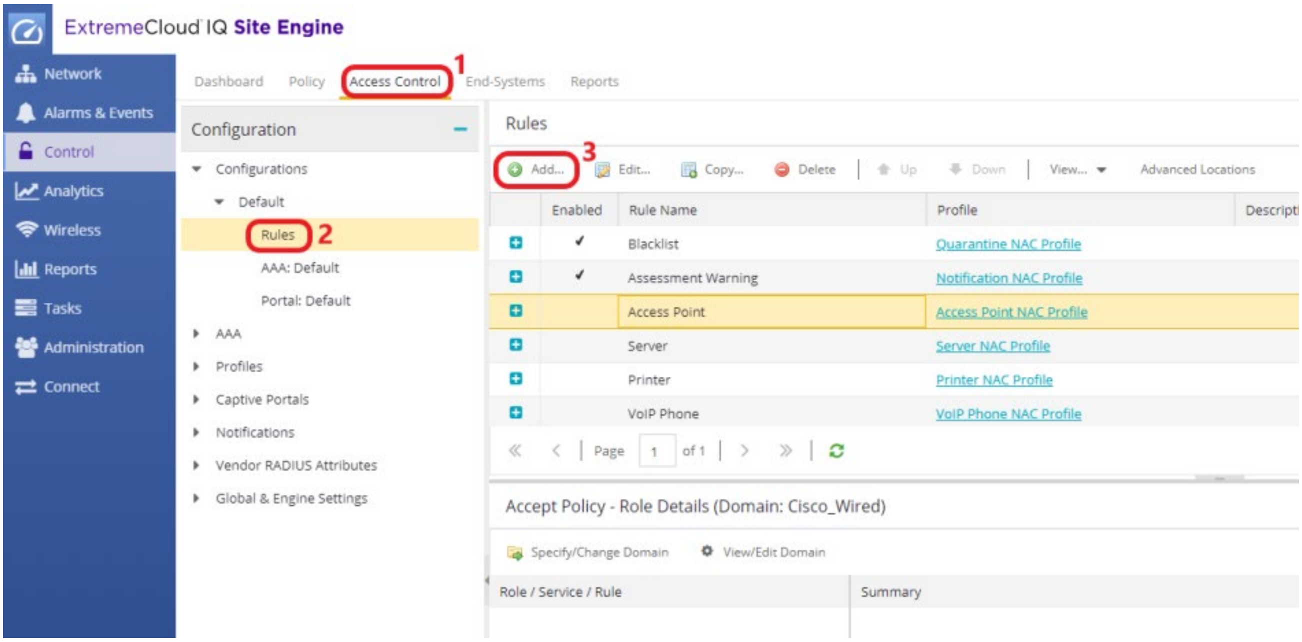
Access Control Engine Enforce

□ Engine	IP Address	Status	Result	Details
□ Control-1	10.8.255.106	Audit Comple...	Pass	

□ Force Reconfiguration for All Switches □ Force Reconfiguration for Captive Portal

Step 7: Create a Rule

To test the Downloadable ACL configuration, 802.1X authentication will be used and an LDAP User Group will be created and added as a Rule Condition. To accomplish this, select the **Access Control** tab, expand **Configurations** and then **Default**. Select **Rules** and then add a new rule.



Rules

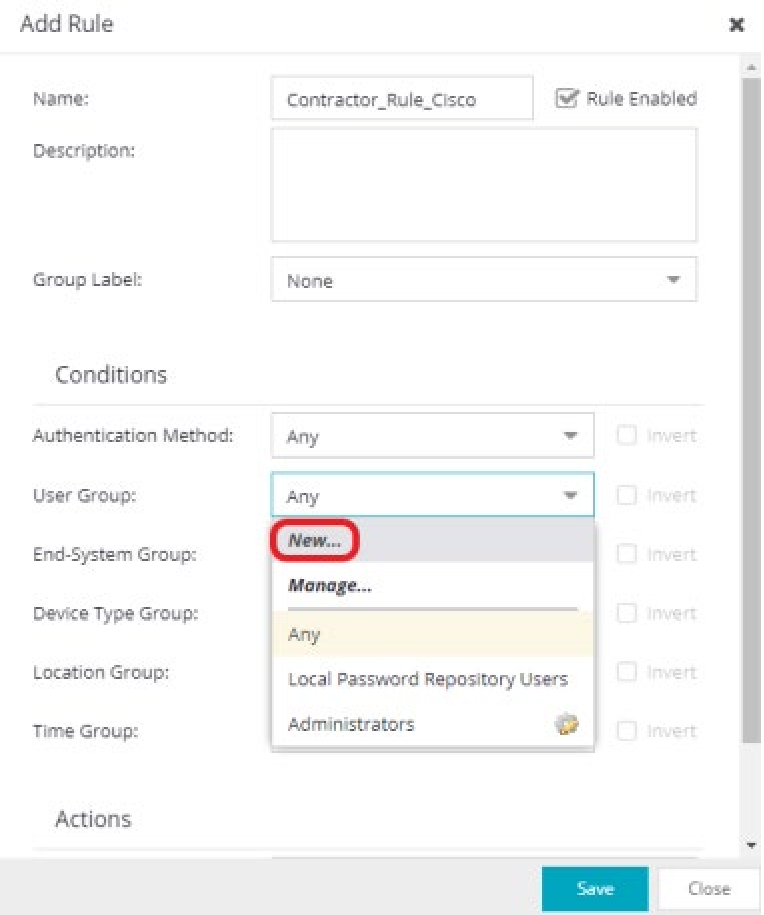
Enabled	Rule Name	Profile	Descripti
✓	Blacklist	Quarantine NAC Profile	
✓	Assessment Warning	Notification NAC Profile	
	Access Point	Access Point NAC Profile	
	Server	Server NAC Profile	
	Printer	Printer NAC Profile	
	VoIP Phone	VoIP Phone NAC Profile	

Accept Policy - Role Details (Domain: Cisco_Wired)

Role / Service / Rule	Summary

Figure 49 – How to add a new rule in Access Control

Name the rule Contractor_Rule_Cisco, select the User Group drop-down, and select New. Select LDAP User Group as Type and name the User Group as Contractor_Users.


