



ExtremeCloud IQ Controller RADIUS Authentication

Using ExtremeCloud IQ SiteEngine

9037938-00
September 2023



Copyright © 2023 Extreme Networks, Inc. All rights reserved.

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: 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/>



Table of Contents

Preface.....	4
Text Conventions.....	4
Documentation and Training.....	5
Open Source Declarations.....	6
Training.....	6
Help and Support.....	6
Subscribe to Product Announcements.....	7
Send Feedback.....	7
Configuring RADIUS Authenticated Management Access on ExtremeCloud IQ Controller with ExtremeControl.....	8
Configuring RADIUS Authenticated Management Access.....	8
Overview.....	8
ExtremeCloud IQ Controller Configuration.....	9
ExtremeControl Configuration.....	11
Testing and Validation.....	18



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings






Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic</i> text	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and Software Compatibility](#) for Extreme Networks products
[Extreme Optics Compatibility](#)
[Other Resources](#) such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the [Open Source Declaration](#) page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the [Extreme Networks Training](#) page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

[Extreme Portal](#)

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

[The Hub](#)

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

[Call GTAC](#)

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



Configuring RADIUS Authenticated Management Access on ExtremeCloud IQ Controller with ExtremeControl

[Configuring RADIUS Authenticated Management Access](#) on page 8

Configuring RADIUS Authenticated Management Access

This document is intended for SEs and partners that are familiar with ExtremeCloud IQ Controller and ExtremeControl (the authentication feature of ExtremeCloud IQ Site Engine). Only the primary touchpoints between these products are covered.

The following prerequisite configuration is assumed:

- ExtremeCloud IQ Controller is configured and added to ExtremeCloud IQ Site Engine.
- ExtremeCloud IQ Site Engine has a working LDAP connection with a directory service such as Microsoft Active Directory.

This document assumes the following firmware and software versions.

- ExtremeCloud IQ Controller build version 10.05.02.009 with AP Firmware 10.1.0.0-036R.
- ExtremeCloud IQ Site Engine build version 22.9.10.73.

Overview

A brief summary of the interactions between ExtremeCloud IQ Controller and ExtremeControl can be broken down into the following steps:

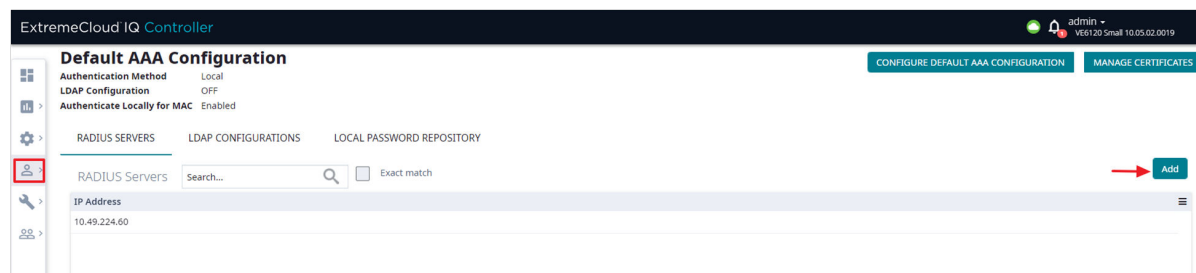
1. The Administrator attempts to log into ExtremeCloud IQ Controller with previously configured login credentials using his/her login credentials, RADIUS authentication occurs.
2. ExtremeCloud IQ Controller sends a RADIUS request to ExtremeControl for administrative login access.
3. ExtremeControl performs an LDAP lookup, authenticates and authorizes the RADIUS request as per its configuration and passes back a RADIUS ACCEPT message: Filter-id set to `Administrator` Access Type Attribute set to `mgmt=su`.
4. ExtremeCloud IQ Controller allows the administrator to login.

ExtremeCloud IQ Controller Configuration

The first step to configuring ExtremeCloud IQ Controller is to configure a AAA policy, then add the RADIUS server to the Authentication Order.

1. Configure ExtremeControl as a designated RADIUS server

From ExtremeCloud IQ Controller, go to **Onboard > AAA Policy > Add**.



