ExtremeCloud IQ - Site Engine and ExtremeControl – VOSS/Fabric Engine Downloadable ACL Guide

Abstract: This document details the utilization of a VOSS or Fabric Engine switch as an edge enforcement point in ExtremeControl using Downloadable ACLs (also known as Per-User ACLs) as an enforcement method.

Part Number: 9037358-00 Rev AB

Published: March 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
OOB	Out of Band
VOSS	VSP Operating System
VSA	Vendor Specific Attribute
ZTP+	Zero Touch Provisioning Plus

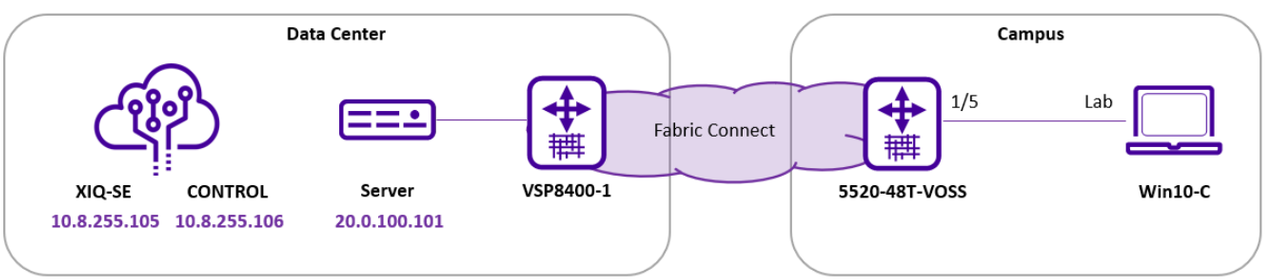
Test Environment

Testing was performed on the following software and hardware models and versions.

- ExtremeCloud IQ - Site Engine (Site Engine) version 21.11.10.57
- ExtremeControl for ExtremeCloud IQ Site Engine version 21.11.10.57
- 5520-48T (VOSS) version 8.4.2.0

Topology

The testing topology can be found below.



Overview

Objective

This guide describes how to deploy a VOSS/Fabric Engine switch as an edge enforcement point in ExtremeControl using Downloadable ACLs (also referred as Per-User ACLs). In particular, the guide focuses on the following tasks:

- How to prepare and construct a policy domain for VOSS/Fabric Engine switches
- How to prepare Access Control settings for the VOSS/Fabric Engine Downloadable ACL method
- How to add a VOSS/Fabric Engine switch to the ExtremeCloud IQ - Site Engine database via Zero Touch Provisioning Plus (ZTP+)
- Verification and troubleshooting

When a VOSS/Fabric Engine switch is deployed at the access layer of the network, it is most commonly done using a Fabric to the Edge topology. The steps needed to deploy a VOSS/Fabric Engine switch in a Fabric to the Edge scenario using Zero Touch Fabric and ExtremeCloud IQ - Site Engine onboarding automation are outside the scope of this guide.

Policy and Downloadable ACLs

A Downloadable ACL is an Access Control List that is created and stored in the RADIUS Server, which in this scenario is ExtremeControl. The Network Access Server device (NAS), which in this case is the VOSS/Fabric Engine switch, does not save any preconfigured ACLs in the running configuration. Downloadable ACLs are dynamically installed on the switch upon successful authentication as part of the RADIUS Access-Accept message. A Downloadable ACL action can assign different ACLs for each user session.

The Policy tab in 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 ExtremeCloud IQ - Site Engine version 21.9.10.90 extends this functionality to VOSS/Fabric Engine 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 Extreme wireless and EXOS based switches is to write the policy rules and roles via SNMP or REST API calls so that they exist locally on the device. This new method does not write the ACLs to switch itself; rather, the ACLs are saved in the local database on the Access Control Engine. Therefore, when an enforce is done, a VOSS/Fabric Engine switch will have the policy converted automatically to a Downloadable ACL that is saved in the database.

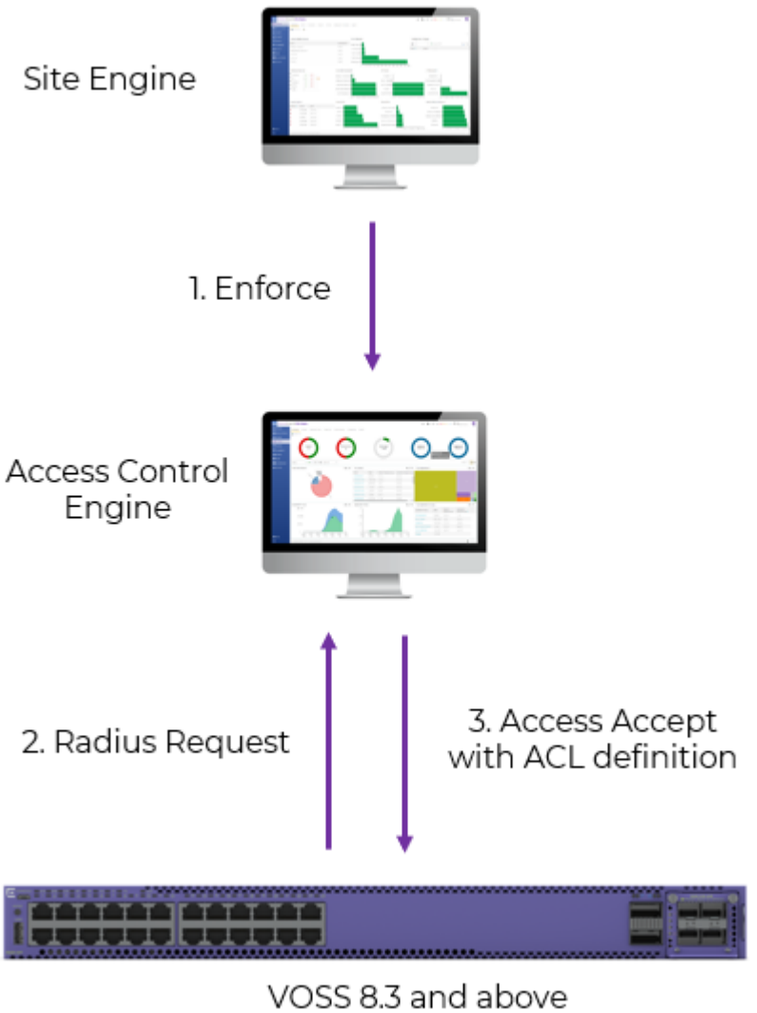


Figure 1 – Policy enforcement with VOSS/Fabric Engine switches

Upon enforcement of the policy domain, the exact ACLs to be assigned can be reviewed in the Enforce Preview screen as shown in Figure 2.

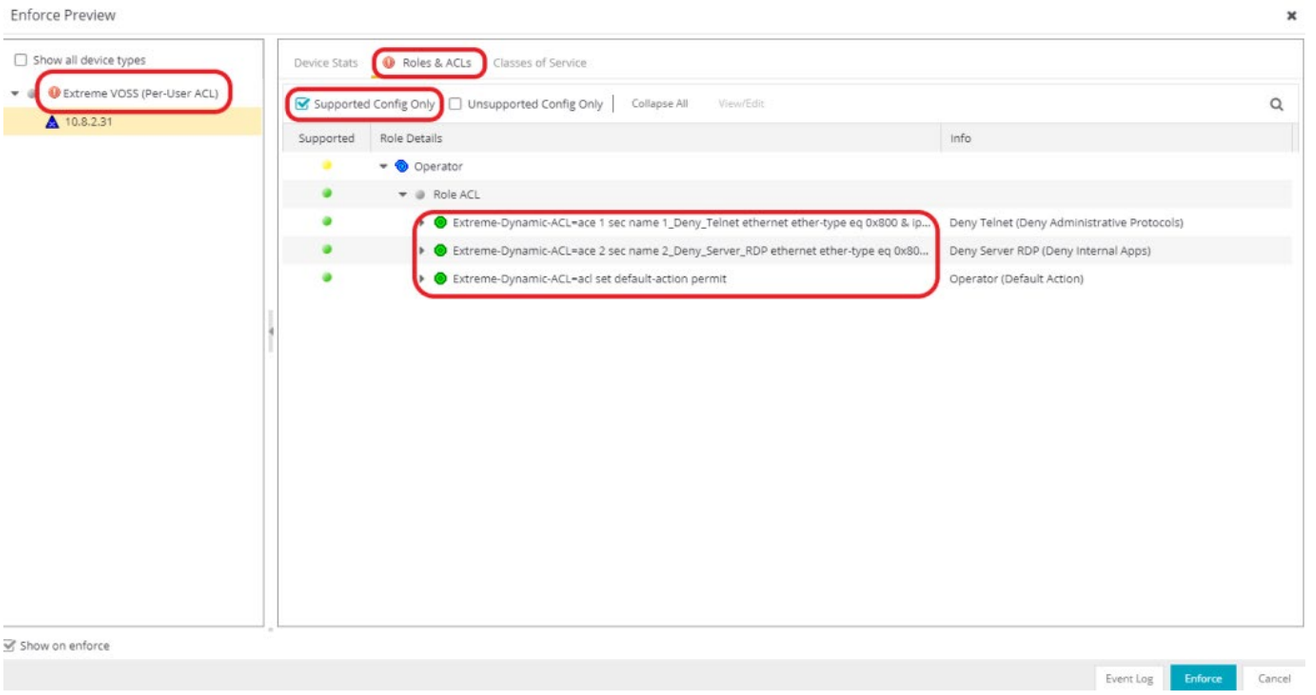


Figure 2 – How to visualize VOSS/Fabric Engine Downloadable ACLs during Policy Enforce

NOTE
The Role ACLs tab appears in the UI only after a VOSS/Fabric Engine switch has been added to the policy domain.

When a device authenticates to Access Control and Downloadable ACLs are configured to be returned to the authenticated session, the appropriate RADIUS attributes are included. These RADIUS attributes specify the ACLs to assign to the authenticated session.

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 outcome you would like. In this case, the ordering of the Downloadable ACLs can be re-arranged during assignment. This is accomplished by following the steps shown in Figure 3, using the “Move Up” or “Move Down” options to arrange the rules as desired.

NOTE
The Rule Ordering view appears in the UI only after a VOSS/Fabric Engine switch has been added to the policy domain.

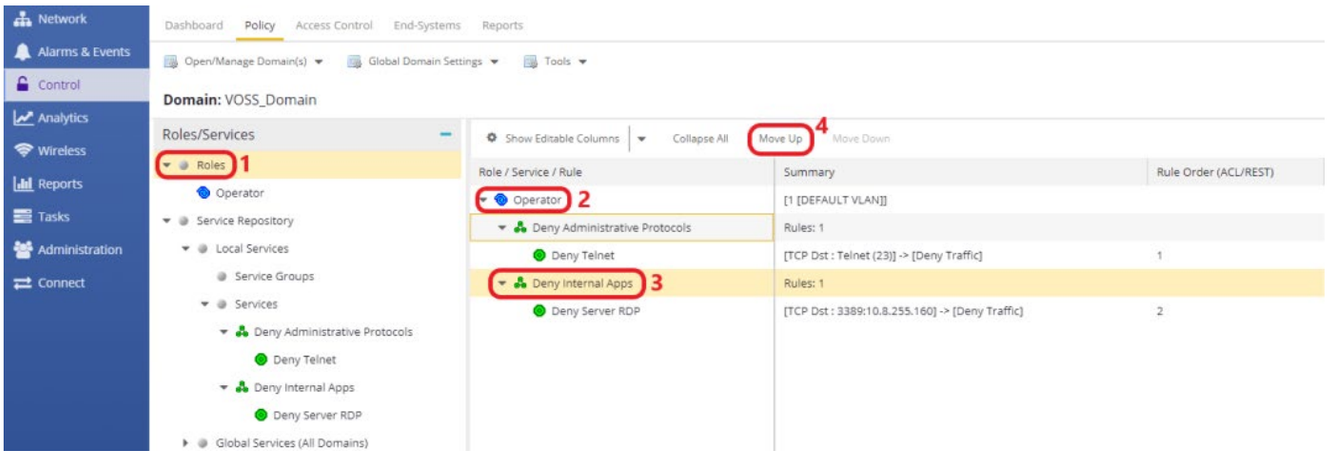


Figure 3 – How to order ACL rules within a policy domain

Policy Support

Because Extreme Policy has many features in addition to traditional ACL support, certain feature sets within Policy cannot be converted to Downloadable ACLs. The following policy match conditions are supported and work properly with VOSS/Fabric Engine.

- Ethertype
- IP Address Source and Destination
- IP Protocol Type
- IP Type of Service
- IP Fragment
- TCP Source and Destination
- UDP Source and Destination
- ICMP
- IP Socket Destination
- IP Socket Source
- Destination MAC Address

CAUTION

- Socket (IPSOCKETDEST, IPSOCKETSOURCE) are translated into two rules, one for UDP and one for TCP.
- Range (IPUDPPORTDESTRANGE, IPTCPPORTDESTRANGE, IPTCPPORTSOURCERANGE, IPUDPPORTSOURCERANGE) are translated to more rules with MASK.
- Hierarchical (Filtering Rules) and ACL mode (Access Control Entries) are supported.
- Bilateral (IPTCPPORTBILAT, IPUDPPORTBILAT, IPADDRESSBILAT) are not supported in the tested release of ExtremeCloud IQ - Site Engine.

Supported Platforms

The following hardware platforms support Downloadable ACLs that work in conjunction with ExtremeCloud IQ - Site Engine Policy. All Fabric Engine versions support Downloadable ACL. The minimum VOSS version to support Downloadable ACLs is 8.3.

- Universal Switching (VOSS and Fabric Engine)
- VSP 4450 Series (VOSS only)
- VSP 4900 Series (VOSS only)
- VSP 7200 Series (VOSS only)
- VSP 7400 Series (VOSS only)
- VSP 8000 Series (VOSS only)

ExtremeCloud IQ - Site Engine Preparation for VOSS/Fabric Engine Downloadable ACL Method

Policy Domain Preparation

Step 1: Create a Policy Domain

Navigate to Control and then Policy and follow the steps illustrated in Figure 4 to create a new policy domain and give the domain a name when prompted.

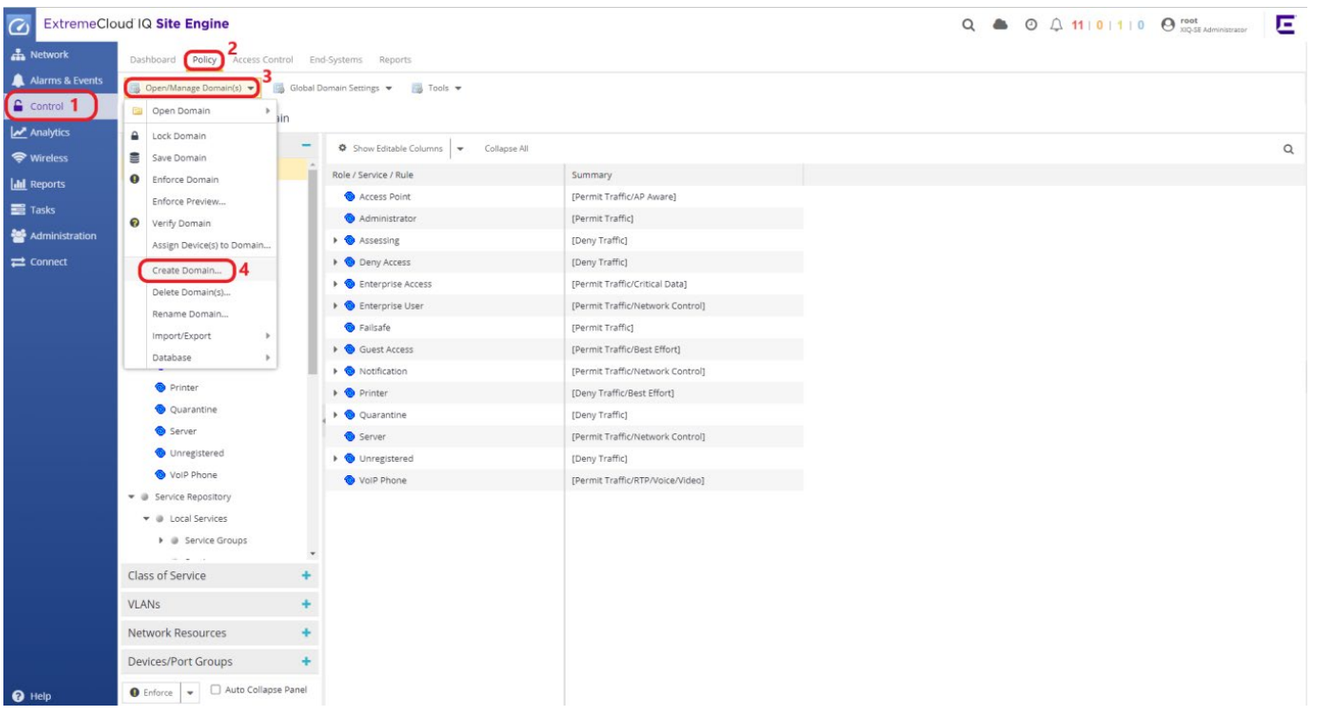


Figure 4 – How to create a new policy domain

Step 2: Set up Roles

The hierarchical Policy Framework consists of three main components: roles, services and rules. Below are the functions of each component within the Policy Framework:

- Roles are at the Business / Network level and define the job responsibility and function of individual employees or groups of employees – for example, engineering, finance, and sales.
- Services are policy containers for groups of similar rules. Grouping rules allows the network administrator to apply rules in groups rather than as individual components.
- Rules are the individual granular policies that are enforced at the port level. When a VOSS/Fabric Engine switch is used, these rules translate into Downloadable ACL entries that can be stored in Access Control and are ready to be included in the RADIUS Access-Accept messages after a successful authentication.