Add Rule

Name: Contractor_Rule_Cisco ☑ Rule Enabled

Description:

Group Label: None

Conditions

Authentication Method: Any □ Invert

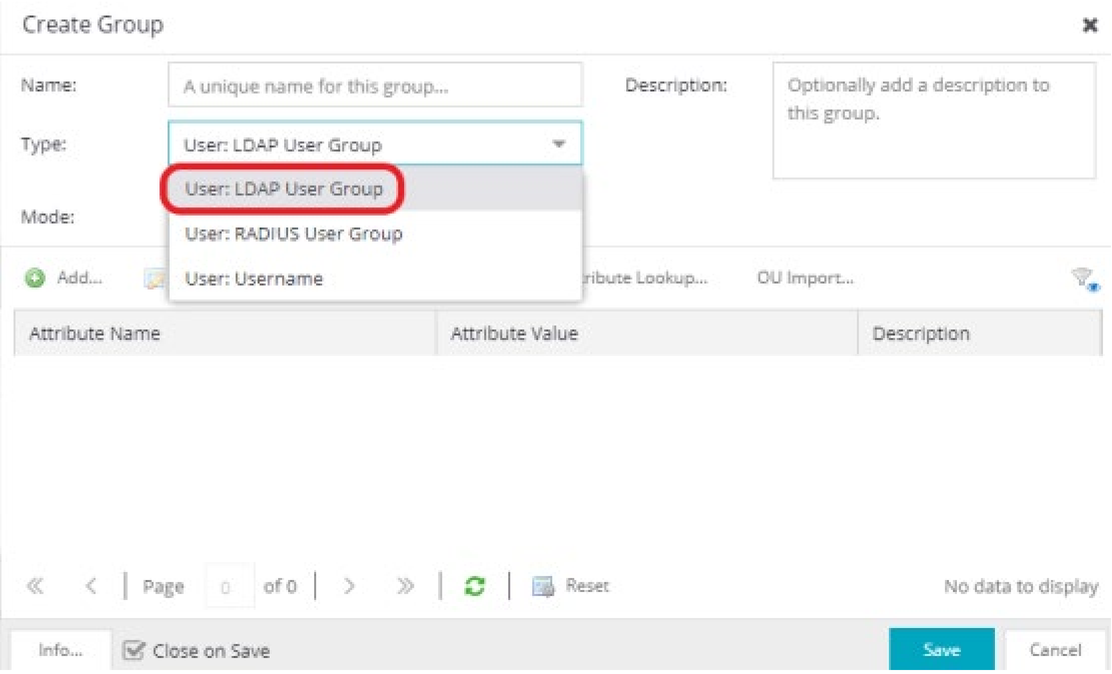
User Group: Any □ Invert

End-System Group: □ Invert

Device Type Group: □ Invert

Location Group: □ Invert

Time Group: □ Invert


Create Group

Name: A unique name for this group...

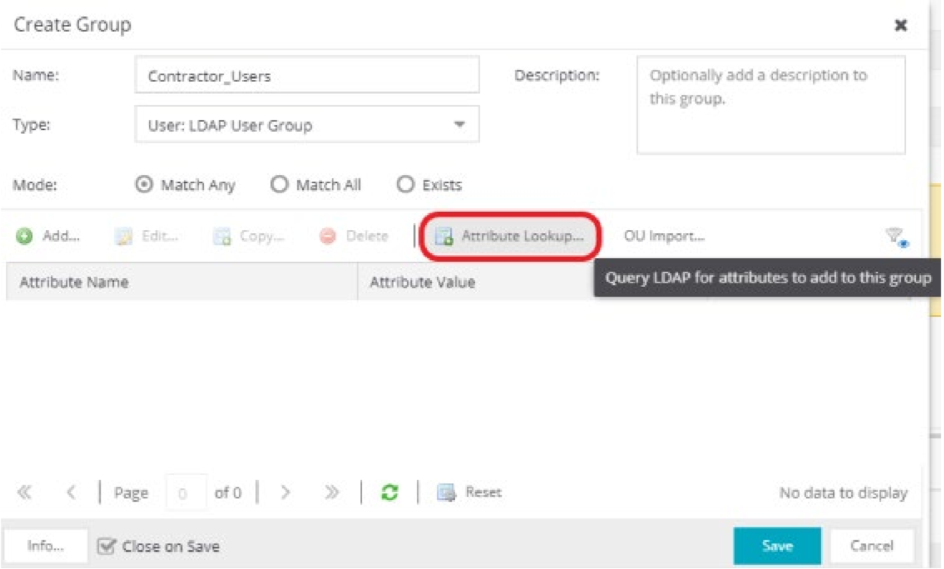
Description: Optionally add a description to this group.

Type: User: LDAP User Group

Mode:

Figure 50 – How to create an LDAP User Group in Access Control - 1

At this point, there is no link between the created User Group and LDAP Server. Therefore, an Attribute Name and Value need to be added to this LDAP User Group in order to look the user up in the LDAP Server during the authentication process. Select **Attribute Lookup** as shown in Figure 51 and search for a known user name belonging to the relevant LDAP User group, which is in our example Contractors.



Create Group

Name: Contractor_Users

Type: User: LDAP User Group

Description: Optionally add a description to this group.