Note

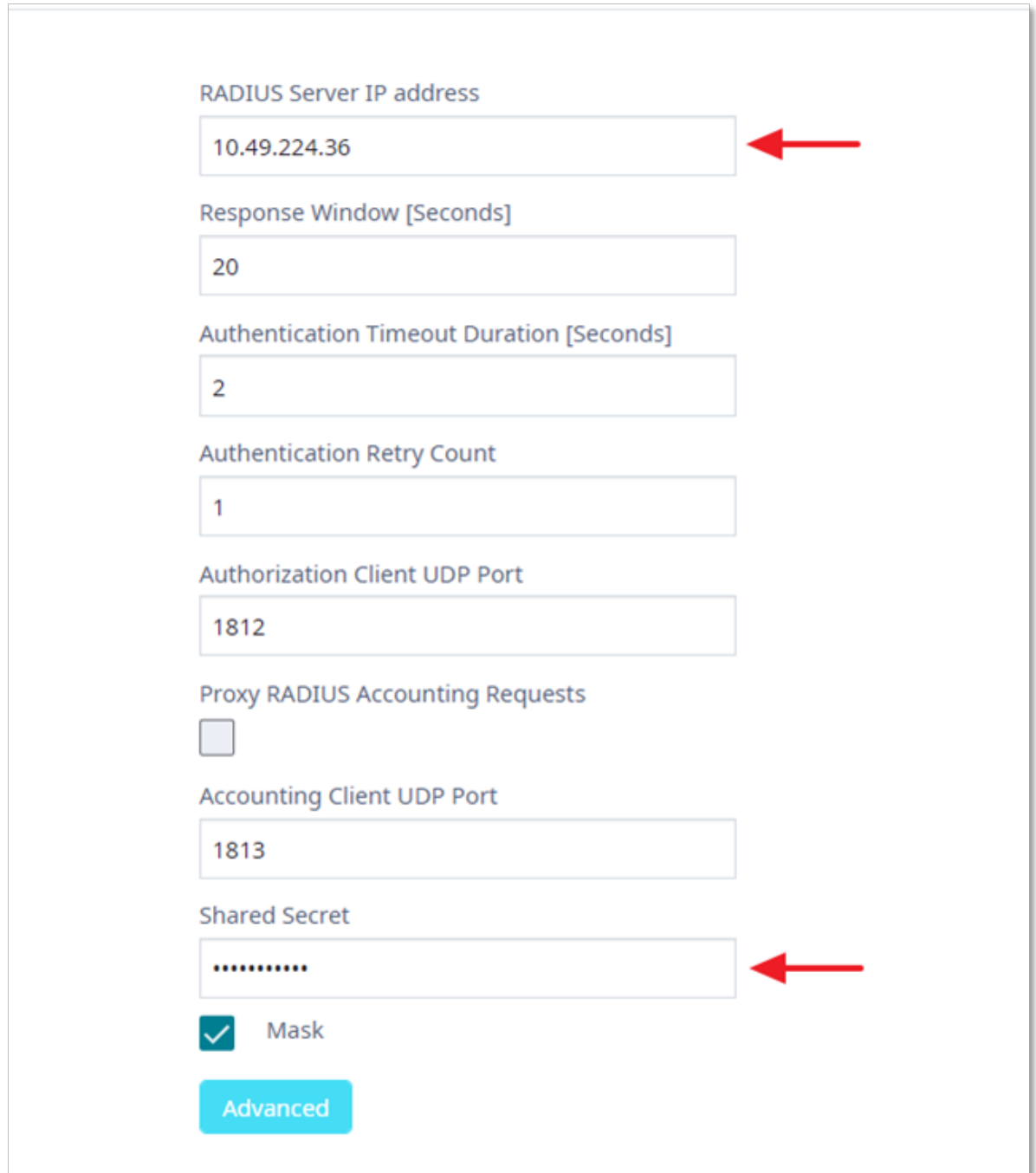
When viewing content online, you can zoom in on screen shots to view them better.

2. Configure the RADIUS server settings

Add a RADIUS authentication server that points to ExtremeControl.

RADIUS server IP address: Accept the default port settings.

Shared Secret: This is the default shared secret used by Xcontrol. This setting can be used for testing and proof of concept. For a real deployment, it is expected that the shared secret will be changed from the defaults. Save the settings.



The screenshot shows a configuration form for a RADIUS server. The fields and their values are as follows:

- RADIUS Server IP address:** 10.49.224.36 (indicated by a red arrow pointing left)
- Response Window [Seconds]:** 20
- Authentication Timeout Duration [Seconds]:** 2
- Authentication Retry Count:** 1
- Authorization Client UDP Port:** 1812
- Proxy RADIUS Accounting Requests:** ☐
- Accounting Client UDP Port:** 1813
- Shared Secret:** (indicated by a red arrow pointing left)
- Mask:** ☒ Mask
- Advanced:** A blue button at the bottom.