After you create the policy domain, either a Top-Down or a Bottom-Up approach can be followed when setting up the Policy Framework. A Top-Down approach would include creating roles which are in most

scenarios in parallel with Organizational Units in Active Directory, followed by adding services and finally rules. This guide will follow the Top-Down approach, which is illustrated in Figure 5.

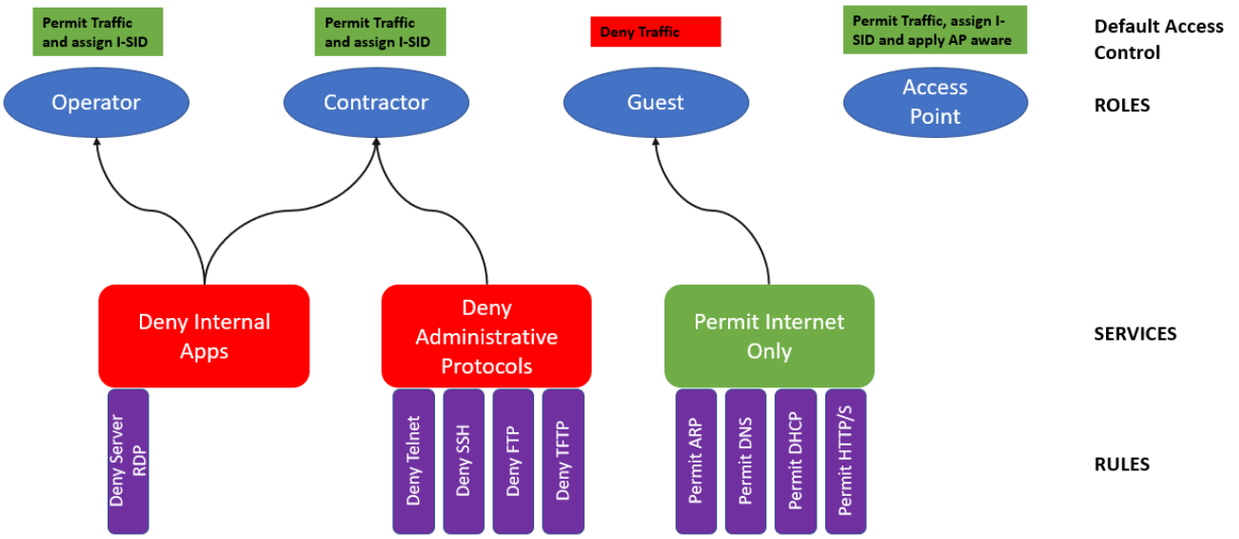


Figure 5 – Policy Framework with roles, services, and rules

Right click on Roles and create the following roles:

- Operator
- Contractor
- Guest
- Access Point

When you have created these roles, the policy domain will look like Figure 6.

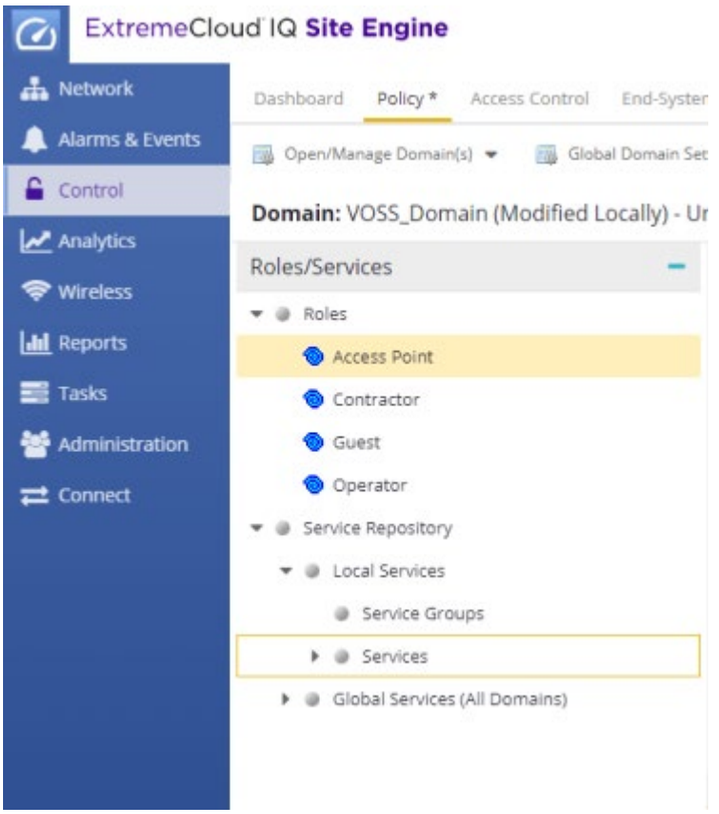


Figure 6 – Creating the roles in a policy domain

After you create each role, select the role, and expand the Default Actions on the right pane by selecting Show All. Figure 7 shows the supported Default Action fields for VOSS/Fabric Engine switches, which are also listed below.

1. Access Control: There are 3 options under Access Control
   i. Permit Traffic
   ii. Deny Traffic
   iii. Contain to VLAN

   In order to assign a Service Identifier (I-SID) value in the context of the Fabric to the Edge architecture, Contain to VLAN must be selected and the Service ID field needs to be populated accordingly. If a Service ID is defined, the following VSA is sent: *"FA-VLAN-ISID=0:ServiceID"*

CAUTION
VLAN assignment is not supported in the tested version of ExtremeCloud IQ - Site Engine.

CAUTION
VSP 4450 does not support the following EAP enhancements: EAP on Flex UNI ports, Auto-sense ports, auto-isid-offset.

NOTE

When a VOSS/Fabric Engine switch is used as an access switch in Fabric to the Edge topology, the most common scenario is when the switch acts as a DvR Leaf which does not allow Platform VLANs to be created. Therefore Flex-UNI is required for L2VSNs, which is more powerful and flexible and which does not require VLAN ID information for untagged bindings because it directly assigns I-SID to ports.

2. *AP Aware*: When AP Aware is enabled as a Default Action on a role, only the access point itself will be authenticated on that particular port and all subsequent traffic through the port will not need authentication. This setting is very useful when you want a uniform port configuration regardless of the connected end-system type. If AP Aware is enabled, the following VSA is sent: **"Extreme-Dynamic-MHSA=1".**

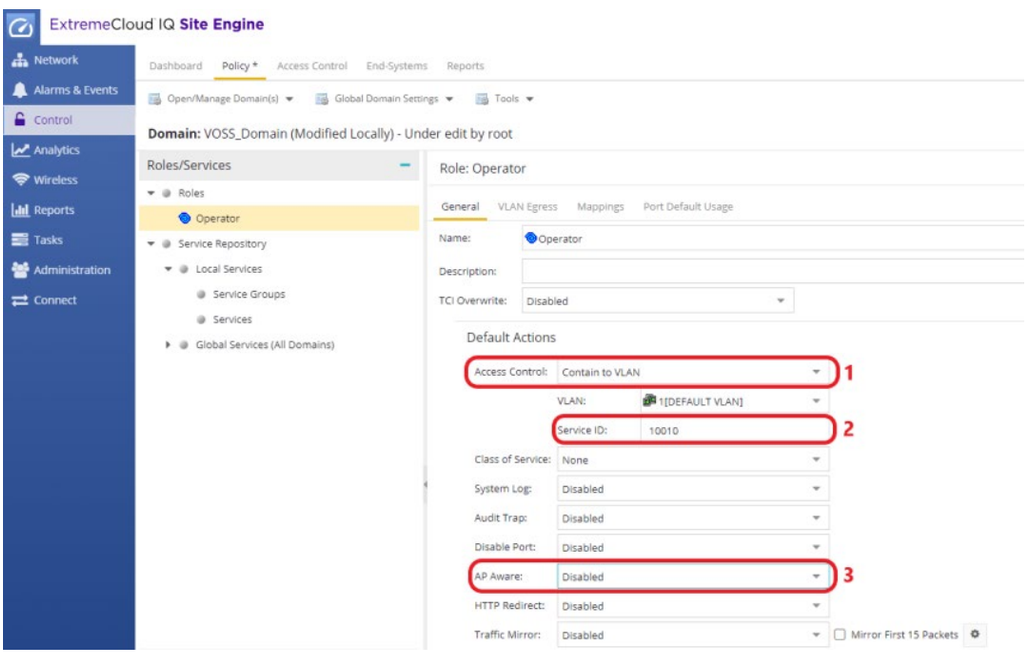


Figure 7 – Supported Default Action fields for VOSS/Fabric Engine switches

After adding the Service-IDs to each role and enabling the AP-Aware feature on the "Access Point" role, the Roles Summary looks like Figure 8.

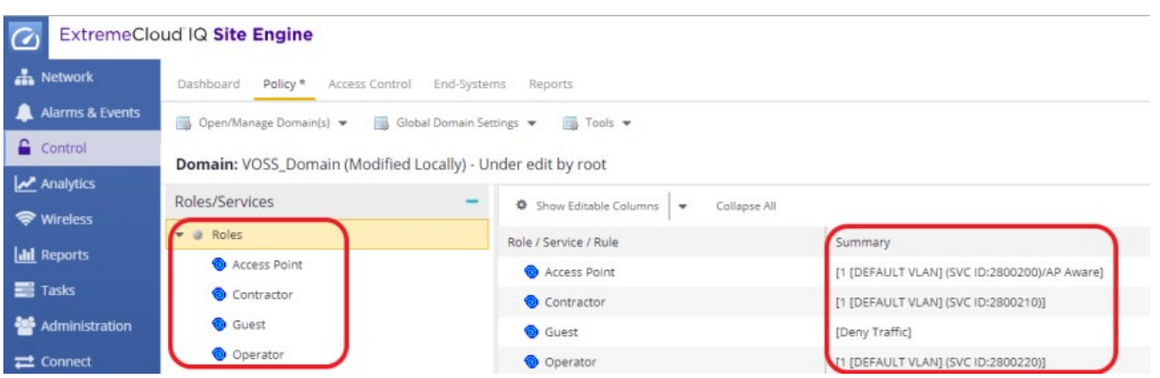


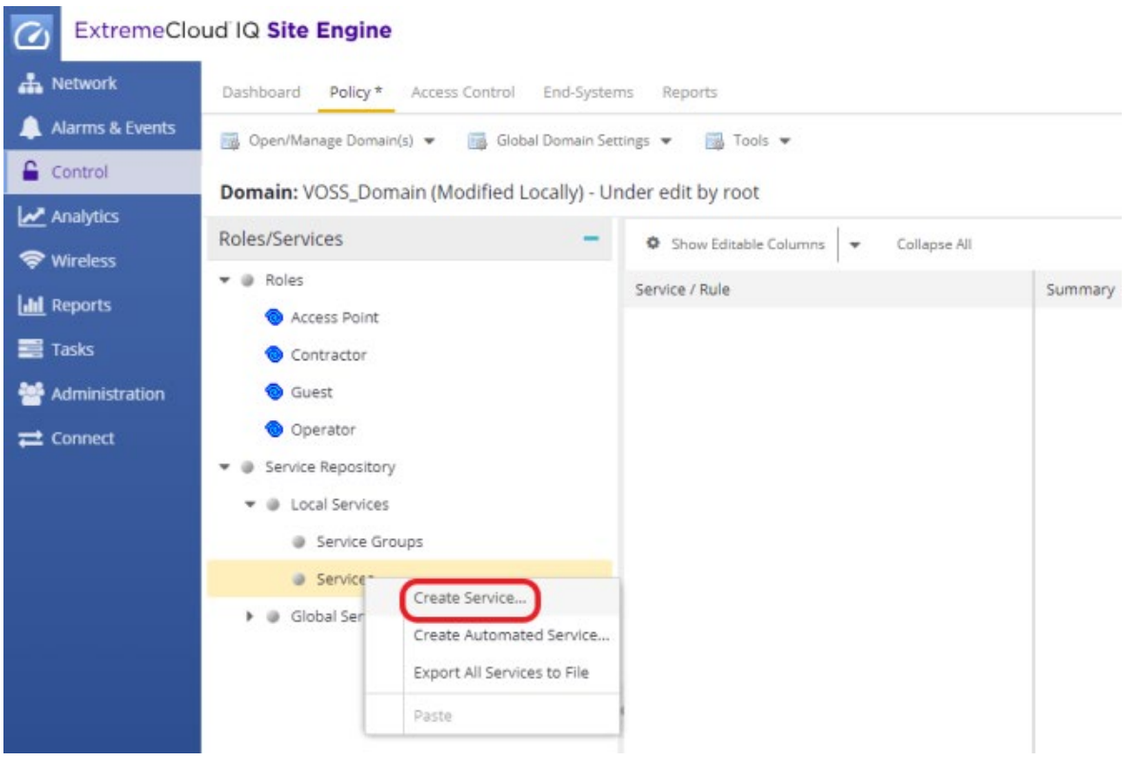
Figure 8 – Roles Summary

Step 3: Create Services

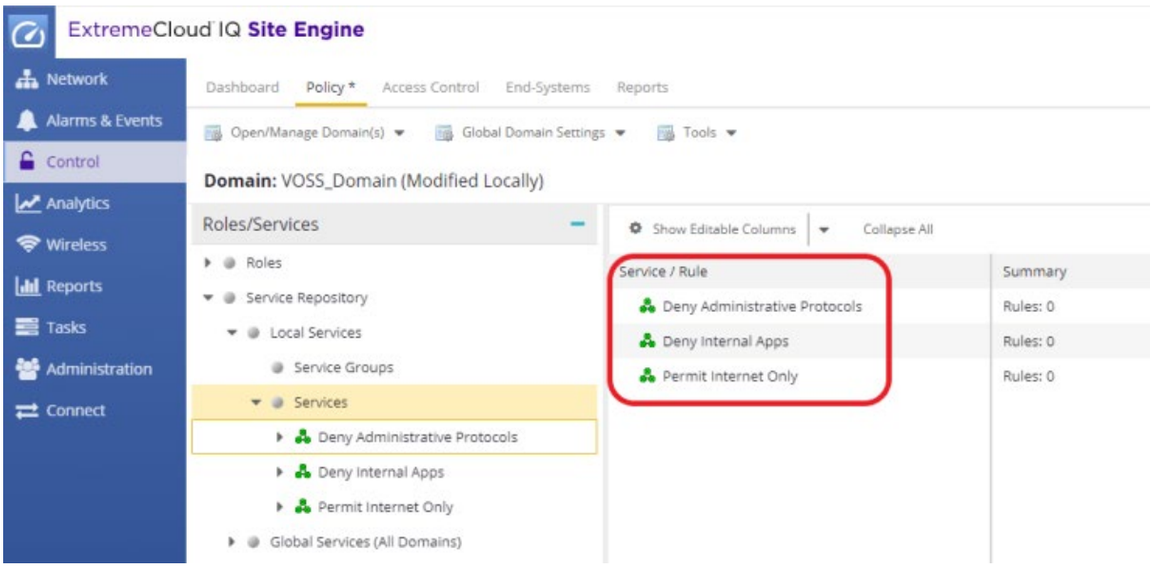
After you set up the roles, the next step is to create services. Services are containers for similar types of rules. To create a new service, expand the **Service Repository** and right click on **Services** as depicted in Figure 9. Give the service a meaningful name. The name will represent a group of rules that will be created in Step 4.

In this guide, the policy structure depicted in Figure 5 will be used; therefore the names of the services are as follows:

- Deny Internal Apps
- Deny Administrative Protocols
- Permit Internet Only

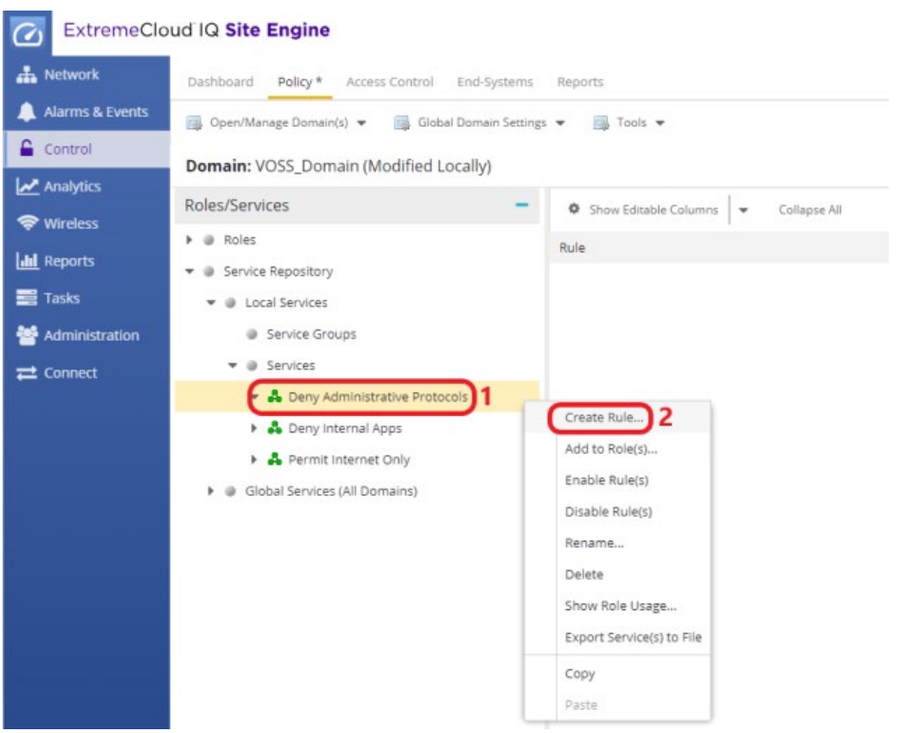


After all the services are created, the Services Summary will look like Figure 10, with no rules in them yet. Continue with Step 4 to create rules within each service.