Mode: ● Match Any ○ Match All ○ Exists

Attribute Name	Attribute Value

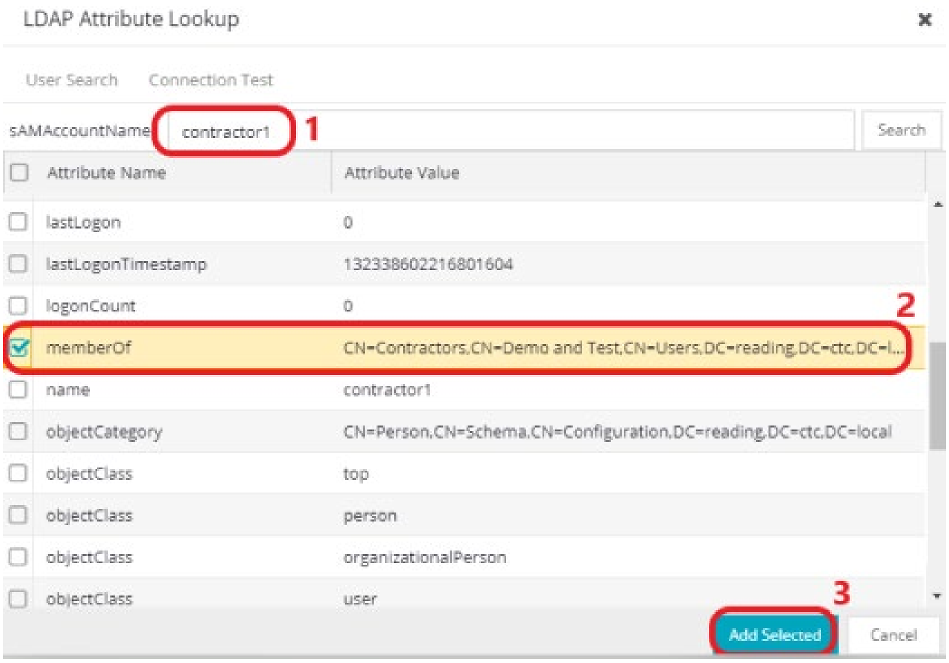
Page 0 of 0

No data to display

☑ Close on Save

Figure 51 – How to create an LDAP User Group in Access Control - 2

Select the LDAP Configuration created in Figure 48, search an Active Directory user belonging to Contractors OU in the Active Directory, and add the “**memberOf**” attribute name and value pair as shown in Figure-52.



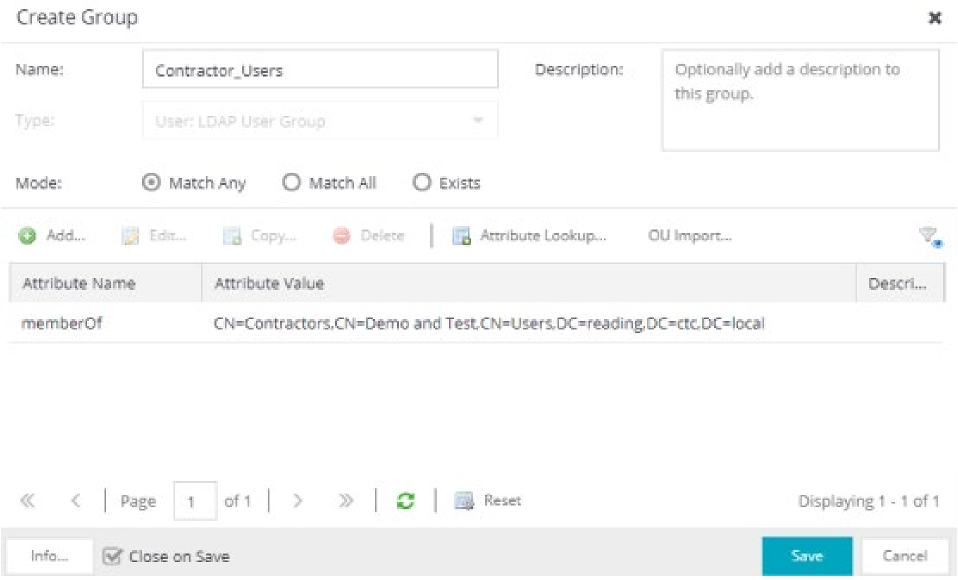
LDAP Attribute Lookup

sAMAccountName: contractor1

□	Attribute Name	Attribute Value
□	lastLogon	0
□	lastLogonTimestamp	132338602216801604
□	logonCount	0
☑	memberOf	CN=Contractors,CN=Demo and Test,CN=Users,DC=reading,DC=ctc,DC=l...
□	name	contractor1
□	objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=reading,DC=ctc,DC=local
□	objectClass	top
□	objectClass	person
□	objectClass	organizationalPerson
□	objectClass	user

Figure 52 – How to create an LDAP User Group in Access Control - 3

The LDAP User Group and the Access Control Rule must look like the ones depicted in Figure 53 and Figure 54, respectively.



Create Group

Name: Contractor_Users

Description: Optionally add a description to this group.