3. Add RADIUS Server to Authentication Order

- Go to **Administration > Accounts > RADIUS**.
- Under **Authentication Order**, select **Add** to add the RADIUS option.
- Authentication Order**

Order the servers as Local first and RADIUS second until the configuration has been tested in order to avoid getting locked out of ExtremeCloud IQ Controller management interface due to bad configuration.

d. RADIUS Server

To add the properties of the RADIUS server, under RADIUS Servers, select **Add** and select **IP Address** to display a list of available RADIUS servers.

Enter the NAS IP, NAS ID details and set the authentication method to MS-CHAPv2.

e. **Save** these settings.

ACCOUNTS **RADIUS**

Authentication Order

Order	Authentication Mode
1	LOCAL
2	RADIUS

RADIUS Servers

Order	IP Address	NAS IP Address	NAS ID	Authentication Method
1	10.49.224.60	10.49.224.42	XIQ-C	MS-CHAP v2

Save Test



Note

Do not test the configuration until you have configured ExtremeControl to handle the management access login requests from ExtremeCloud IQ Controller.

ExtremeControl Configuration

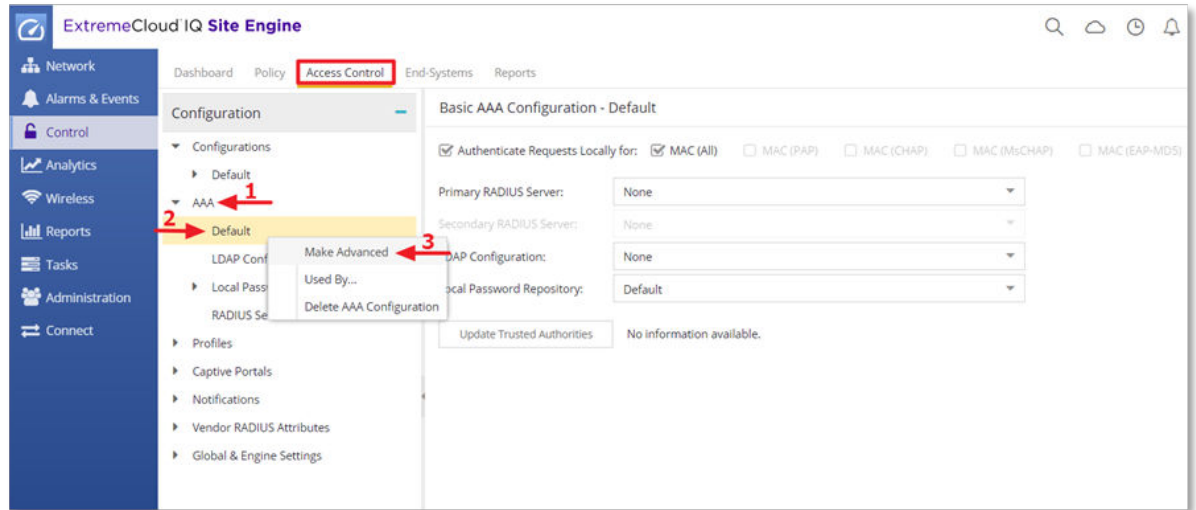
From ExtremeControl, carry out the following overall process:

- Configure AAA authentication rule
- Create an LDAP user group
- Edit the default Administrator policy role
- Add a new rule to the Rule Engine

1. Configure AAA Authentication Rule

To handle the Management Login Access, a AAA authentication rule with Authentication Type *Management* is needed.

- From ExtremeControl main screen, go to **Access Control > AAA > Default**.
- If the AAA authentication rules are not visible, change the view to Advanced: Right-click **Default** and select **Make Advanced**.