Step 4: Create Rules

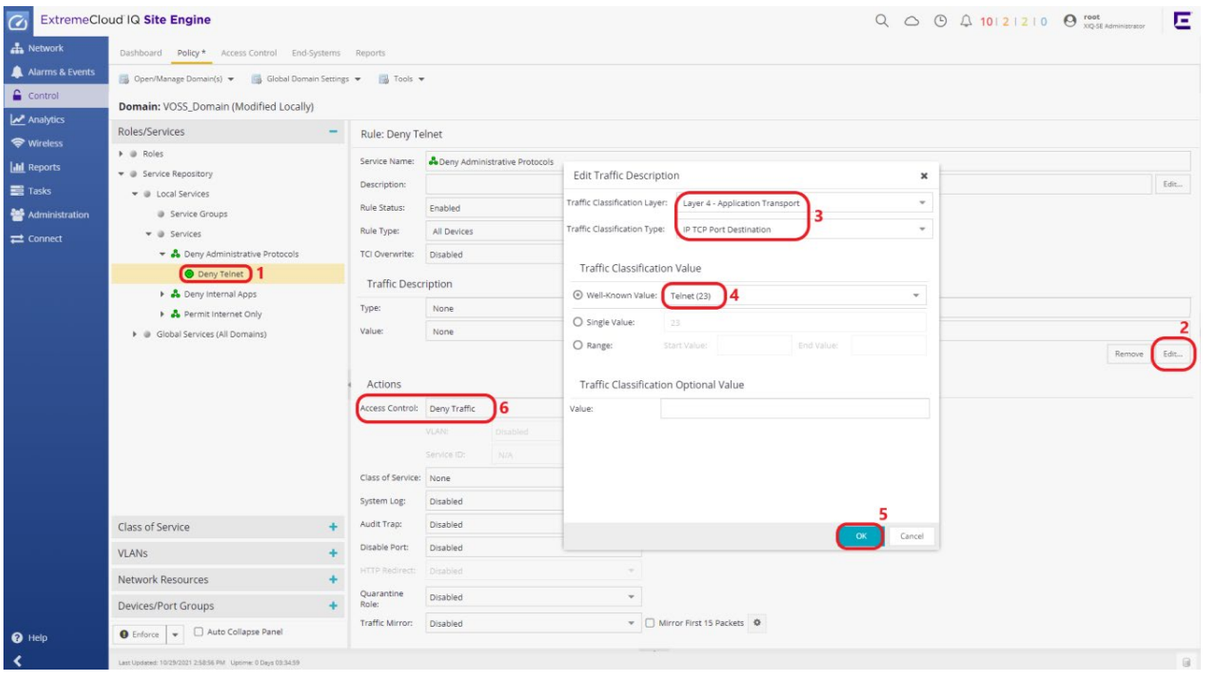
Each of the services created in Step 3 needs to be populated with rules. These rules will then be translated into Downloadable ACL entries for VOSS/Fabric Engine switches. Right click on a service and select **Create Rule** as shown in Figure 11.



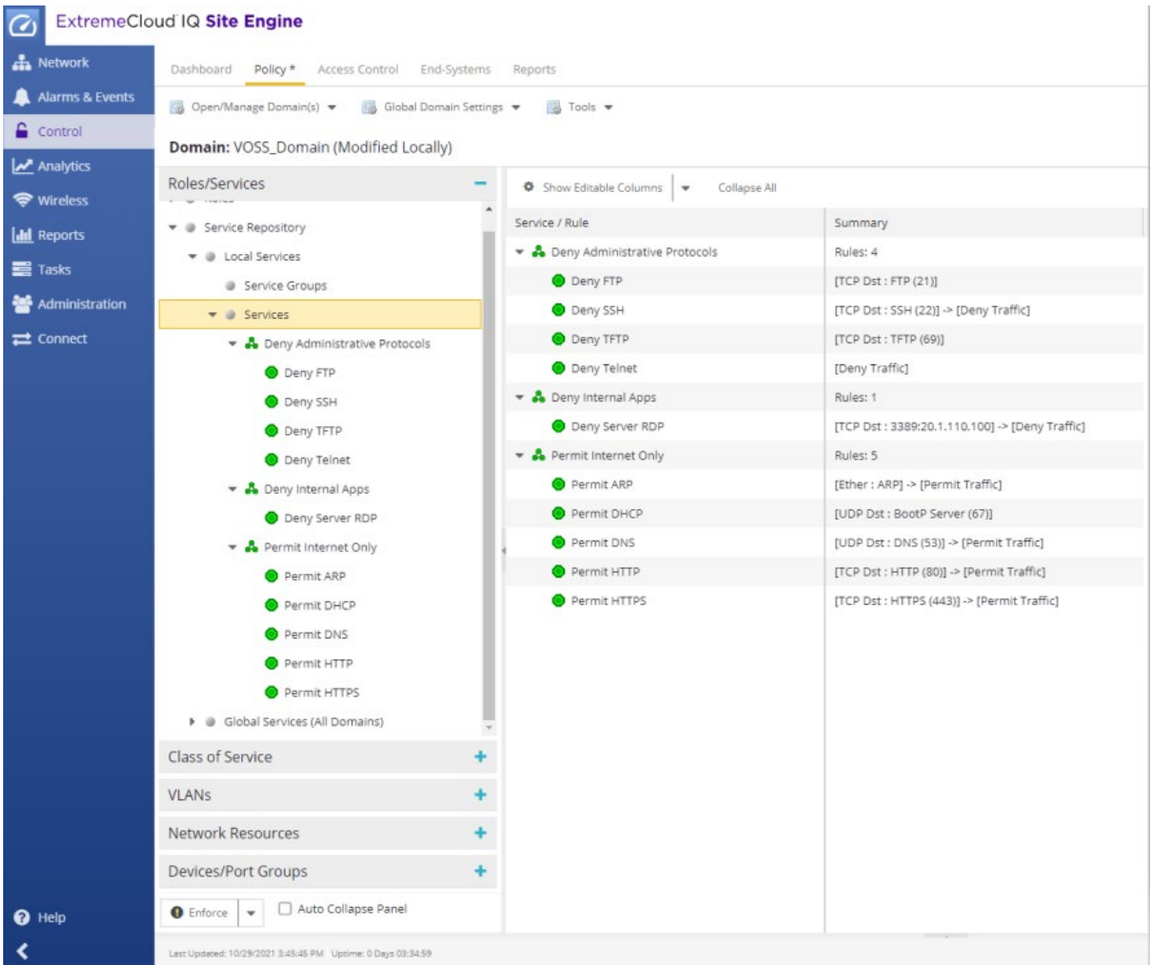
After the rule is created, two actions need to be performed for VOSS/Fabric Engine switches:

1. **Edit Traffic Description:** L2, L3 and L4 Traffic Classification Layers
2. **Access Control:** Permit or Deny

Supported traffic description types for VOSS/Fabric Engine switches can be found in the **Policy Support** section under **Overview**. As an example, Figure 12 shows a rule description that denies Telnet protocol.

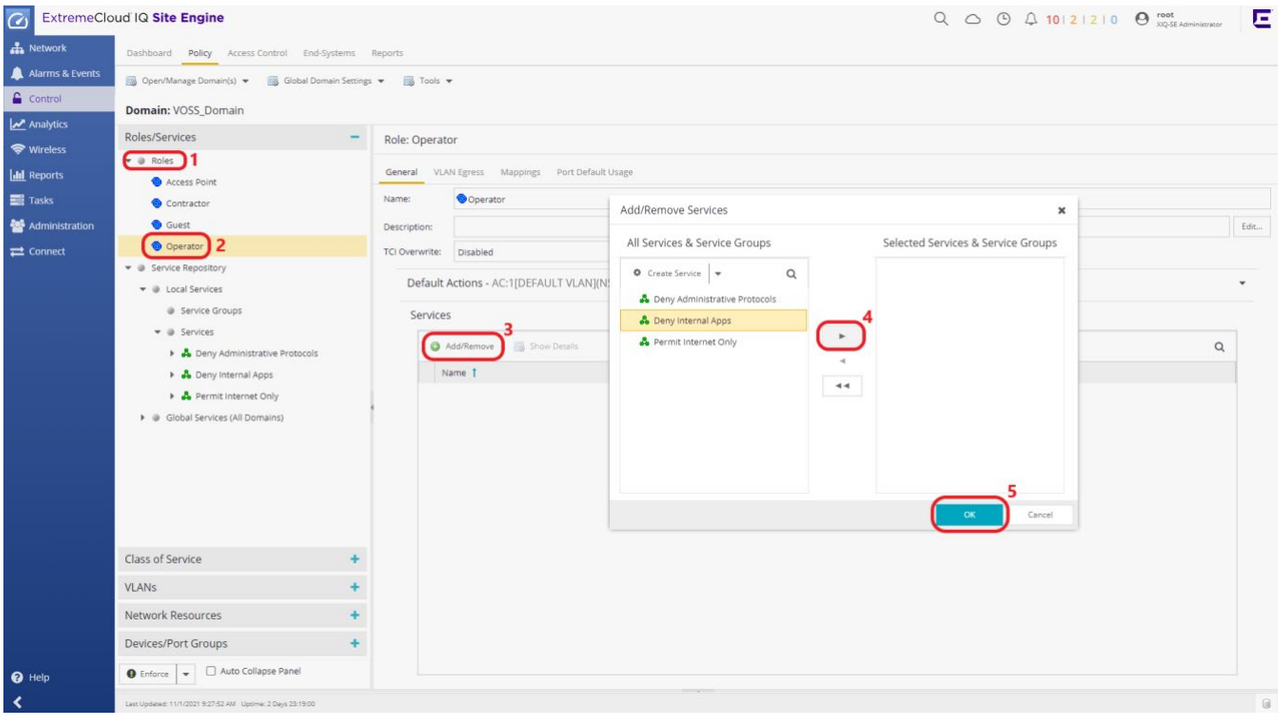


After you create all the rules for the services, the Services Summary will look like Figure 13. Rule details are listed under each respective service.

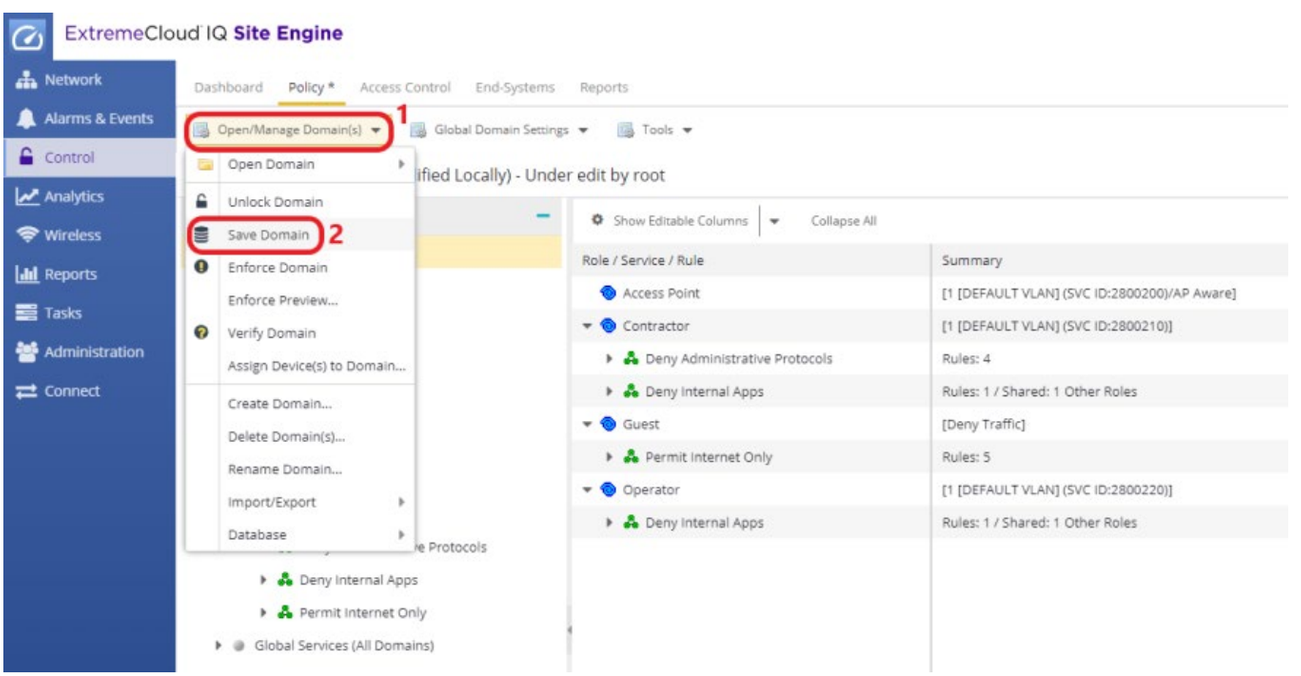


Step 5: Assign Services to Roles

The final step in policy domain preparation is to assign the services to their respective roles. To achieve this, select Roles and then Add/Remove under Services to add the desired services to the role. See Figure 14 for reference.



After all the services are assigned according to the Policy Framework in Figure 5, save the domain to the database as shown in Figure 15. The domain enforce will be done automatically after a VOSS/Fabric Engine switch is discovered, onboarded, and added to the policy domain using ZTP+. This process is detailed in the following section.



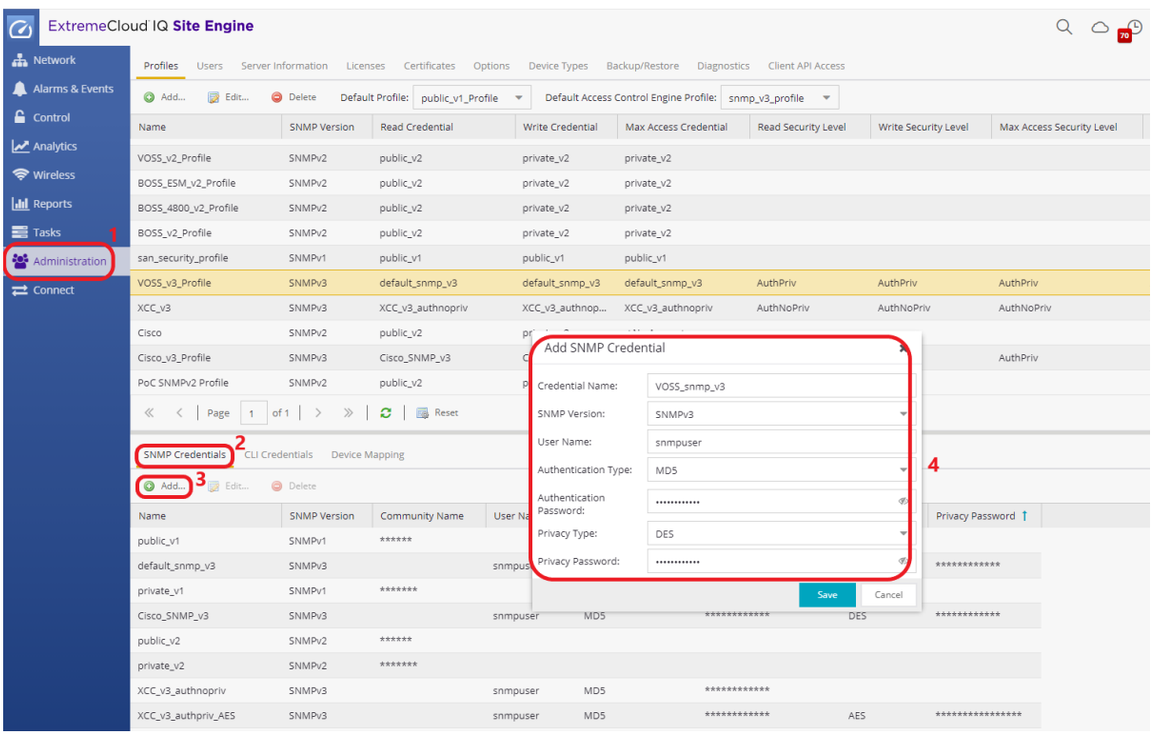
VOSS/Fabric Engine Switch Discovery

In order to manage a VOSS/Fabric Engine switch in ExtremeCloud IQ - Site Engine, the switch needs to be discovered and added to the ExtremeCloud IQ - Site Engine database. There are two ways a VOSS/Fabric Engine switch can be added to the ExtremeCloud IQ - Site Engine database. These are as follows:

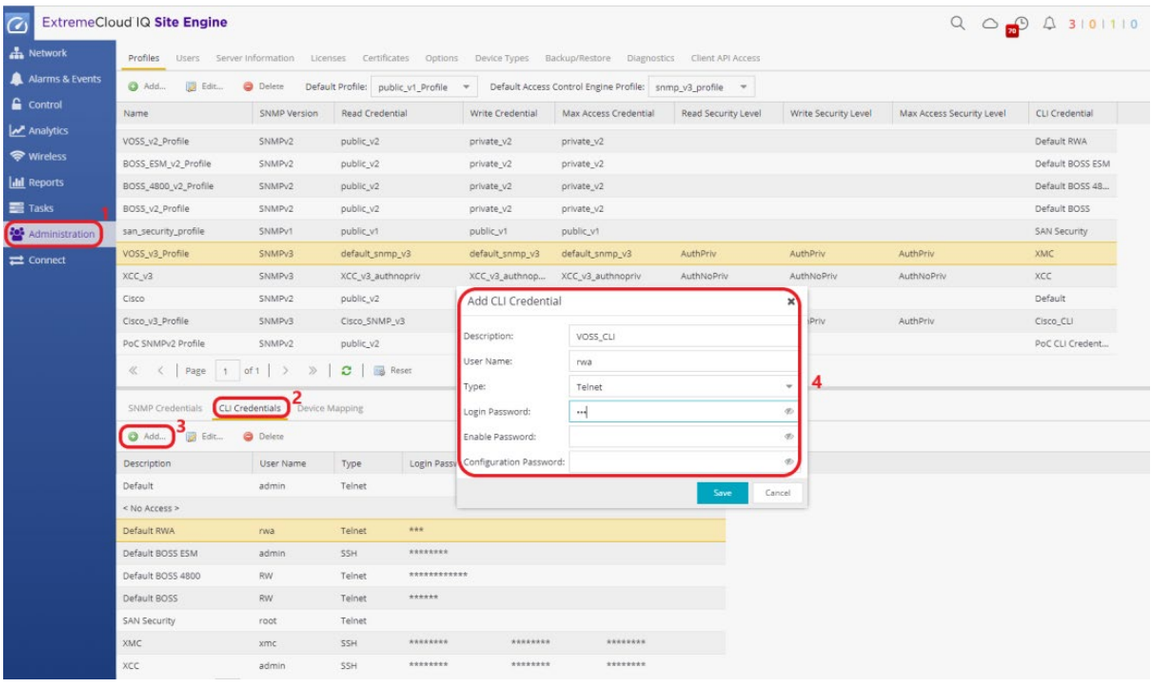
Option 1: Manual Discovery

Any Extreme Networks or third-party device can be added manually 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.