Type: User: LDAP User Group

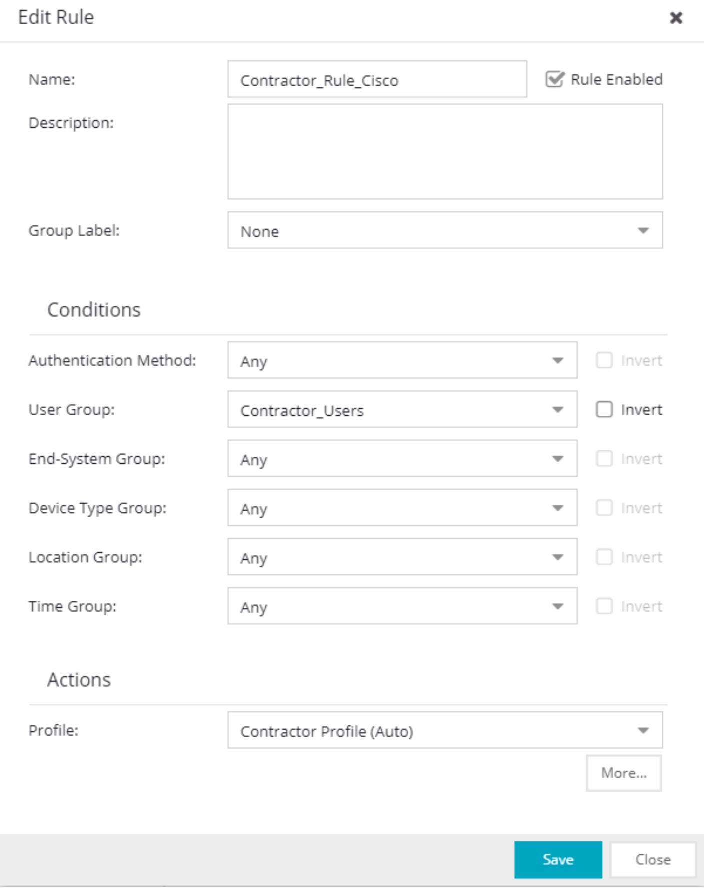
Mode: ● Match Any ○ Match All ○ Exists

Attribute Name	Attribute Value	Descri...
memberOf	CN=Contractors,CN=Demo and Test,CN=Users,DC=reading,DC=ctc,DC=local	

Displaying 1 - 1 of 1

☑ Close on Save

Figure 53 – LDAP User Group Example



Edit Rule

Name: Contractor_Rule_Cisco ☑ Rule Enabled

Description:

Group Label: None

Conditions

Authentication Method:	Any	□ Invert
User Group:	Contractor_Users	□ Invert
End-System Group:	Any	□ Invert
Device Type Group:	Any	□ Invert
Location Group:	Any	□ Invert
Time Group:	Any	□ Invert

Actions

Profile: Contractor Profile (Auto)

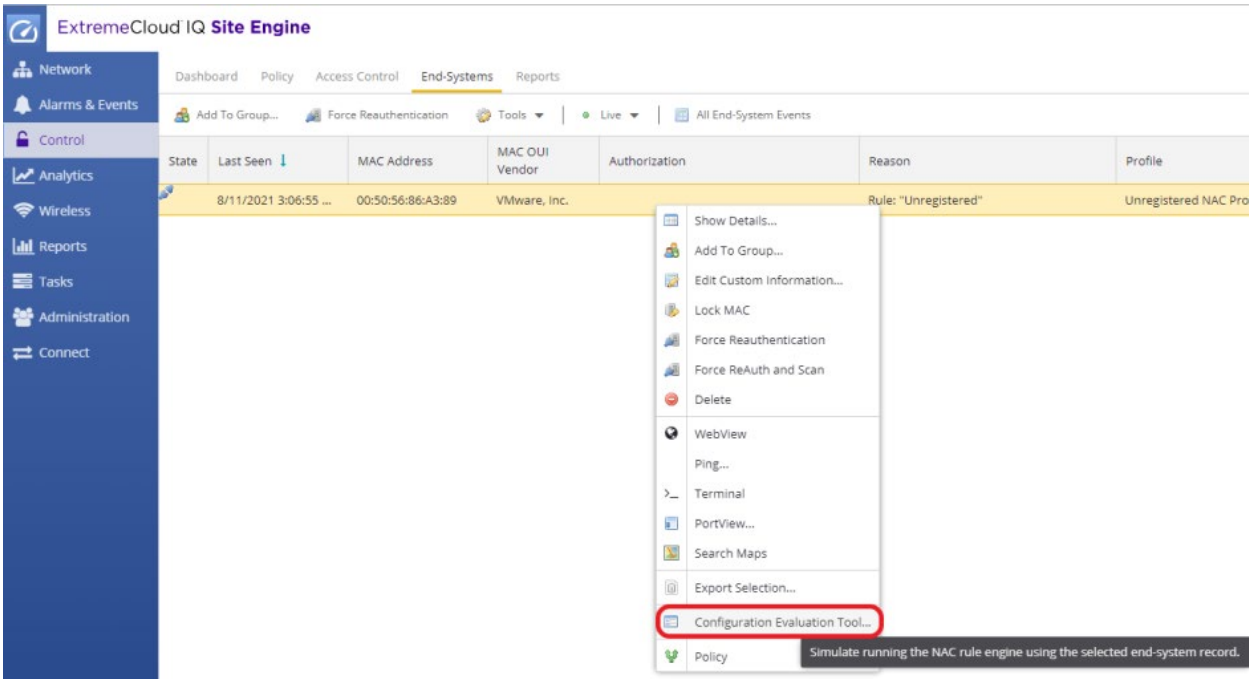
Figure 54 – Rule Example with User Group condition

Additional conditions can also be added to the rule depending on the use-case. After the rule is created, be sure to enforce this configuration to Access Control Engine(s).

Step 8: Verify - Client Testing

Clients that are attached to the Cisco switch with 802.1X supplicants properly configured will be 802.1X authenticated. When the user authenticates with the appropriate user credentials that belong to the Contractors OU in the Active Directory, the Rule Engine will process the authentication request. The rule that has all conditions “True” (conditions are logically “AND”ed) will be selected, and the respective profile will be applied.

If for some reason the desired rule and profile are not applied, a helpful tool to troubleshoot the rule engine settings is the **Configuration Evaluation Tool.** The tool can be accessed directly from the End-Systems tab by right clicking on the end-system in question as shown in Figure 55.