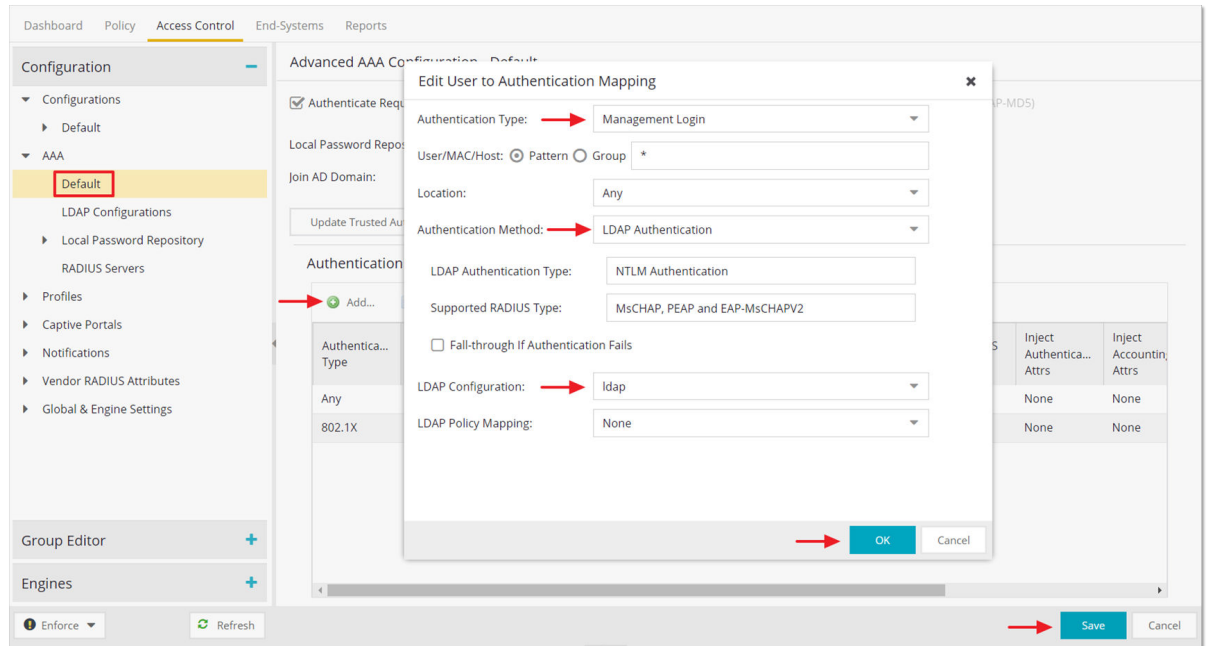
2. ExtremeControl authenticates administrators against a directory service such as Microsoft Active Directory.
 - a. Create a new rule with **Authentication Type** set to Management Login.
 - b. Change the **Authentication Method** to LDAP Authentication. The LDAP Authentication Type should show as NTLM Authentication with the supported RADIUS types.



Note

If using multiple LDAP servers, enable **Fall-through if Authentication Fails** option to authenticate against the next AAA authentication rule in case the first AAA authentication rule results in an authentication failure or the directory service is unreachable.

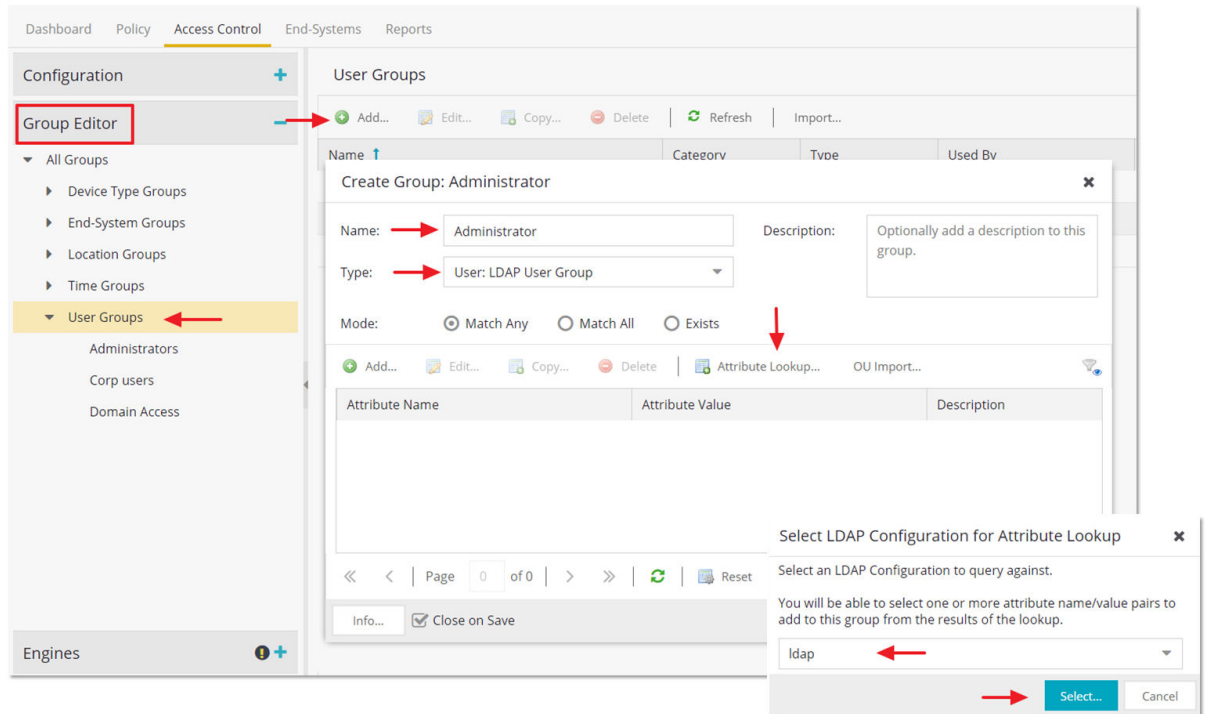
- c. Select the **LDAP policy** from the LDAP Configuration drop-down menu.
- d. Select **Save** to save all changes made to the AAA Authentication Rule.