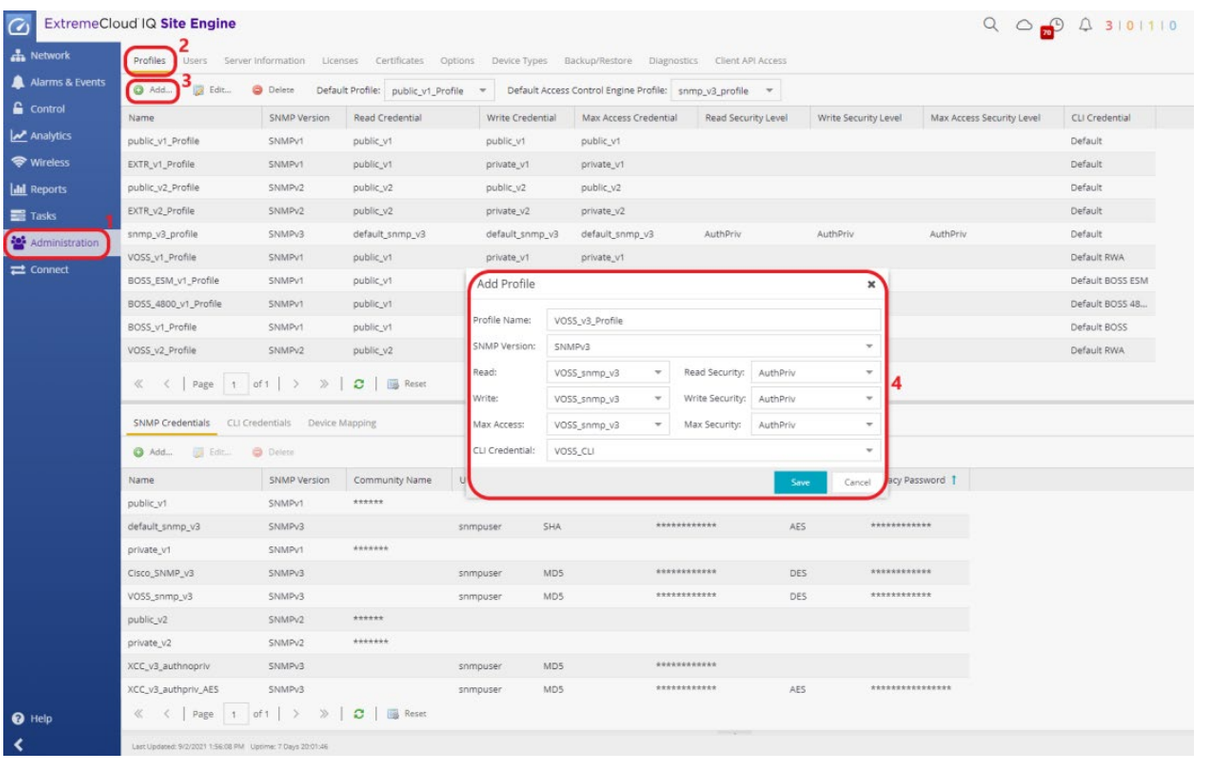
As depicted in Figure 16, navigate to **Administration** and follow the steps to create SNMP and CLI credentials for the VOSS/Fabric Engine switch. Be sure to configure the same SNMP user name, authentication and privacy types, and passwords that are configured on the switch.



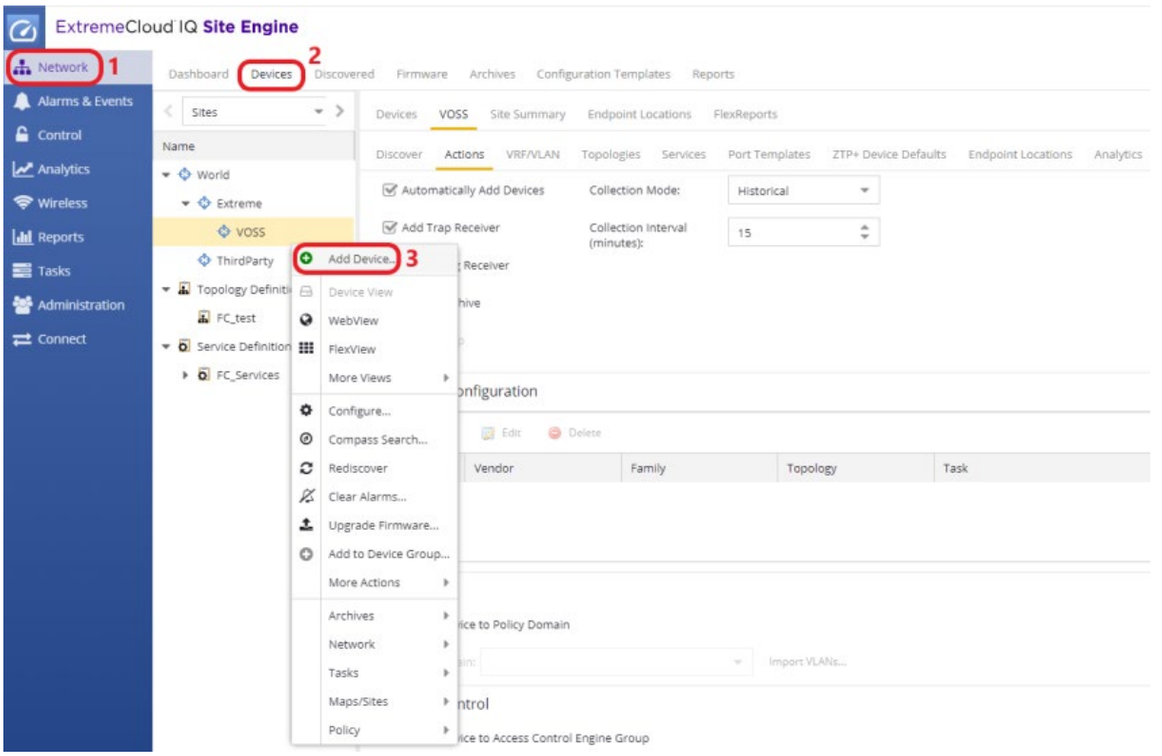
A CLI credential is needed to access the CLI terminal of the device directly from ExtremeCloud IQ - Site Engine and to run scripts or workflows that will interact with the device through the CLI. Note that the CLI credential is also needed for RADIUS configuration on VOSS/Fabric Engine devices starting from ExtremeCloud IQ - Site Engine version 21.11.



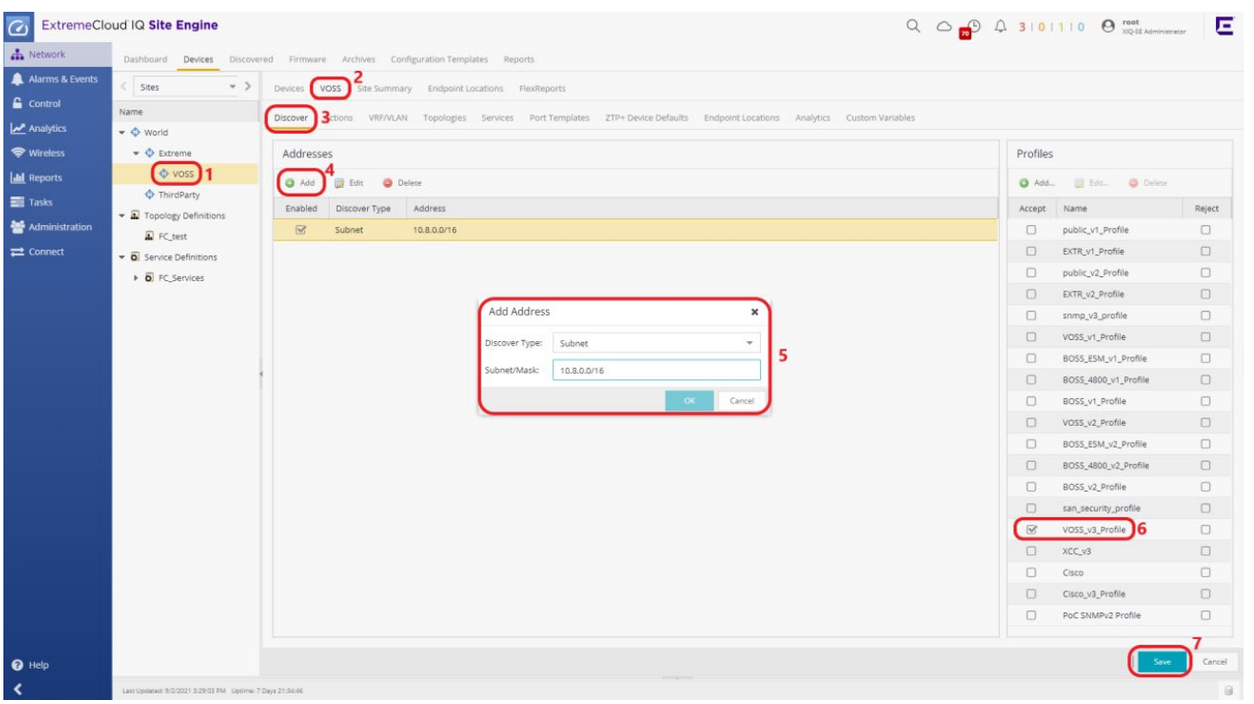
When both SNMP and CLI credentials have been set up, add a new Device Profile and bind the credentials to the profile as shown in Figure 18.



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 VOSS/Fabric Engine switch to be added in and then right click on that Site and select "**Add Devices**".



Alternatively, if there are multiple switches that need to be onboarded, a more convenient method is to use the “Discover” operation under the Site as illustrated in Figure 20. The Discover type can be a Subnet, a Seed Address, or an Address Range.



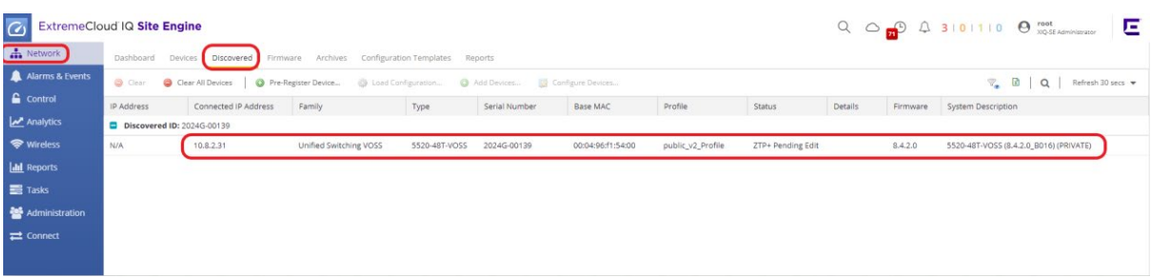
Option 2: Automated Discovery through ZTP+

Adding or discovering switches manually can be cumbersome for the network operator and require follow-up configuration after the switches are added to the ExtremeCloud IQ - Site Engine database. A better method of discovery for VOSS/Fabric Engine switches is through the use of Zero Touch Provisioning Plus (ZTP+). VOSS/Fabric Engine devices, starting from version 8.2.5, support ZTP+, which enables them to send information to ExtremeCloud IQ - Site Engine automatically after they are initially powered up with factory default settings. When a VOSS/Fabric Engine device is discovered in ExtremeCloud IQ - Site Engine through ZTP+, it can quickly be added to the ExtremeCloud IQ - Site Engine database with minimal to no manual configuration. This process minimizes the amount of time needed to configure a new device and deploy it on the network.

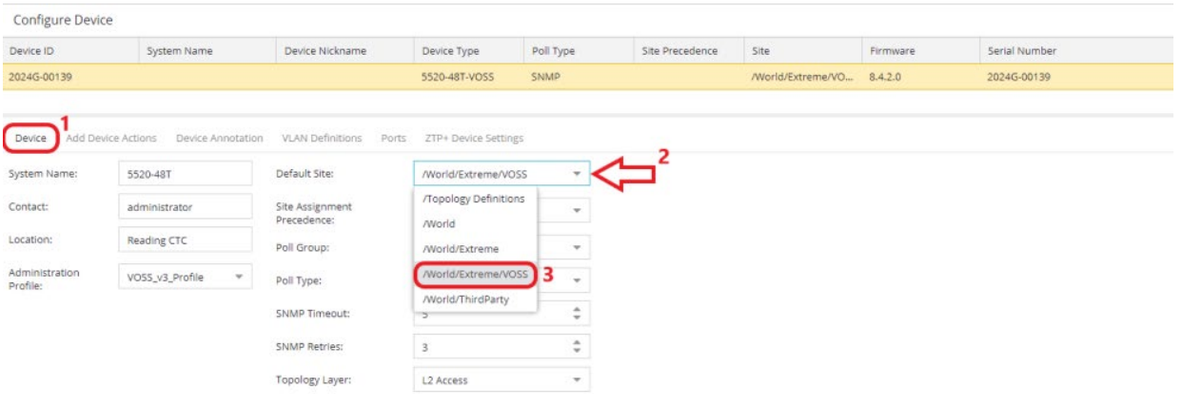
For the ZTP+ process to work properly, there are some prerequisites which are listed below:

- The switch should have a factory default configuration. After a configuration file is saved, the ZTP+ process will not run on the next reboot of the switch.
- The switch should be able to reach the DHCP server and receive IP address through its OOB interface or Management VLAN.
- The switch should obtain one or more DNS servers and a domain name from the DHCP server.
- The switch will make a DNS query to resolve *extremecontrol.domain* to start the ZTP+ process and reach ExtremeCloud IQ - Site Engine. *extremecontrol.domain* should resolve to the ExtremeCloud IQ - Site Engine IP address.