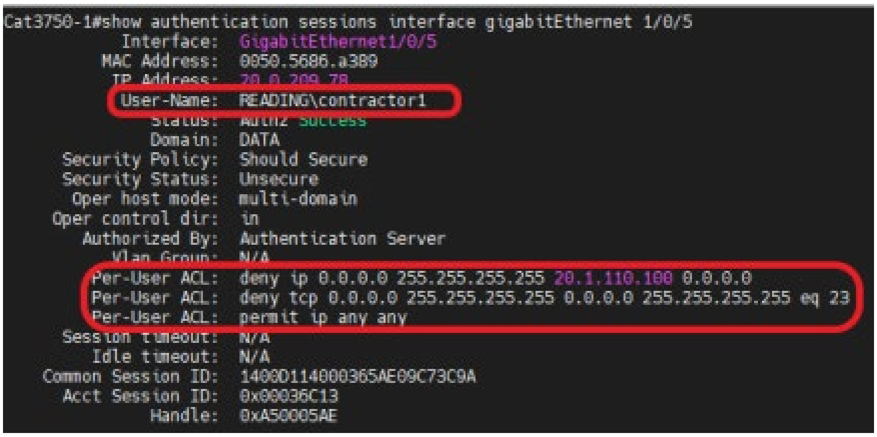


State	Last Seen	MAC Address	MAC OUI Vendor	Authorization	Reason	Profile
	8/11/2021 3:06:55 ...	00:50:56:86:A3:89	VMware, Inc.		Rule: "Unregistered"	Unregistered NAC Pro

Simulate running the NAC rule engine using the selected end-system record.

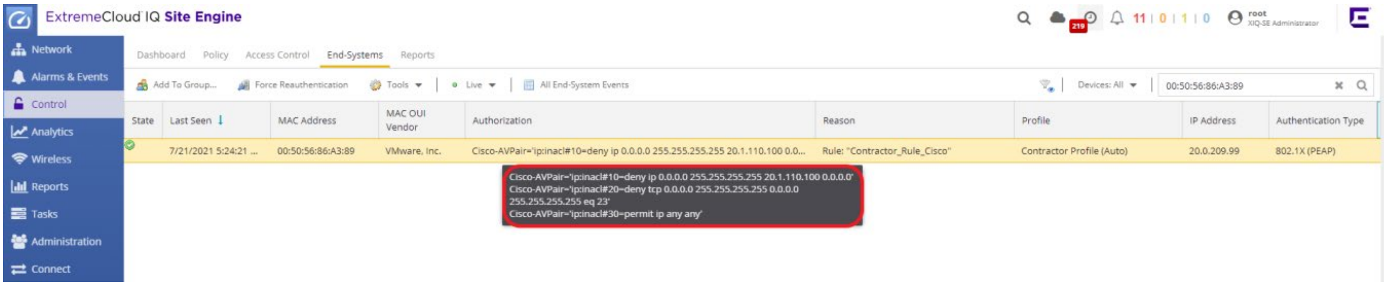
Figure 55 – Configuration Evaluation Tool

The profile can be verified on the Cisco switch by issuing the command **show authentication sessions interface <interface>**.



```
Cat3750-1#show authentication sessions interface gigabitEthernet 1/0/5
            Interface:  GigabitEthernet1/0/5
          MAC Address:  0050.5686.a389
           IP Address:  20.0.209.78
            User-Name:  READING\contractor1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  in
        Authorized By:  Authentication Server
           Vlan Group:  N/A
         Per-User ACL:  deny ip 0.0.0.0 255.255.255.255 20.1.110.100 0.0.0.0
         Per-User ACL:  deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 23
         Per-User ACL:  permit ip any any
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  1400D114000365AE09C73C9A
      Acct Session ID:  0x00036C13
               Handle:  0xA50005AE
```

Figure 56 – Verifying downloadable ACLs from the Cisco CLI



00:50:56:86:A3:89

State	Last Seen	MAC Address	MAC OUI Vendor	Authorization	Reason	Profile	IP Address	Authentication Type
✓	7/21/2021 5:24:21 ...	00:50:56:86:A3:89	VMware, Inc.	Cisco-AVPair='ip:inacl#10=deny ip 0.0.0.0 255.255.255.255 20.1.110.100 0.0...	Rule: "Contractor_Rule_Cisco"	Contractor Profile (Auto)	20.0.209.99	802.1X (PEAP)

```
Cisco-AVPair='ip:inacl#10=deny ip 0.0.0.0 255.255.255.255 20.1.110.100 0.0.0.0'
Cisco-AVPair='ip:inacl#20=deny tcp 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255 eq 23'
Cisco-AVPair='ip:inacl#30=permit ip any any'
```

Figure 57 – Verifying downloadable ACLs from the End-Systems table in Access Control

Appendix A – Troubleshooting

When troubleshooting a Cisco switch, a few commands are useful to verify specifics related to client sessions.

```
show authentication sessions interface <interface>
```

This command is the most useful on the switch. It shows the authentication status of the devices connected to a specific port.

Utilizing this command with Web Redirection yields results similar to the example below. In particular, note the URL Redirect and URL Redirect ACL fields as these are assigned by the Access Control Engine.

```
Table1-Cisco#show authentication sessions interface GigabitEthernet 1/0/8
            Interface:  GigabitEthernet1/0/8
          MAC Address:  0050.5692.5807
           IP Address:  10.201.20.201
            User-Name:  005056925807
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  in
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
         URL Redirect:  http://10.220.1.101/static/index.jsp
     URL Redirect ACL:  Unregistered
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0AC90A650000001D17877321
      Acct Session ID:  0x00000027
               Handle:  0xD500001E

Runnable methods list:
       Method   State
       mab      Authc Success
```

When URL Redirect is not in use, the command produces a response similar to the following. Note that the **Filter-ID** field is utilized in this example and represents the ACL assigned to the client.

```
Table1-Cisco#show authentication sessions interface GigabitEthernet 1/0/8
            Interface:  GigabitEthernet1/0/8
          MAC Address:  0050.5692.5807
           IP Address:  10.201.20.201
            User-Name:  005056925807
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  in
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
            Filter-Id:  GuestAccess
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0AC90A650000001D17877321
      Acct Session ID:  0x00000027
               Handle:  0xD500001E

Runnable methods list:
       Method   State
       mab      Authc Success
```

Additionally, note that the **Domain** will either be VOICE or DATA depending on whether the voice attribute was used. For more information, see Appendix B.