3. Create an LDAP User Group

In order for Access Control engine to find users in the Microsoft Active Directory, an LDAP user group with a **memberOf** attribute lookup can be used. This LDAP user group is later used as one of the match conditions in the Access Control rule engine.

- To create a new LDAP user group, select the **Group Editor** and select **User Groups** tab.
- Add a new User Group, name it **Administrator**, and change **Type** to **LDAP User Group**.
- To define the user group attributes, select **Attribute Lookup** and then select the available LDAP configuration from the drop-down menu.



4. a. On the next screen, search for a valid username to retrieve LDAP information for this user.
- b. Select the **memberOf** parameter as the key attribute.
- c. Select **Save** to complete the User Group settings.

LDAP Attribute Lookup ✕

User Search Connection Test

sAMAccountName: Ovais Search

<input type="checkbox"/>	Attribute Name	Attribute Value
<input type="checkbox"/>	instanceType	4
<input type="checkbox"/>	lastLogoff	0
<input type="checkbox"/>	lastLogon	133148296733674412
<input type="checkbox"/>	lastLogonTimestamp	133301451889730780
<input type="checkbox"/>	logonCount	43
<input type="checkbox"/>	mail	mqayyum@extremenetworks.com
<input type="checkbox"/>	memberOf	CN=Domain Admins,CN=Users,DC=tmelab,DC=ca
<input checked="" type="checkbox"/>	memberOf	CN=Administrators,CN=Builtin,DC=tmelab,DC=ca
<input type="checkbox"/>	msNPAllowDialin	TRUE
<input type="checkbox"/>	name	Ovais

Add Selected Cancel

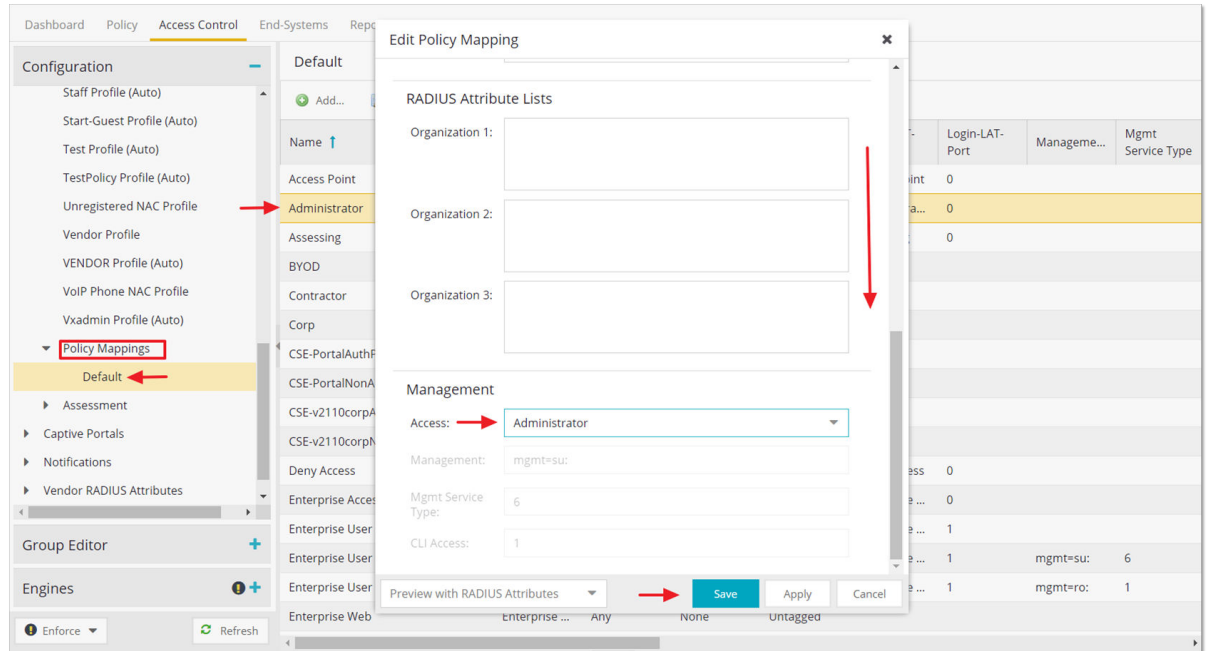
5. Edit Default Administrator Policy Role