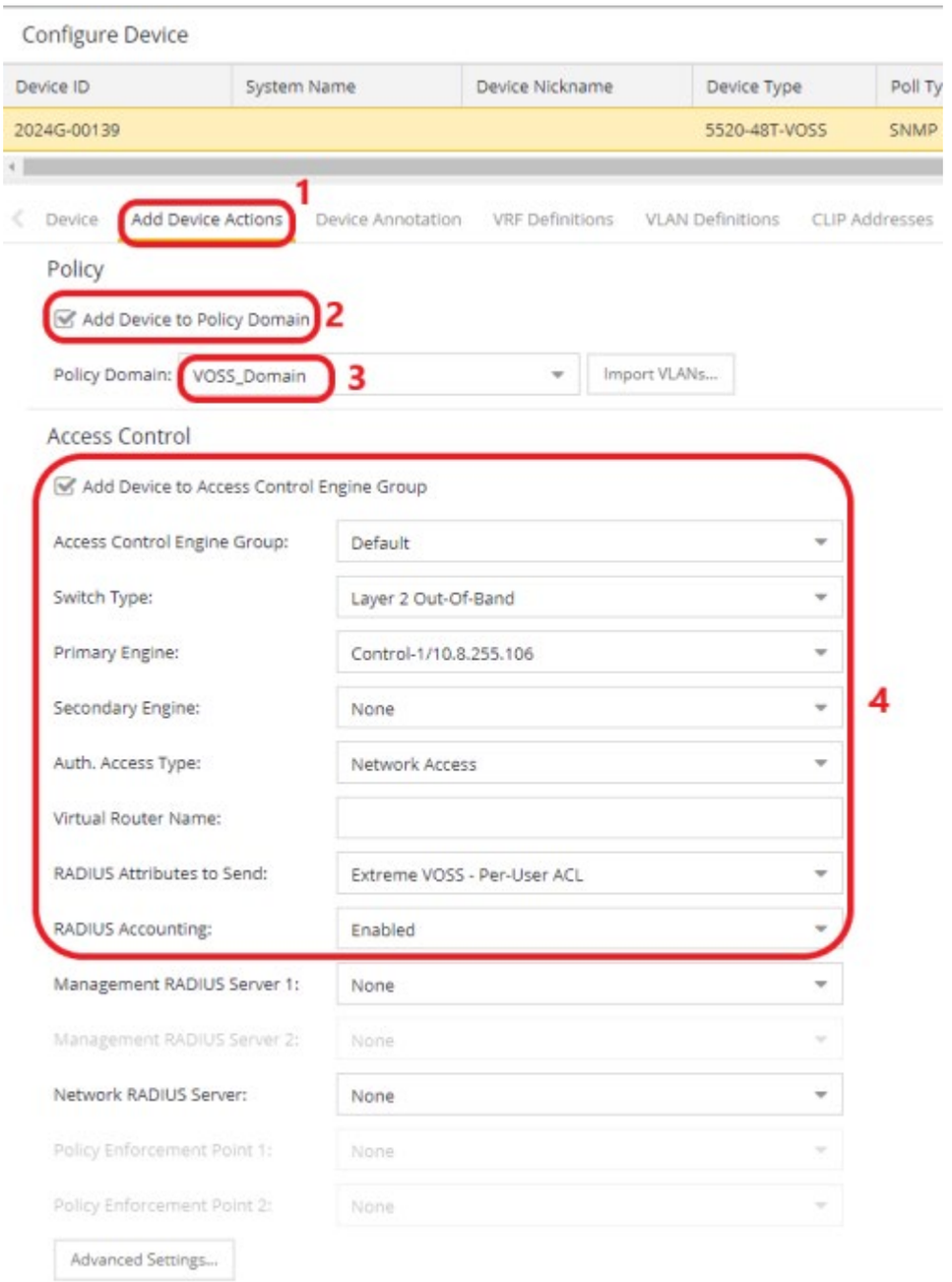
When the prerequisites are fulfilled and the switch is powered up, it will appear in the Discovered tab as shown in Figure 21.



Select the switch and select **Configure Devices**. In the resulting pop-up window, modify the ZTP+ settings as needed. If the site is already configured with "**Add Device Actions**", the default site can be selected as illustrated in Figure 22, such that all the site settings related to ZTP+ are inherited automatically.



To automatically add the VOSS/Fabric Engine switch to the policy domain and Access Control Engine group, navigate to **Add Device Actions** and select the appropriate Policy Domain and Access Control settings as shown in Figure 23. Then select **Save**.



NOTE

Auth Access Type “Network Access”, “Management Access” and “Any Access” for VOSS/Fabric Engine switches are supported starting from ExtremeCloud IQ - Site Engine version 21.11.

NOTE

If the shared secret will be different from Access Control's default shared secret, select **Advanced Settings** under Access Control in Figure 23 and set the shared secret to match the one that will be configured on the VOSS/Fabric Engine switch. Otherwise, the default shared secret (*ETS_TAG_SHARED_SECRET*) will be used.

After saving the ZTP+ settings, the status should change to **ZTP+ Staged** as shown in Figure 24, meaning that ExtremeCloud IQ - Site Engine will now push the configured settings to the VOSS/Fabric Engine switch. If there are no issues during this process, after a couple of minutes the switch will disappear from the **Discovered** tab and will automatically be added to the respective Site under Devices.

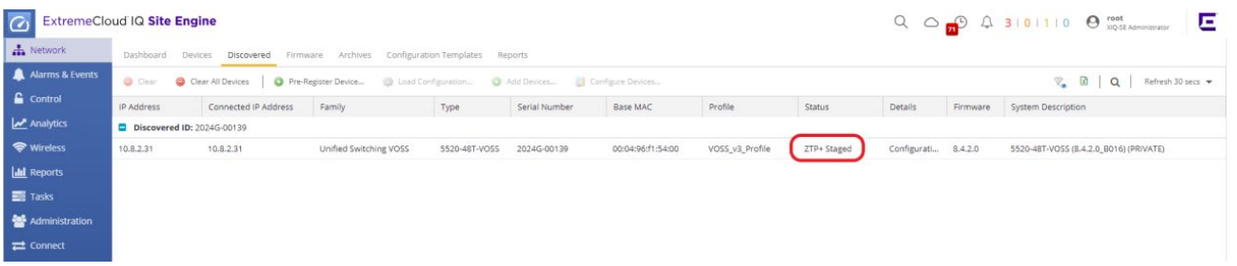


Figure 24 – Status change from *ZTP+ Pending Edit* to *ZTP+ Staged*

NOTE

The initial step of configuring the ZTP+ default settings and adding the VOSS/Fabric Engine switch to the appropriate Site can also be automated with the Global IP to Site Mapping feature. Follow the steps highlighted in Figure 25 to map a subnet to a specific site such that when the switch is initially discovered, ExtremeCloud IQ - Site Engine will assign the switch to the correct Site according to this mapping.

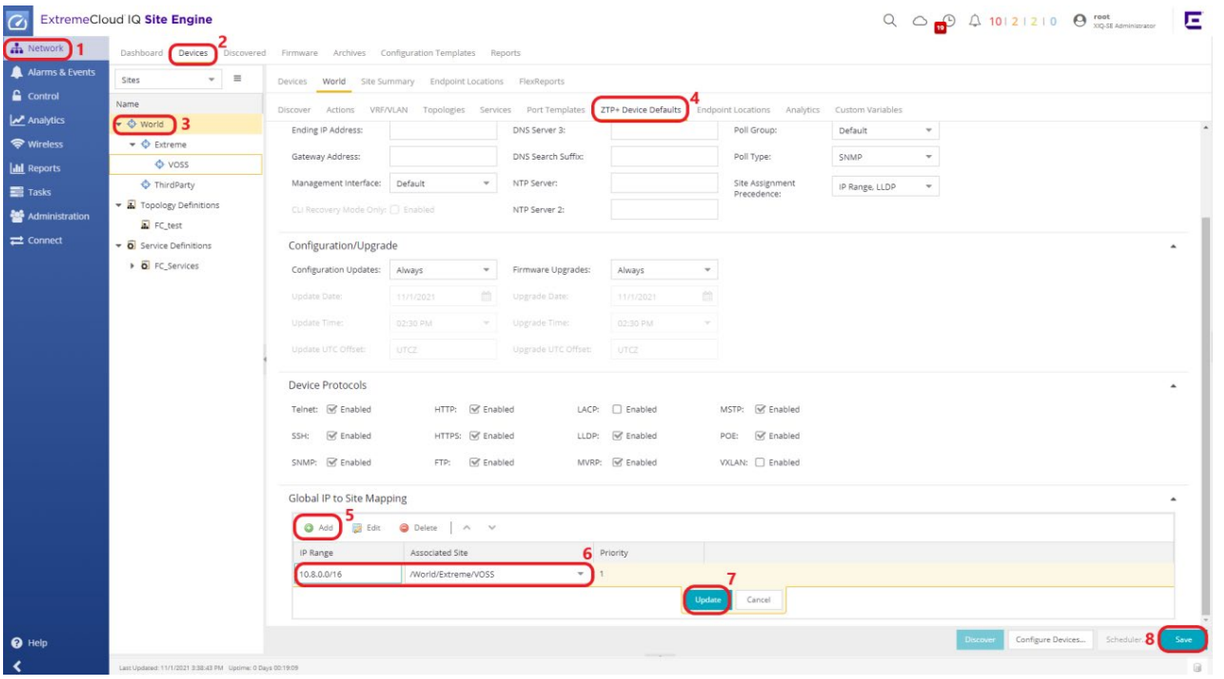


Figure 25 – Global IP to Site Mapping for Automated Site assignment during ZTP+

CAUTION

When a device is added to the ExtremeCloud IQ - Site Engine database, the license is checked before the Site Discover Actions are performed. The onboard status and license state of the switch can be checked from Diagnostics / System / Device Message Details, and Site Discover Actions can be verified from the Operations tab as shown in Figure 26.

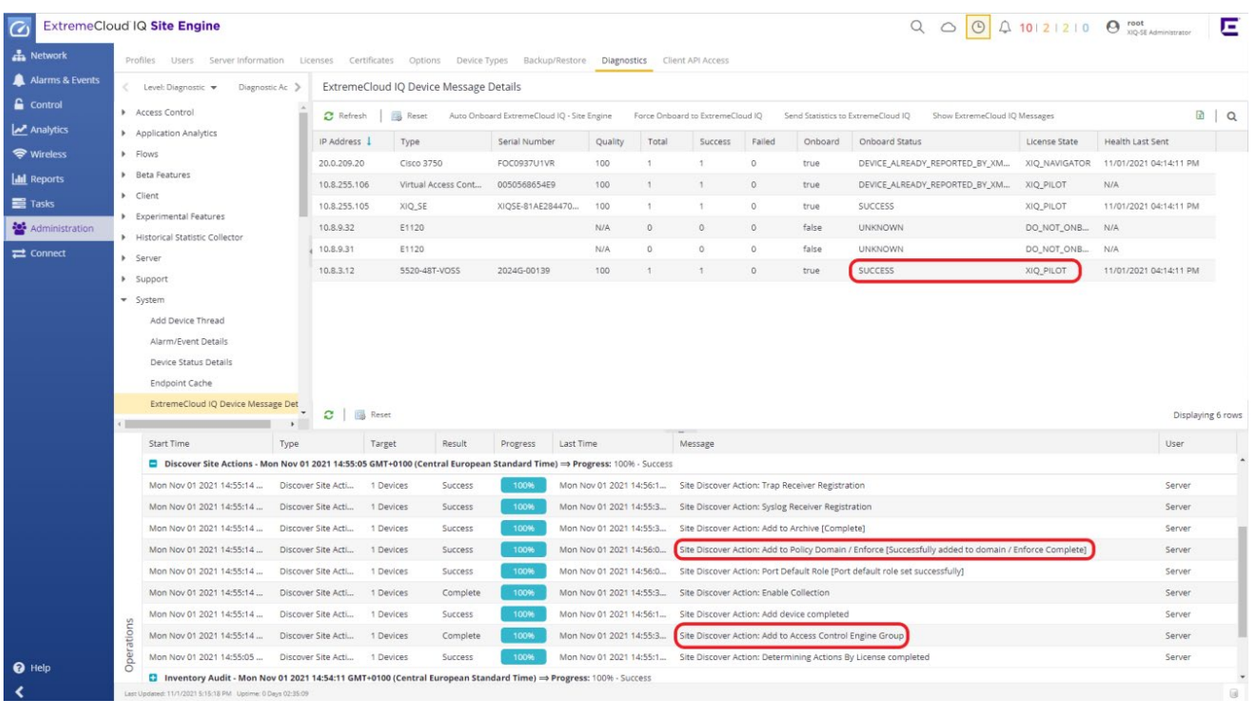


Figure 26 – *Switch Onboard Status and License State Verification*

Navigate to the policy domain and select Devices/Port Groups as shown in Figure 27 to validate that the VOSS/Fabric Engine switch was added to the domain.

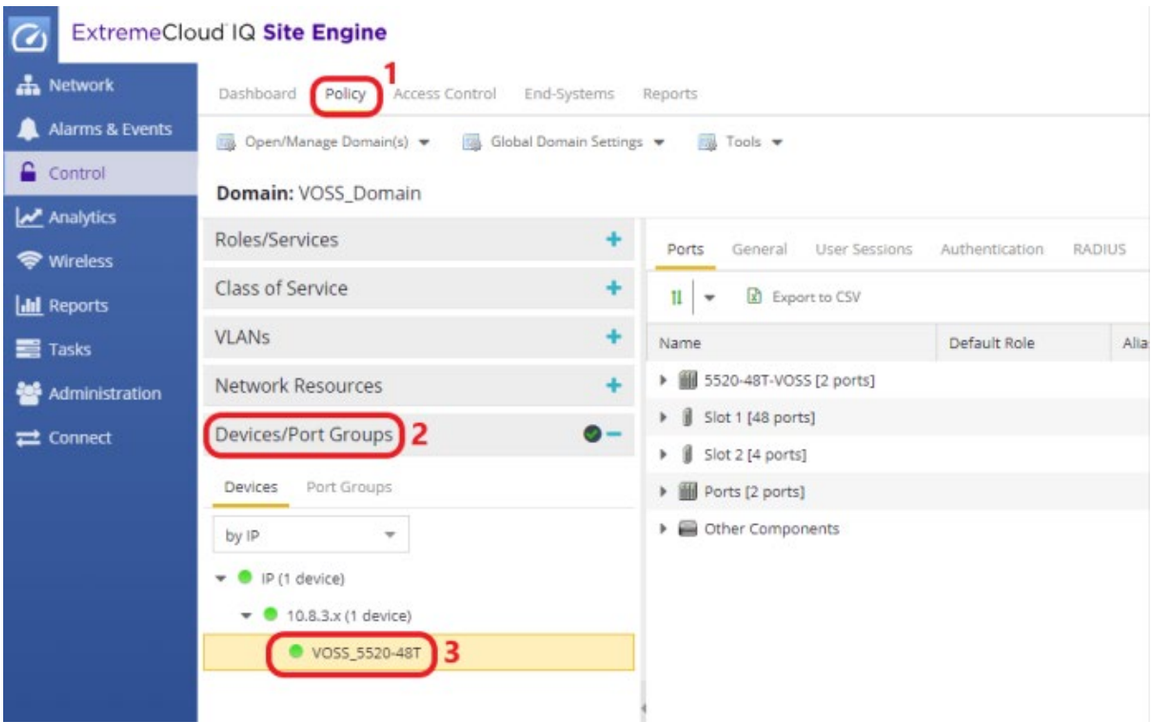


Figure 27 – VOSS/Fabric Engine switch added to the policy domain via ZTP+

Finally, navigate to **Access Control** and select **Engines** to verify that the VOSS/Fabric Engine switch is also added to the Control Engine group.

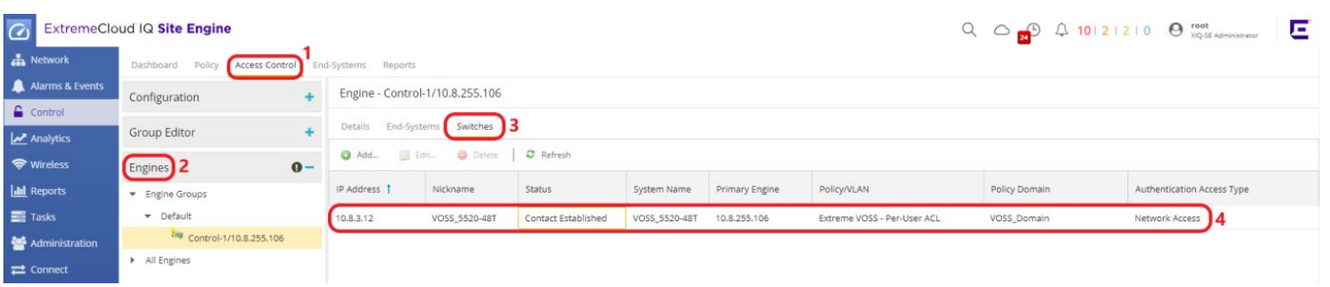


Figure 28 – VOSS/Fabric Engine switch added to Access Control Engine group via ZTP+

CAUTION
In the tested version of ExtremeCloud IQ - Site Engine (21.11.10.57), when VOSS/Fabric Engine devices are added to ExtremeControl through ZTP+ or through run site actions, the **Extreme Policy** attribute is assigned by default as **Radius Attributes to Send**. This will be corrected in a future release. As a workaround, manually change the attribute value to **Extreme VOSS - Per-User ACL** so that you can use Downloadable ACLs.

Access Control Preparation

Step 1: AAA Configuration

Under **Access Control**, select the **Configuration** section, expand **AAA** in the Configuration tree, and right-click the **Default** AAA configuration. Select **Make Advanced**.