The following commands can be used to enable debug logging on the switch.

```
debug radius authentication

debug dot1x all
debug dot1x events
debug dot1x errors

debug epm all

debug authentication all
```

The following command can be used to verify the statically or dynamically assigned port VLAN.

```
show interfaces GigabitEthernet1/0/10 switchport
```

Appendix B – Considerations for VoIP Connections

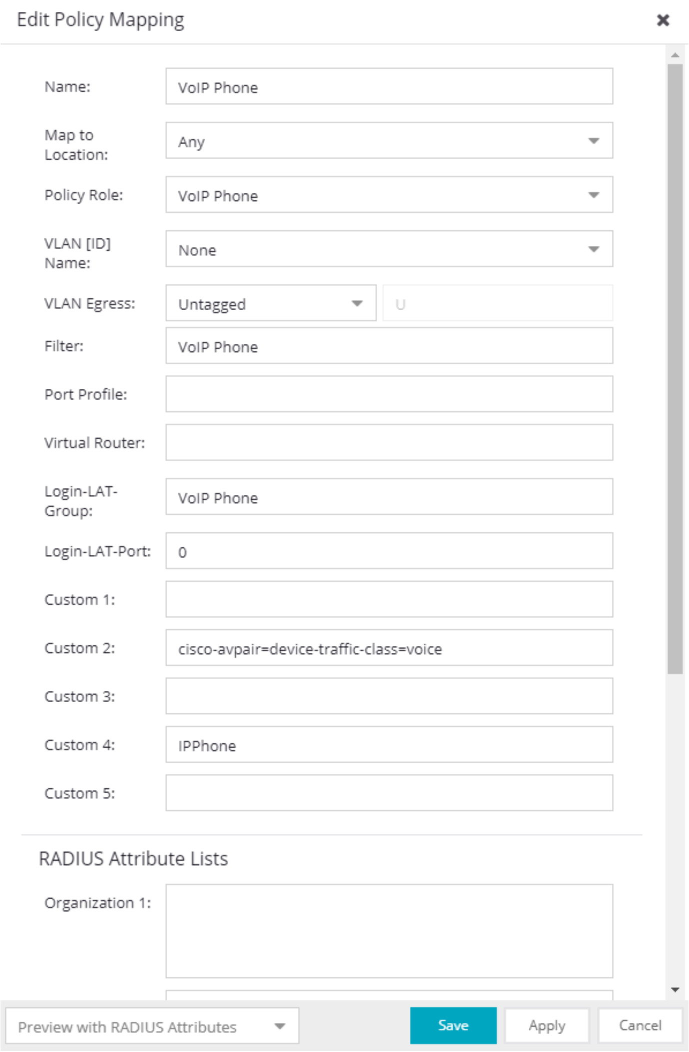
When an IP Phone is connected to a Cisco switch port that has Access Control enabled, some considerations need to be made. The first is that the IP Phone should be defined in an End System group within Access Control and have a Profile and Policy assigned specifically to it. Furthermore, an ACL should be created for the IP Phone. Lastly, in the switch configuration, each interface that could have a phone connection should have the following command that substitutes the Voice VLAN appropriately:

```
switchport voice vlan 40
```

With that command on the interface, configure Access Control to send back the following attributes in either the Custom 2 or Custom 3 column in addition to any ACL that will be assigned in Column 4:

cisco-avpair=device-traffic-class=voice

The Policy mapping should be similar to this:



Edit Policy Mapping

Name:	VoIP Phone
Map to Location:	Any
Policy Role:	VoIP Phone
VLAN [ID] Name:	None
VLAN Egress:	Untagged U
Filter:	VoIP Phone
Port Profile:	
Virtual Router:	
Login-LAT-Group:	VoIP Phone
Login-LAT-Port:	0
Custom 1:	
Custom 2:	cisco-avpair=device-traffic-class=voice
Custom 3:	
Custom 4:	IPPhone
Custom 5:	

RADIUS Attribute Lists

Organization 1:

Figure 58 – VoIP Phone policy mapping

Appendix C – IP Resolution Options

DHCP Snooping

Typical IP Resolution for Cisco switches is done when a DHCP message is discovered via DHCP Relay snooping. However, sometimes this can be expedited by configuring DHCP snooping on the Cisco switch. There have been problems in the past with DHCP snooping not working properly, so if an end system is not getting an IP even though it should be, the first thing that should be removed is DHCP snooping.

To enable DHCP snooping on the Cisco switch, it must be first enabled on all VLANs where snooping is required. Additionally, snooping must be enabled globally.

```
ip dhcp snooping vlan 3-4,40,52,98
ip dhcp snooping
```

Once snooping is added globally, add the following command for the uplink port where the DHCP server messages will be coming from.

```
ip dhcp snooping trust
```

The DHCP snooping configuration can be shown with the command:

```
show ip dhcp snooping
```

The DHCP snooping binding table can be shown with the command:

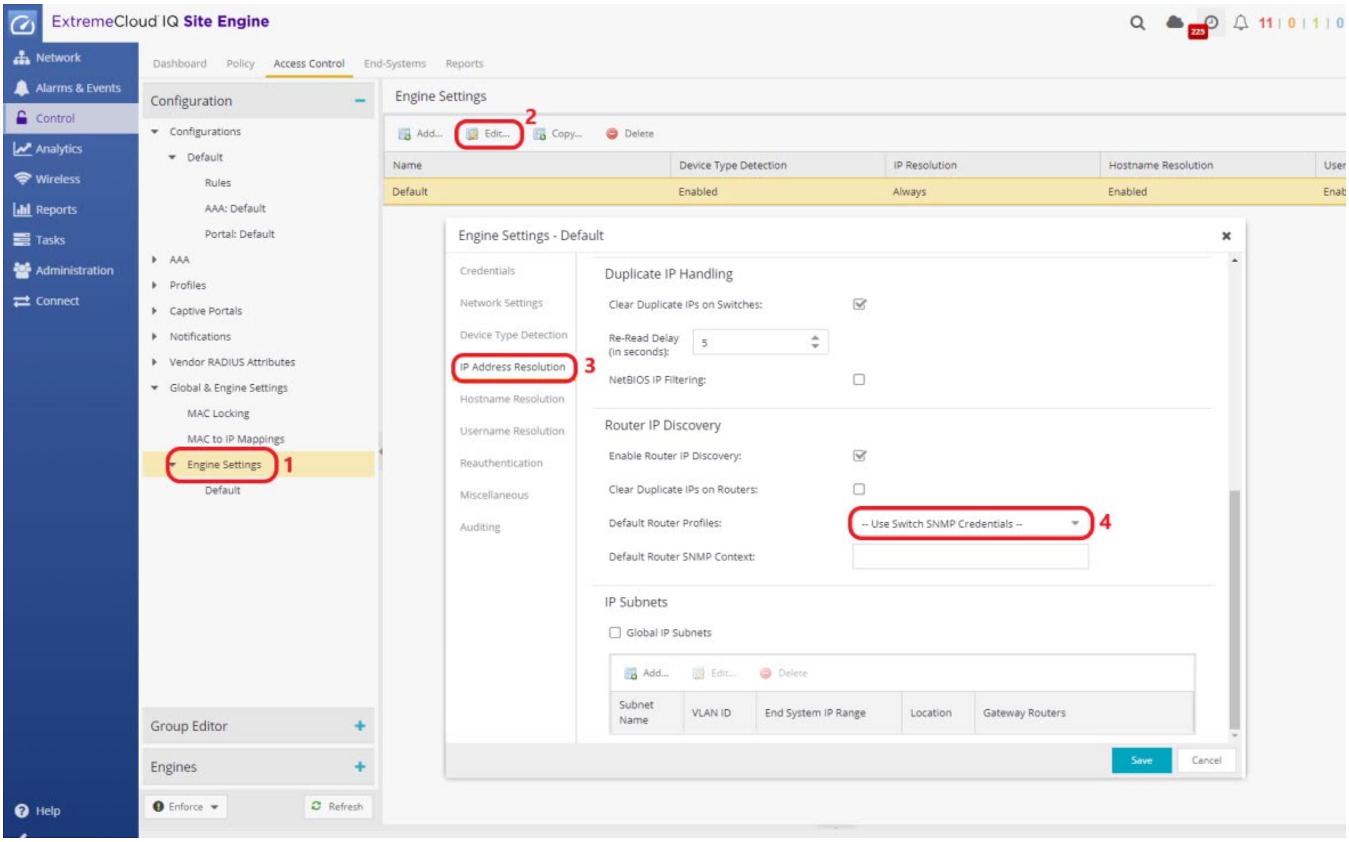
```
show ip dhcp snooping binding
```

Router Lookups

In the cases where IP Resolution is failing, router lookups might be necessary for Access Control to ensure proper IP Resolution. For this to work properly, it is highly recommended that SNMPv3 read-only credentials are configured on the edge routers through which the clients connect. With these credentials configured, Access Control can be set to do an SNMP lookup of the ARP cache to find possible IP to MAC address bindings.

To configure this, navigate to **Engine Settings** under **Global & Engine Settings** and select **Edit** as shown in Figure 59. On the **IP Resolution** tab, select the appropriate SNMP Profile for the router. If one is not already created, create a set of SNMP credentials in Management Center that can be used with the router. If the switch and router(s) share the same SNMP credentials, this step can be skipped as the default action is to use the same SNMP credentials as the switch.

> NOTE
>
> It is highly recommended that SNMPv3 be used instead of SNMPv1 or v2. SNMP v3 provides a much higher level of security and efficiency.



Name	Device Type Detection	IP Resolution	Hostname Resolution	User
Default	Enabled	Always	Enabled	Enab

Duplicate IP Handling

Clear Duplicate IPs on Switches: ☑

Re-Read Delay (in seconds): 5

NetBIOS IP Filtering: □

Router IP Discovery

Enable Router IP Discovery: ☑

Clear Duplicate IPs on Routers: □

Default Router Profiles: -- Use Switch SNMP Credentials --

Default Router SNMP Context:

IP Subnets

□ Global IP Subnets

Subnet Name	VLAN ID	End System IP Range	Location	Gateway Routers

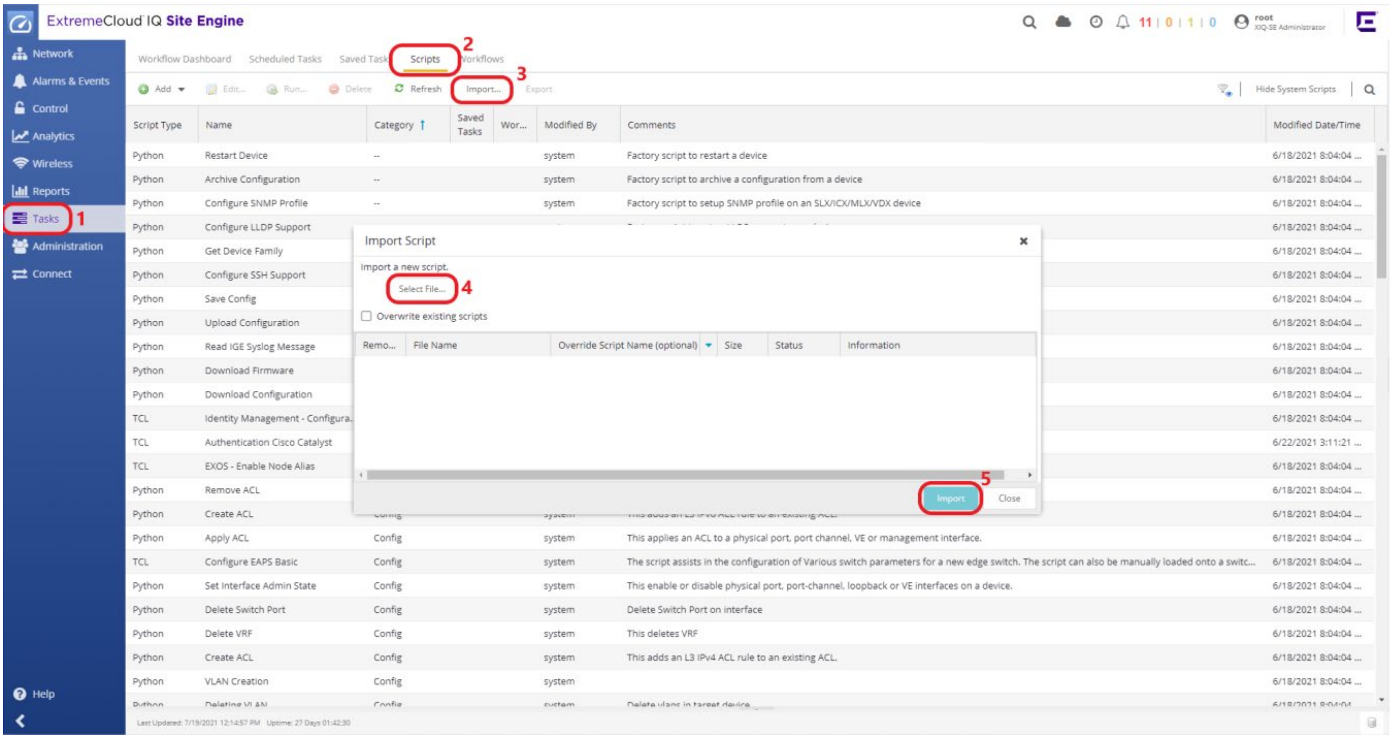
Figure 59 – IP address resolution settings