- Go to **Configuration > Profiles > Policy Mappings > Default** and select the **Administrator** profile.
- Scroll-down and change the **Access** permission to **Administrator**.
- Save the settings.



Note

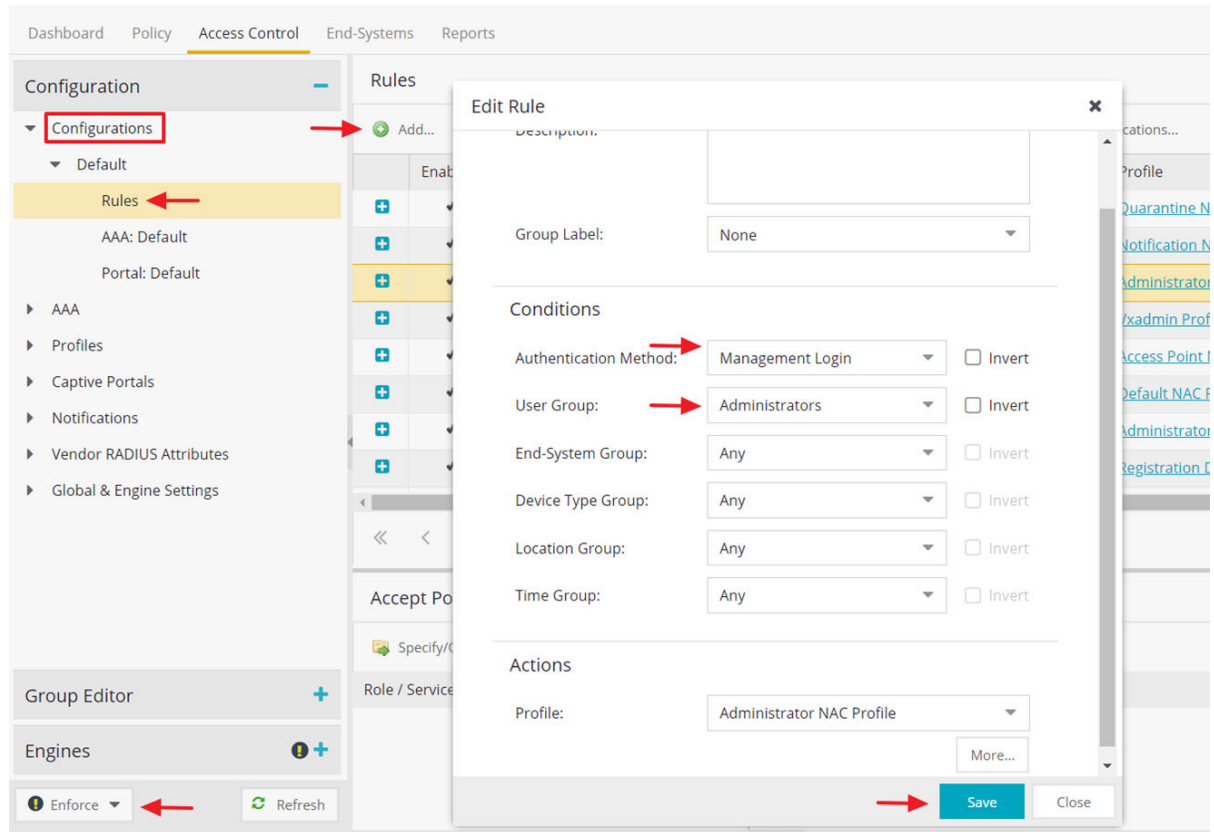
This predefined profile is already set up to enable Super User access for management, if used.