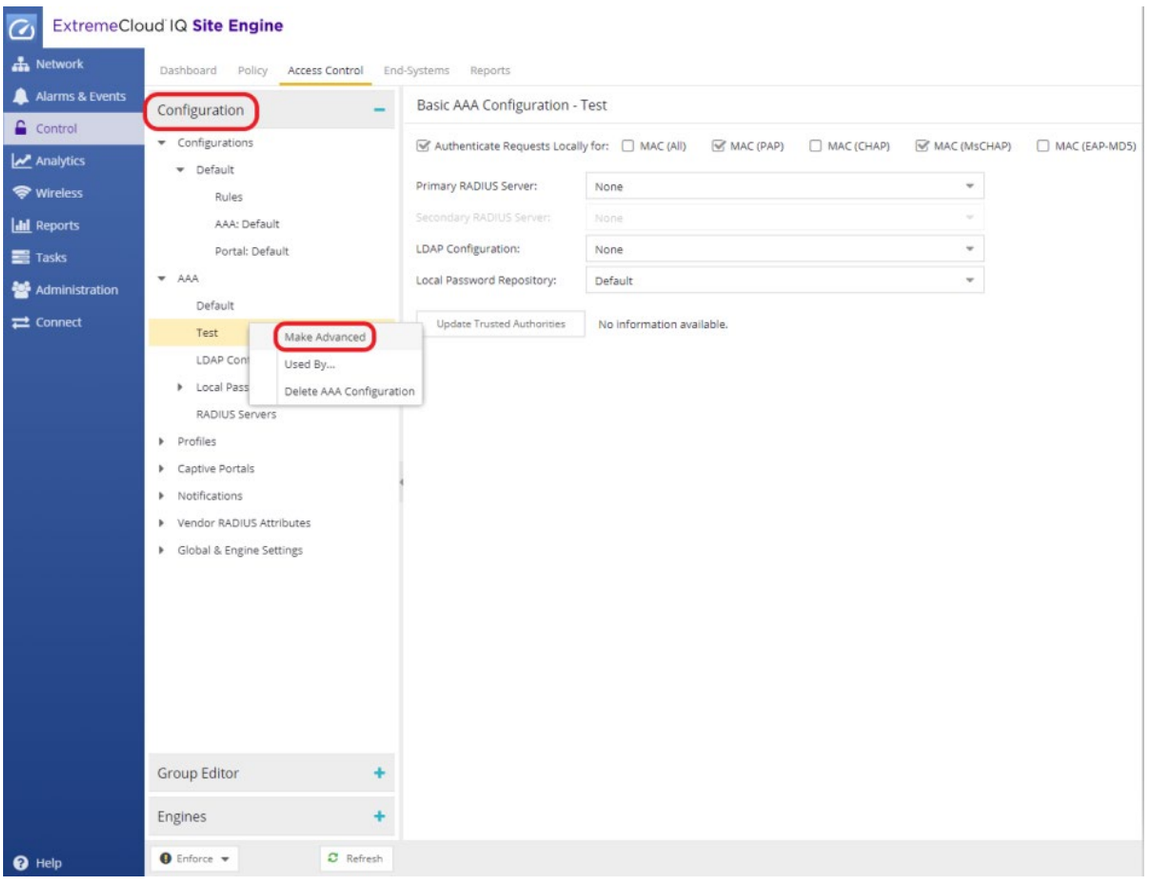


Figure 29 – AAA Configuration - 1

Select the **Any** authentication rule and then select **Edit**.

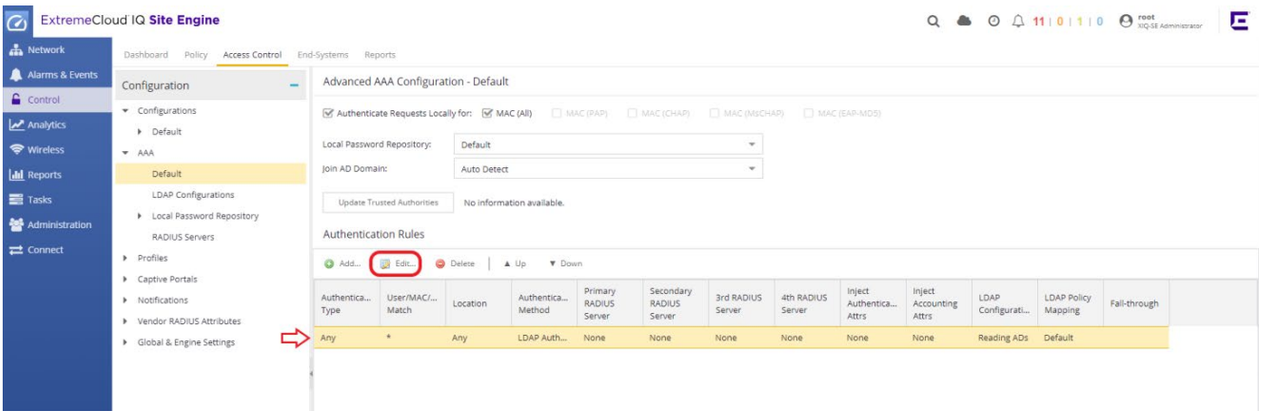


Figure 30 – AAA Configuration - 2

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 **OK**.

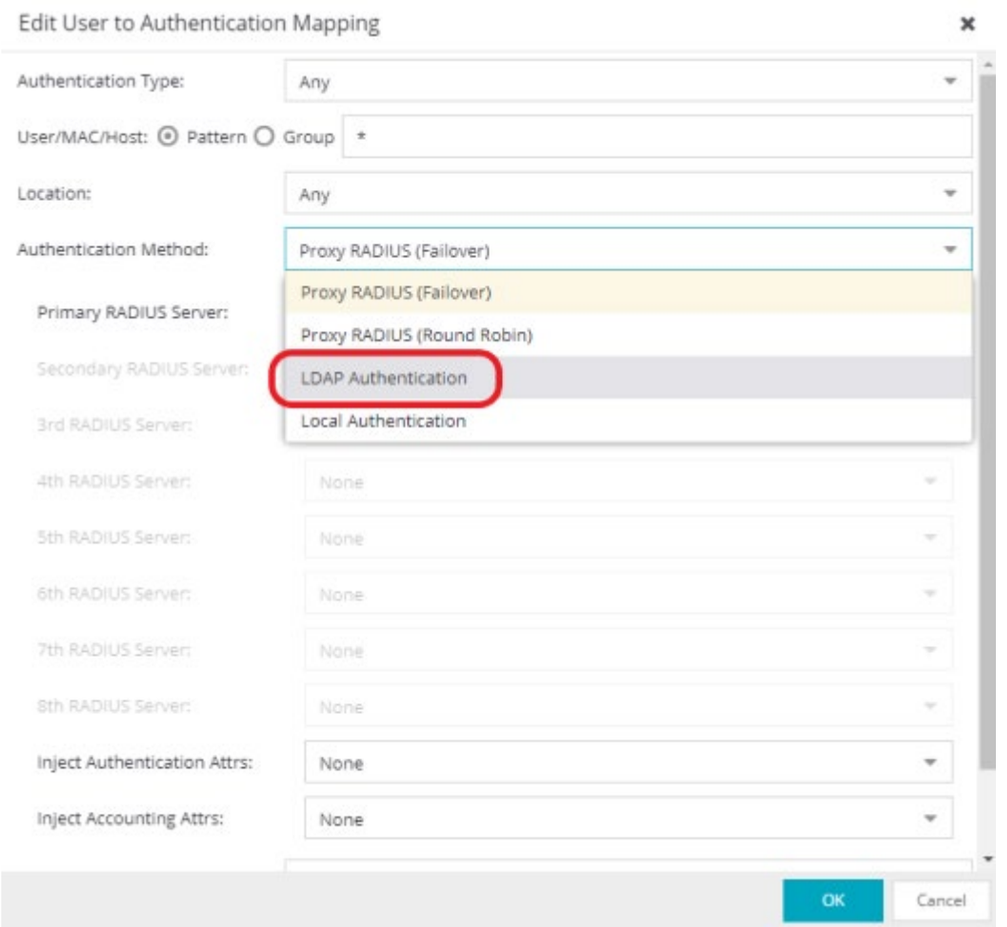


Figure 31 – AAA Configuration – LDAP Authentication Setting

After you select **LDAP Authentication**, a new LDAP configuration needs to be created so that Extreme Control can communicate with Active Directory. Select the drop-down menu in **LDAP Configuration** and then select **New** as shown in Figure 32.

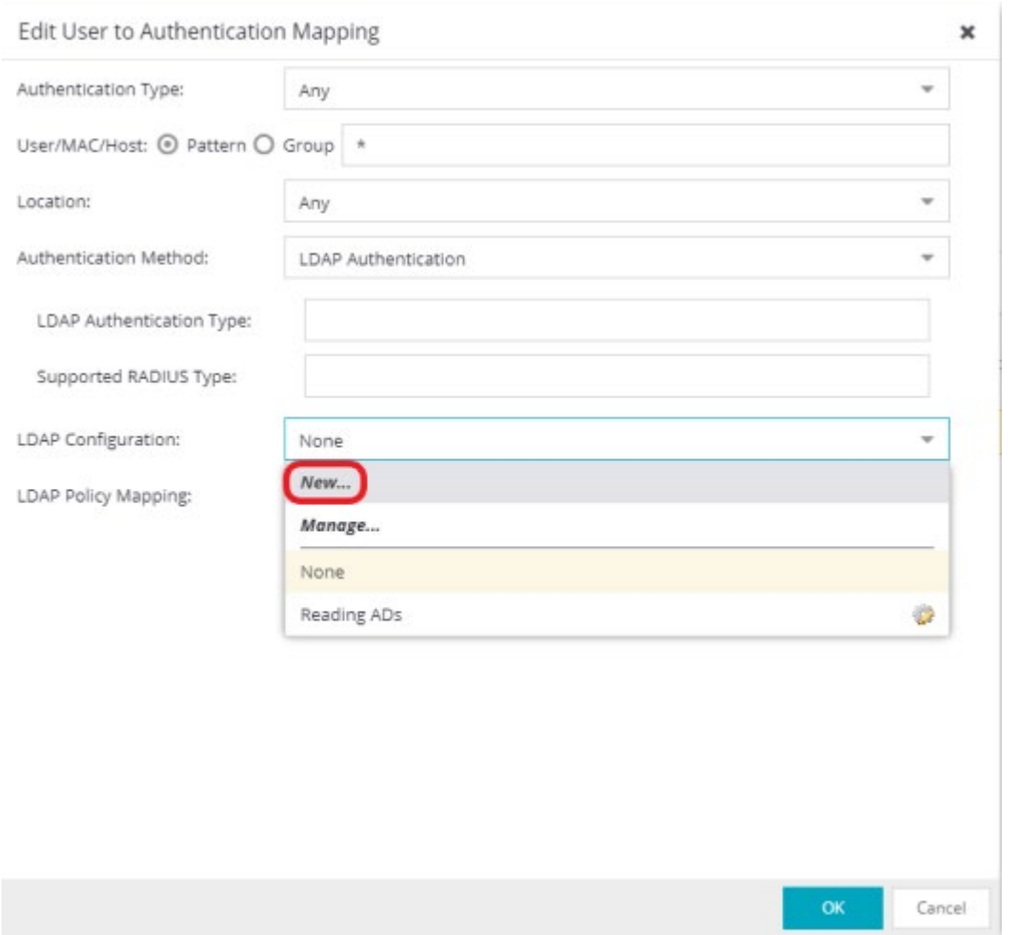


Figure 32 – AAA Configuration – Add LDAP Configuration – 1

Follow the steps illustrated in Figure 33 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 1 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, FQDN of the domain needs to be broken into separate DC= statements, command delimited. And add CN=Users and CN=Computers at the beginning of User and Computer search roots respectively.

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

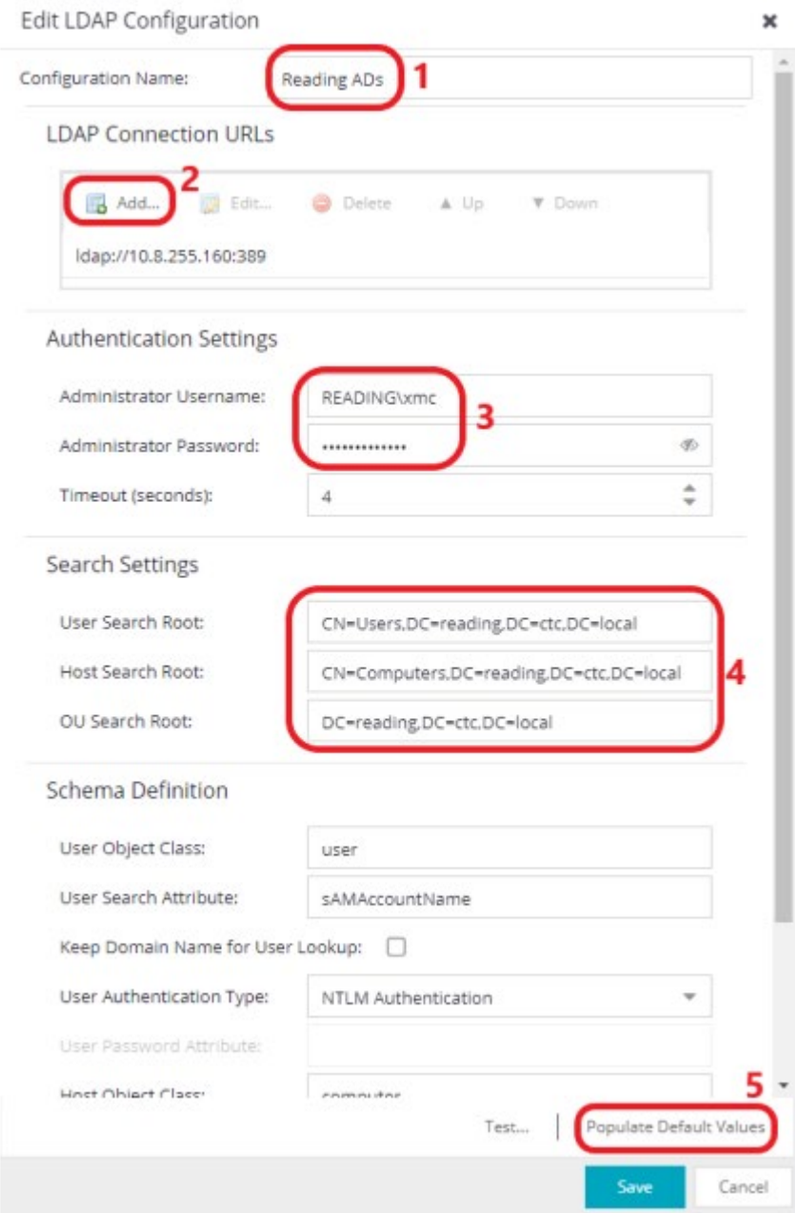


Figure 33 – AAA Configuration – Add LDAP Configuration – 2

Save the configuration, and **Enforce** again as shown in Figure 34.

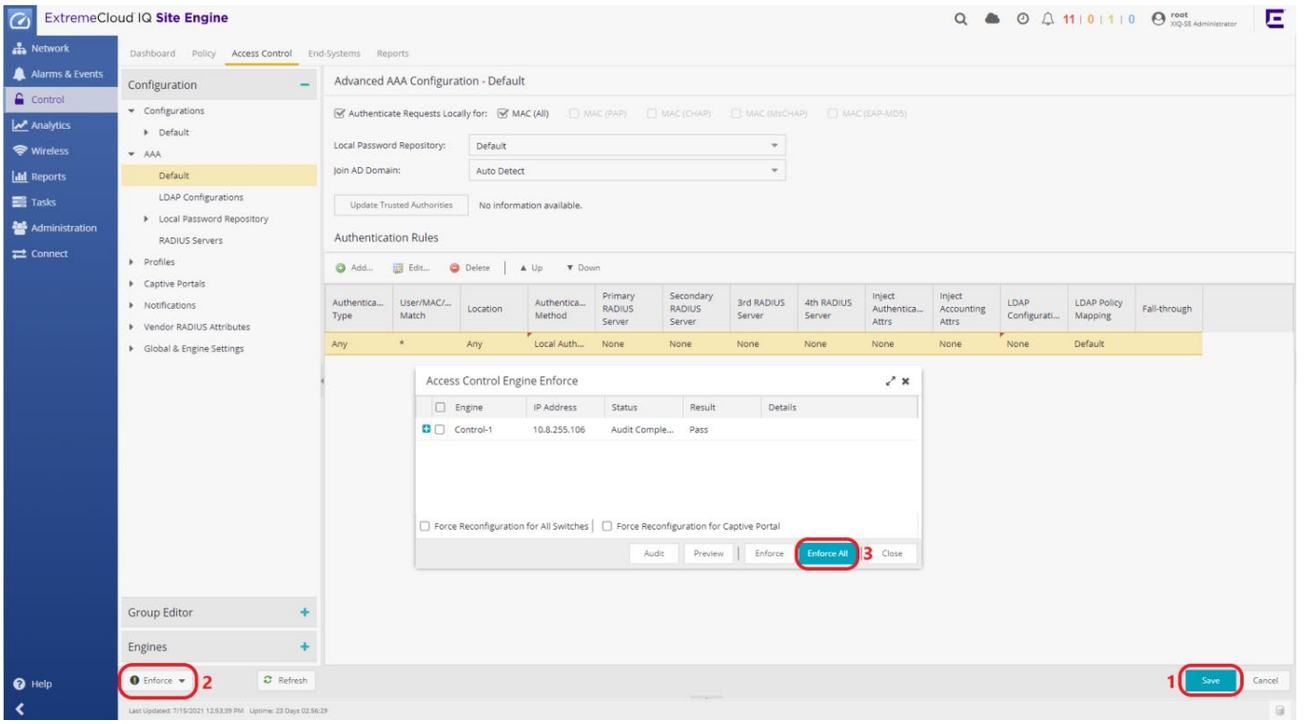


Figure 34 – How to enforce the configuration in ExtremeControl

Step 2: Create Rules

In order 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 and expand **Configurations > Default**. Select **Rules** and then add a new rule.