Appendix D – ExtremeCloud IQ - Site Engine Add-On Script

The scripting feature can be utilized to automate the authentication related configuration of Cisco switches after they are onboarded to ExtremeCloud IQ - Site Engine. Community developed scripts are available on GitHub for this specific purpose.

Name	Type	GitHub URL
Authentication Catalyst	TCL Script	https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_CLI_scripts/xml
Authentication Catalyst - unconfigure	TCL Script	https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_CLI_scripts/xml

After downloading the script from GitHub, navigate to **Tasks** and follow the steps depicted in Figure 60.



Import a new script.

☐ Overwrite existing scripts

Remo...	File Name	Override Script Name (optional)	Size	Status	Information

Script Type	Name	Category	Saved Tasks	Wor...	Modified By	Comments	Modified Date/Time
Python	Restart Device	--			system	Factory script to restart a device	6/18/2021 8:04:04 ...
Python	Archive Configuration	--			system	Factory script to archive a configuration from a device	6/18/2021 8:04:04 ...
Python	Configure SNMP Profile	--			system	Factory script to setup SNMP profile on an SLX/ICX/MLX/VDX device	6/18/2021 8:04:04 ...
Python	Configure LLDP Support						6/18/2021 8:04:04 ...
Python	Get Device Family						6/18/2021 8:04:04 ...
Python	Configure SSH Support						6/18/2021 8:04:04 ...
Python	Save Config						6/18/2021 8:04:04 ...
Python	Upload Configuration						6/18/2021 8:04:04 ...
Python	Read IGE Syslog Message						6/18/2021 8:04:04 ...
Python	Download Firmware						6/18/2021 8:04:04 ...
Python	Download Configuration						6/18/2021 8:04:04 ...
TCL	Identity Management - Configura...						6/18/2021 8:04:04 ...
TCL	Authentication Cisco Catalyst						6/22/2021 3:11:21 ...
TCL	EXOS - Enable Node Alias						6/18/2021 8:04:04 ...
Python	Remove ACL						6/18/2021 8:04:04 ...
Python	Create ACL						6/18/2021 8:04:04 ...
Python	Apply ACL	Config			system	This applies an ACL to a physical port, port channel, VE or management interface.	6/18/2021 8:04:04 ...
TCL	Configure EAPS Basic	Config			system	The script assists in the configuration of Various switch parameters for a new edge switch. The script can also be manually loaded onto a switc...	6/18/2021 8:04:04 ...
Python	Set Interface Admin State	Config			system	This enable or disable physical port, port-channel, loopback or VE interfaces on a device.	6/18/2021 8:04:04 ...
Python	Delete Switch Port	Config			system	Delete Switch Port on interface	6/18/2021 8:04:04 ...
Python	Delete VRF	Config			system	This deletes VRF	6/18/2021 8:04:04 ...
Python	Create ACL	Config			system	This adds an L3 IPv4 ACL rule to an existing ACL.	6/18/2021 8:04:04 ...
Python	VLAN Creation	Config			system		6/18/2021 8:04:04 ...
Python	Deleting VLAN	Config			system	Delete vlans in target device	6/18/2021 8:04:04

Last Updated: 7/19/2021 12:14:57 PM Uptime: 27 Days 01:42:30

Figure 60 – How to import a script to ExtremeCloud IQ - Site Engine

Terms and Conditions of Use

Extreme Networks, Inc. reserves all rights to its materials and the content of the materials. No material provided by Extreme Networks, Inc. to a Partner (or Customer, etc.) may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, or incorporated into any other published work, except for internal use by the Partner and except as may be expressly permitted in writing by Extreme Networks, Inc.

This document and the information contained herein are intended solely for informational use. Extreme Networks, Inc. makes no representations or warranties of any kind, whether expressed or implied, with respect to this information and assumes no responsibility for its accuracy or completeness. Extreme Networks, Inc. hereby disclaims all liability and warranty for any information contained herein and all the material and information herein exists to be used only on an "as is" basis. More specific information may be available on request. By your review and/or use of the information contained herein, you expressly release Extreme from any and all liability related in any way to this information. A copy of the text of this section is an uncontrolled copy, and may lack important information or contain factual errors. All information herein is Copyright © Extreme Networks, Inc. All rights reserved. All information contain in this document is subject to change without notice.

For additional information refer to: http://www.extremenetworks.com/company/legal/terms/