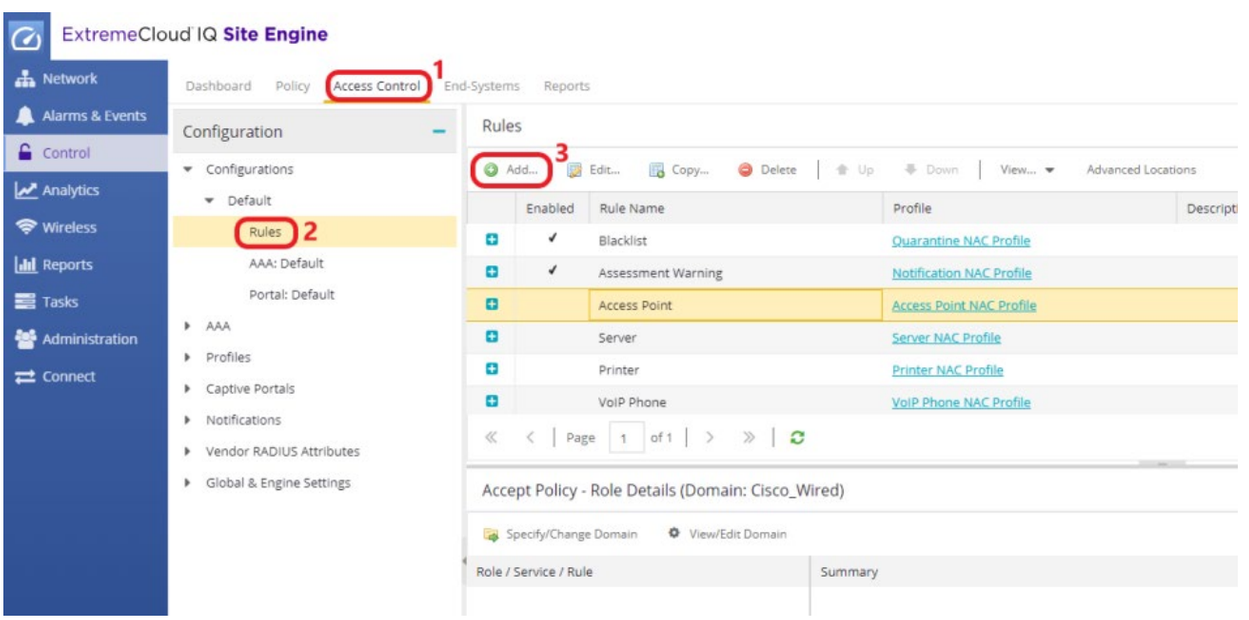


Figure 35 – How to add a new rule in Access Control - 1

Name the rule **Contractor_Rule**. Then select the **User Group** drop-down list and select **New**. Select **LDAP User Group** as the Type, and name the User Group **Contractor_Users**.

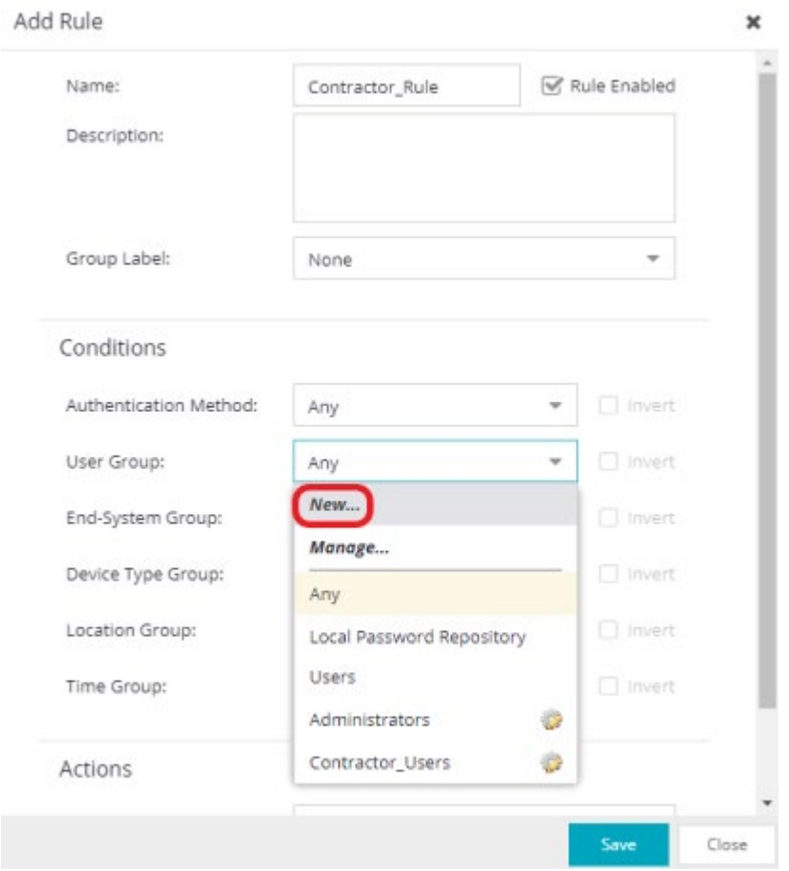


Figure 36 – How to add a new rule in Access Control – 2

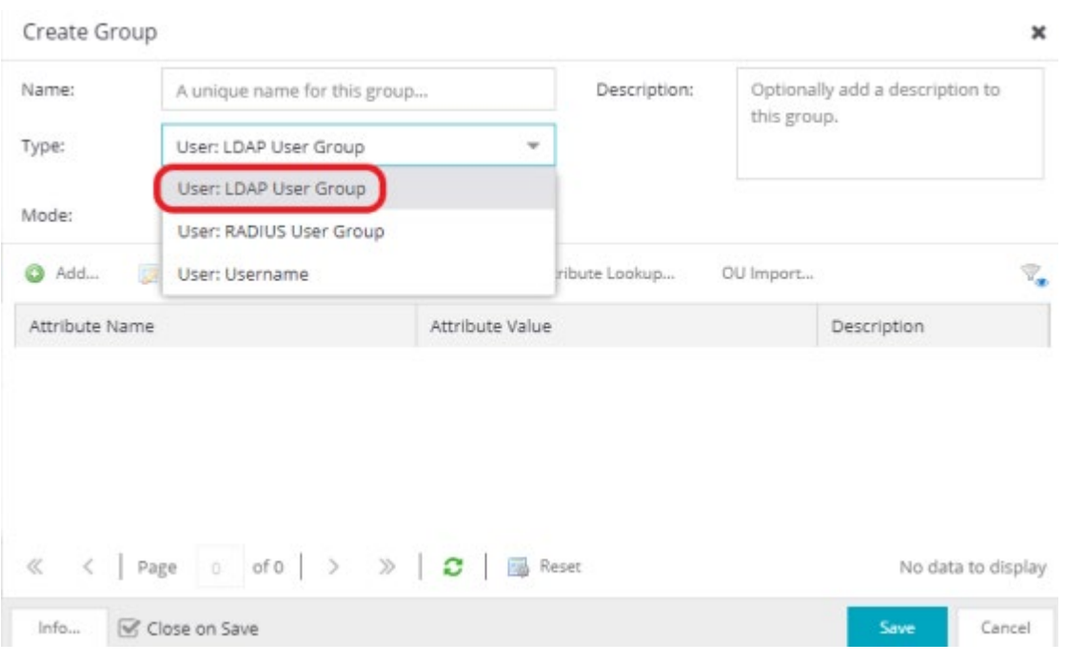


Figure 37 – How to create an LDAP User Group in Access Control - 1

At this point, there is no link between the created User Group and LDAP Server. Therefore, Attribute Name and Value pair need to be added to this LDAP User Group in order to look the user up in LDAP Server during the authentication process. Easiest way to add Attribute Name and Value pair is to select **Attribute Lookup** as shown in Figure 38 and search for a known user name belonging to the relevant LDAP User group, which is in our example Contractors.

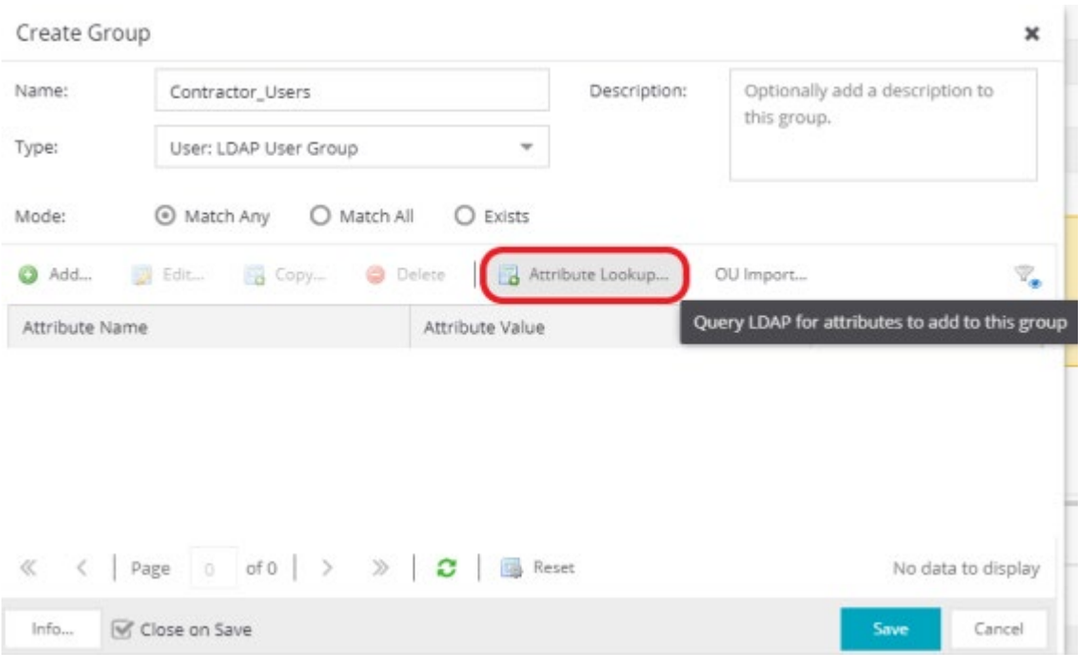


Figure 38 How to create an LDAP User Group in Access Control - 2

Select the LDAP Configuration created in Figure 33 and search for an Active Directory user belonging to Contractors OU. Then add the **memberOf** attribute name and value pair as shown in Figure 39.

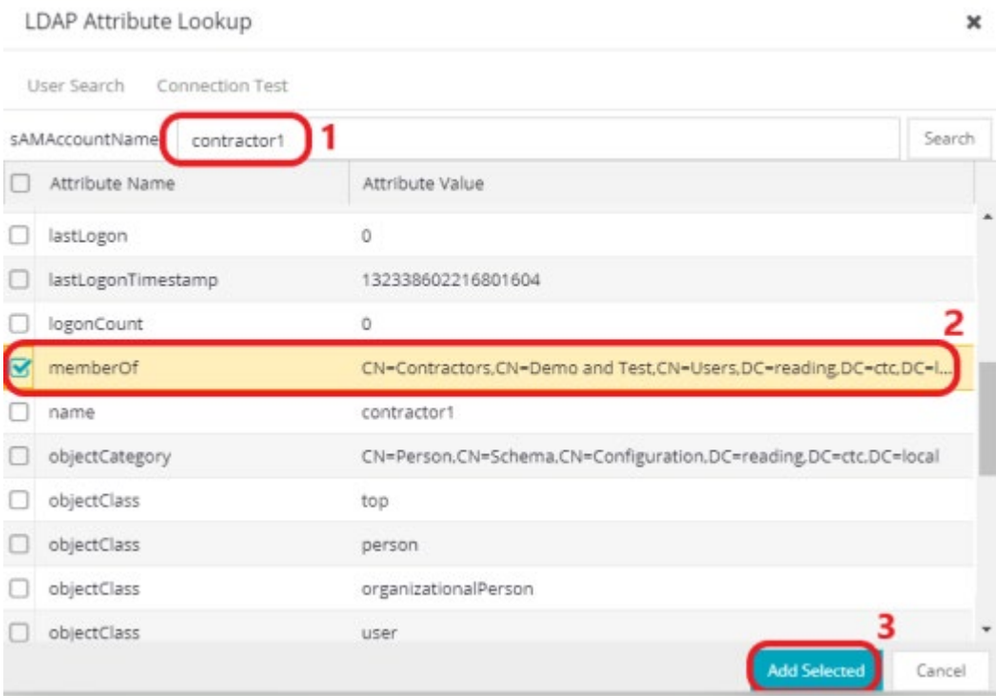


Figure 39 – How to create an LDAP User Group in Access Control - 3

The LDAP User Group and the Access Control rule will look like the ones depicted in Figure 40 and Figure 41, respectively.

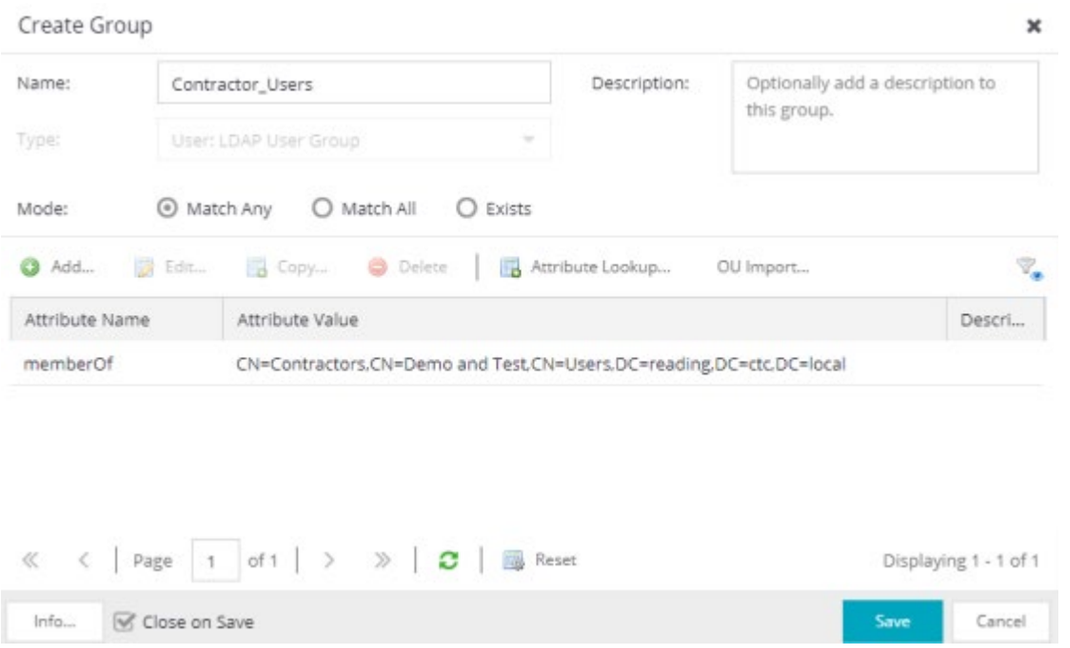


Figure 40 – LDAP User Group Example

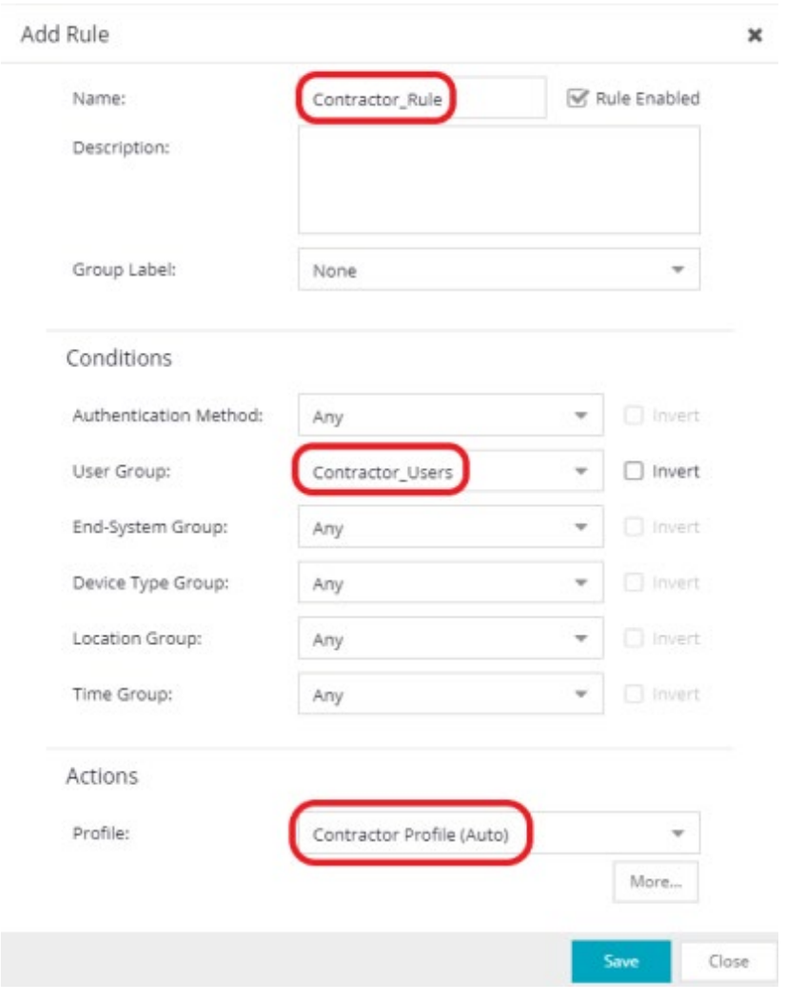


Figure 41 – Rule example with User Group condition

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

Note
Profiles for each role created in the policy domain are auto-created when a switch is added to the Access Control Engine group with the same policy domain.

VOSS/Fabric Engine Switch Configuration

The main goal is to minimize manual CLI configuration of the VOSS/Fabric Engine switch as much as possible. Below are snippets of CLI commands needed for specific features. When ZTP+ is used as the switch discovery method, which is the preferred method for this guide, both SNMP and RADIUS configurations will also be automated. All the rest of the configuration is automated through ZTP+ and Auto-sense functionalities.

SNMP Configuration

SNMP configuration is sent to the switch during onboarding via ZTP+. Below are the CLI commands in case manual configuration is preferred.

```
conf t
cli password xmc read-write-all
Do you want to change username for the default RWA user ?
(y/n) ? y
Enter the old password : rwa
Enter the New password : password
Re-enter the New password : password
snmp-server user snmpuser sha snmpauthcred aes snmpprivcred
snmp-server user snmpuser group initial
no snmp-server user initial
```

RADIUS Configuration

```
config terminal
radius server host 10.8.255.106 key ETS_TAG_SHARED_SECRET used-by eapol
radius enable
radius accounting enable
radius dynamic-server client 10.8.255.106 secret ETS_TAG_SHARED_SECRET enable
eapol enable
end
```

Verification – Client Testing

Clients that are attached to the VOSS/Fabric Engine switch with 802.1X supplicants properly configured will be 802.1X authenticated. When the user logs-in with the appropriate user credentials that belong to Contractors OU in the Active Directory, the Rule Engine processes the authentication request. The Rule Engine selects the rule for which all the conditions are “True” (conditions are logically “AND”ed), and the respective profile is applied.

If for some reason the desired rule and profile are not applied, the **Configuration Evaluation Tool** can help you troubleshoot the Rule Engine settings. The tool can be accessed directly from the End-Systems table by right clicking on the end-system in question as shown in Figure 42.

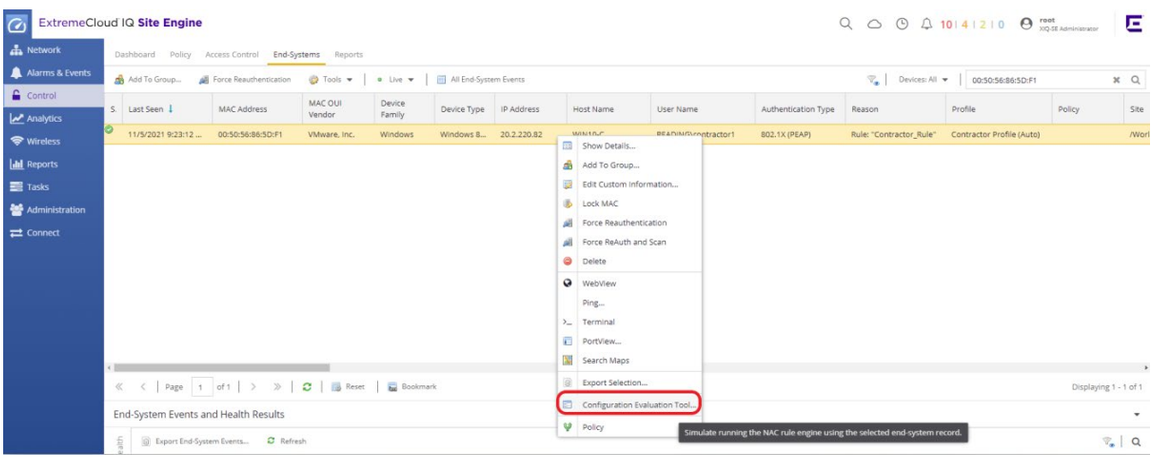


Figure 42 – Configuration Evaluation Tool

The assigned profile and ACL entries can be verified on the VOSS/Fabric Engine switch by issuing the command **show eapol sessions eap** *PortNum* **verbose** and **show filter acl.** See Figures 43 and 44. More VOSS/Fabric Engine CLI commands to verify and troubleshoot authentication and authorization steps can be found in the troubleshooting appendix.

```
VOSS_5520-48T:1#show eapol sessions eap 1/5 verbose
********************************************************************************
               Command Execution Time: Tue Nov 02 11:13:45 2021 GMT
********************************************************************************

                                  Eap Oper Status Verbose
--------------------------------------------------------------------------------
PORT  MAC               PAE            VLAN  PRI  Flex-UNI  I-SID      VLAN:I-SID          ACL  ACEs          RADIUS DYNAMIC
NUM                     STATUS         ID          Enable    SOURCE                                            SETTINGS
--------------------------------------------------------------------------------
1/5   00:50:56:86:5d:f1  authenticated  N/A   0     true      radius     0:2800210           1    1,2,3,4,
                                                                                             5,6
--------------------------------------------------------------------------------
Total Number of EAP sessions : 1
```

Figure 43 – Verify EAP Session Details from the VOSS/Fabric Engine CLI

```
VOSS_5520-48T:1#show filter acl ace
********************************************************************************
                Command Execution Time: Tue Nov 02 11:28:27 2021 GMT
********************************************************************************

                              Ace Action Table (Part I)
================================================================================
Acl  Ace  AceName                 Admin   Oper    Mode    Mlt Remark  Remark
Id   Id                          State   State           Id DSCP    Dot1p
--------------------------------------------------------------------------------
1    1    1_Deny_Telnet           Enable  Up      deny    0   disable disable
1    2    2_Deny_SSH              Enable  Up      deny    0   disable disable
1    3    3_Deny_FTP              Enable  Up      deny    0   disable disable
1    4    4_Deny_TFTP             Enable  Up      deny    0   disable disable
1    5    5_Deny_Server_RDP       Enable  Up      deny    0   disable disable
1    6    ACE-6                   Enable  Up      permit  0   disable disable
```

Figure 44 – Verify Downloadable ACL Details from the VOSS/Fabric Engine CLI

The End-System table Authorization column also shows the Downloadable ACL which is sent to the VOSS/Fabric Engine switch as seen in Figure 45.

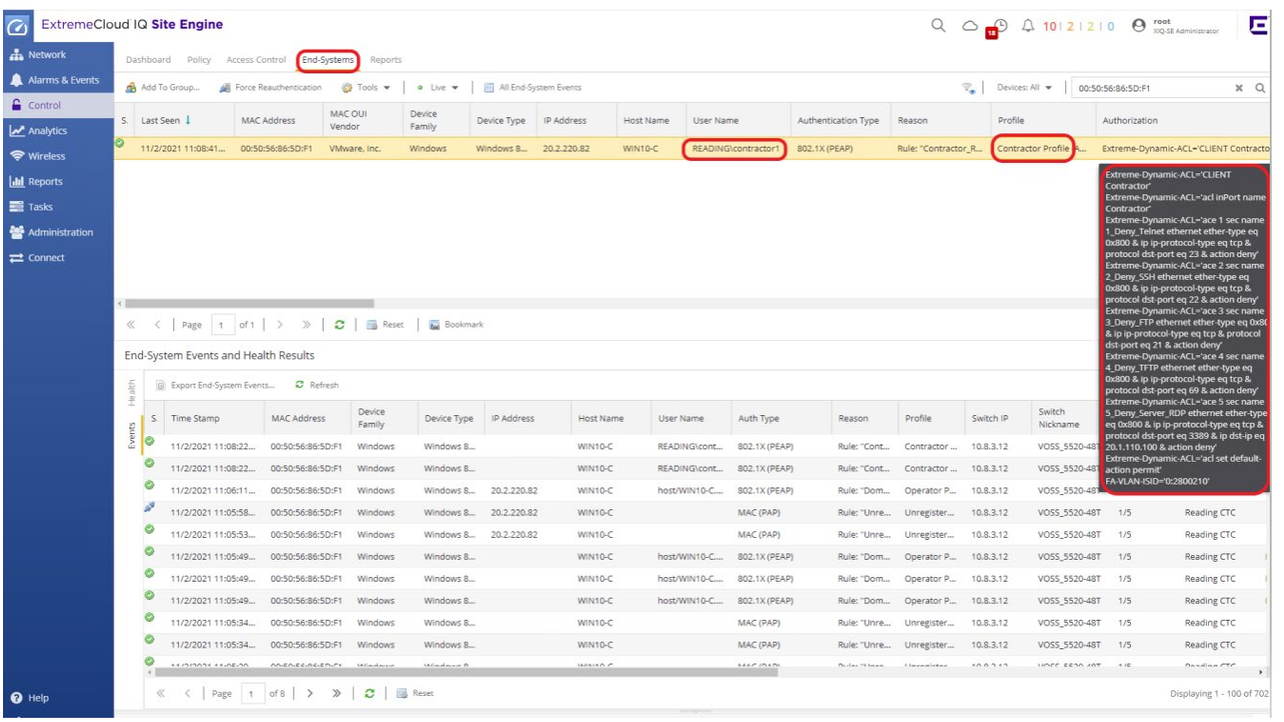


Figure 45 – Verify Downloadable ACLs from the End-Systems table in Access Control

Appendix – Troubleshooting

ZTP+ Troubleshooting

When troubleshooting ZTP+ from a VOSS/Fabric Engine switch, the following CLI commands are useful for understanding the state of the cloud connector on the switch.

- **show application auto-provision**

```
VOSS_5520-48T:1#show application auto-provision
*********************************************************************************************
            Command Execution Time: Fri Nov 05 15:27:10 2021 GMT
*********************************************************************************************

=============================================================================================================
                                    Auto-provision Info
=============================================================================================================
Operational Status              : Complete
```

- **show logging file**

Downloadable ACL Troubleshooting

When troubleshooting a VOSS/Fabric Engine switch, several commands are useful for verifying specifics related to client sessions and Downloadable ACLs.

- **show eapol session-stats interface gigabitEthernet <interface>**

```
VOSS_5520-48T:1#show eapol session-stats interface gigabitEthernet 1/5
*********************************************************************************************
            Command Execution Time: Fri Nov 05 15:06:34 2021 GMT
*********************************************************************************************

=============================================================================================================
                              Eap Authenticator Session Statistics
=============================================================================================================
PORT  MAC                  SESSION   AUTHENTIC       SESSION              TERMINATE       USER
NUM                        ID        METHOD          TIME                 CAUSE           NAME
-------------------------------------------------------------------------------------------------------------
1/5   00:50:56:86:5d:f1    0000004c  remote-server   0 day(s), 06:43:35   not-terminated  READING\contractorl
```

- **show eapol sessions eap**

```
VOSS_5520-48T:1#show eapol sessions eap
*********************************************************************************************
            Command Execution Time: Fri Nov 05 15:17:44 2021 GMT
*********************************************************************************************

=============================================================================================================
                                        Eap Oper Status
=============================================================================================================
PORT  MAC                PAE              VLAN  PRI  Flex-UNI  I-SID       VLAN:I-SID
NUM                      STATUS           ID         Enable    SOURCE
-------------------------------------------------------------------------------------------------------------
1/5   00:50:56:86:5d:f1  authenticated    N/A   0    true      radius      0:2800210
-------------------------------------------------------------------------------------------------------------
Total Number of EAP sessions : 1
```

- **show eapol sessions eap verbose**

```
VOSS_5520-48T:1#show eapol sessions eap verbose
*********************************************************************************************
            Command Execution Time: Fri Nov 05 15:19:43 2021 GMT
*********************************************************************************************

=============================================================================================================
                                    Eap Oper Status Verbose
=============================================================================================================
PORT  MAC                PAE              VLAN  PRI  Flex-UNI  I-SID       VLAN:I-SID                ACL  ACEs                RADIUS DYNAMIC
NUM                      STATUS           ID         Enable    SOURCE                                      SETTINGS
-------------------------------------------------------------------------------------------------------------
1/5   00:50:56:86:5d:f1  authenticated    N/A   0    true      radius      0:2800210                 1    1,2,3,4,
                                                                                                         5,6
-------------------------------------------------------------------------------------------------------------
Total Number of EAP sessions : 1
```

- **show filter acl**

```
VOSS_5520-48T:1#show filter acl
********************************************************************************
            Command Execution Time: Fri Nov 05 15:22:13 2021 GMT
********************************************************************************

================================================================================================================
                                    Vlan/VSN ACL Table
================================================================================================================
Acl  Type    AclName             PktType State    Origin # of Default CtrPkt Vlan/I-sid
Id                                                      ACEs Action  Rule   Id
----------------------------------------------------------------------------------------------------------------

================================================================================================================
                                  Vlan ACL Global-Action Table
================================================================================================================
Acl  Type    Ipfix       Monitor     Monitor
Id                       Dst-Mlt     Dst-Port
----------------------------------------------------------------------------------------------------------------

================================================================================================================
                                     Port ACL Table
================================================================================================================
Acl  Type    AclName             PktType State    Origin # of Default CtrPkt Port
Id                                                      ACEs Action  Rule
----------------------------------------------------------------------------------------------------------------
1    Ingress Contractor          nonipv6 enabled  eap    6    permit permit  1/5
================================================================================================================
                                   Port ACL Global-Action Table
================================================================================================================
Acl  Type    Ipfix       Monitor     Monitor
Id                       Dst-Mlt     Dst-Port
----------------------------------------------------------------------------------------------------------------
1    Ingress Disable     0

Displayed 1 of 1 Entries
```

- **show eapol sessions eap <interface> verbose**

```
VOSS_5520-48T:1#show eapol sessions eap 1/5 verbose
********************************************************************************
            Command Execution Time: Fri Nov 05 15:25:00 2021 GMT
********************************************************************************

================================================================================================================================================================
                                                        Eap Oper Status Verbose
================================================================================================================================================================
PORT  MAC               PAE             VLAN  PRI  Flex-UNI  I-SID       VLAN:I-SID                ACL  ACEs                 RADIUS DYNAMIC
NUM                     STATUS          ID         Enable    SOURCE                                      SETTINGS
----------------------------------------------------------------------------------------------------------------------------------------------------------------
1/5   00:50:56:86:5d:f1 authenticated   N/A   0    true      radius      0:2800210                 1    1,2,3,4,
                                                                                                       5,6
----------------------------------------------------------------------------------------------------------------------------------------------------------------
Total Number of EAP sessions : 1
```

802.1X Supplicant Configuration for Windows Clients

Below are the Windows 10 802.1X supplicant settings for Protected EAP (EAP-PEAP) authentication by using the Windows logon name and password as credentials.

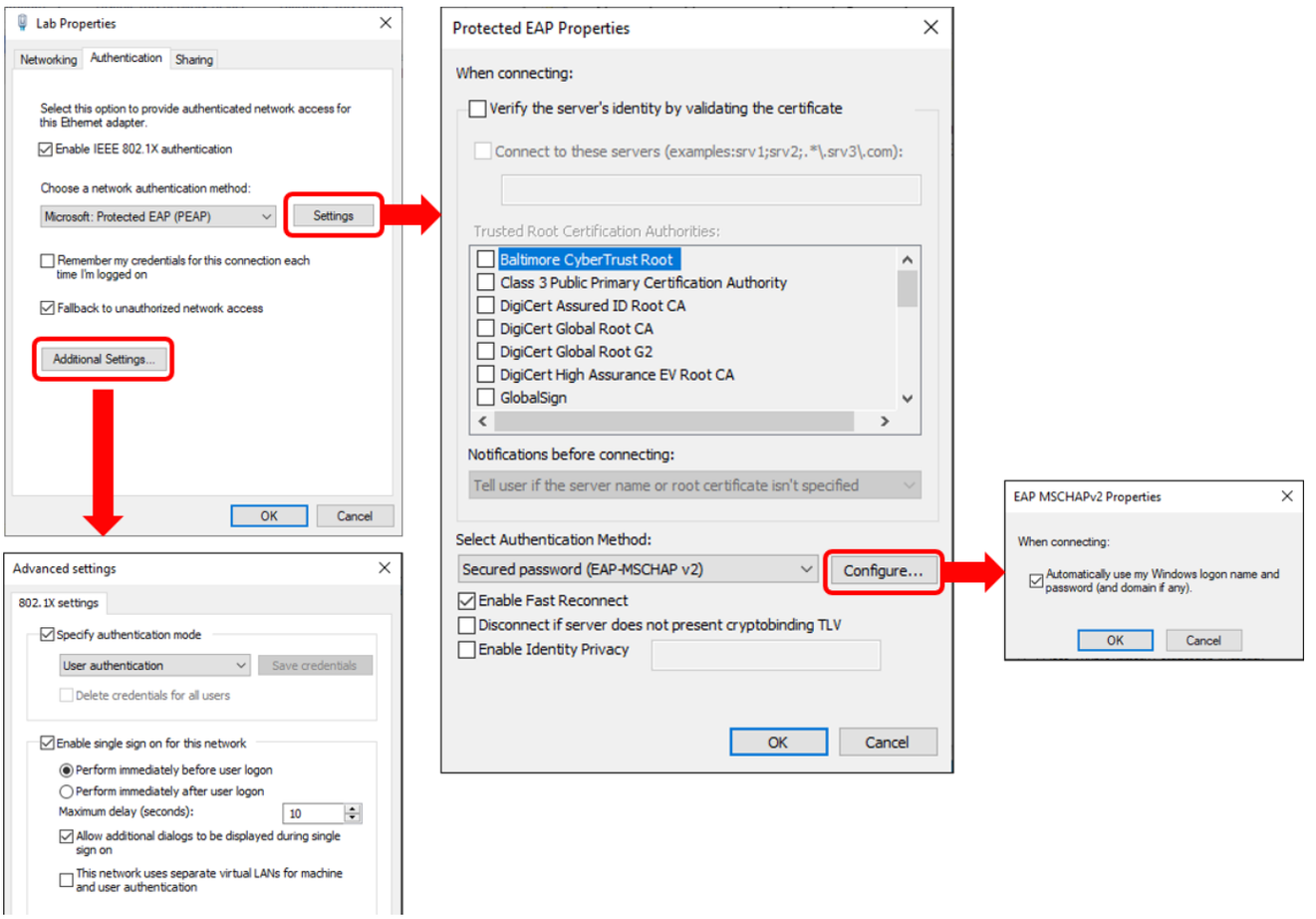


Figure 46 – Windows 10 802.1X supplicant settings for EAP-PEAP authentication

Terms and Conditions of Use