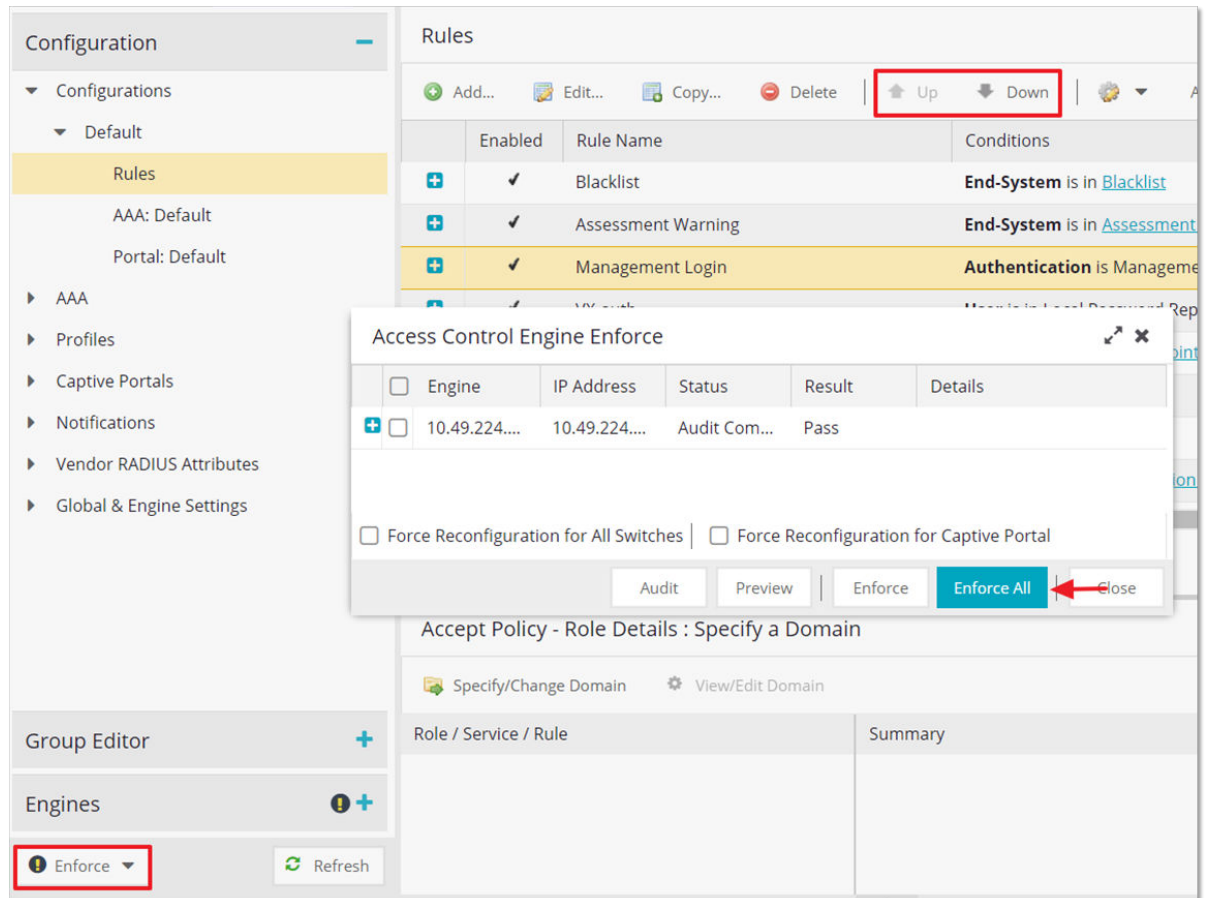
6. Create a New Rule

Create a new Access Control rule so that ExtremeControl can assess the incoming administrative login requests.

- Go to the **Configuration > Default > Rules** tab.
- Select **Add** to add a new rule.
- Set **Authentication Method** to Management Login and **User Group** to the Administrator group you created earlier.

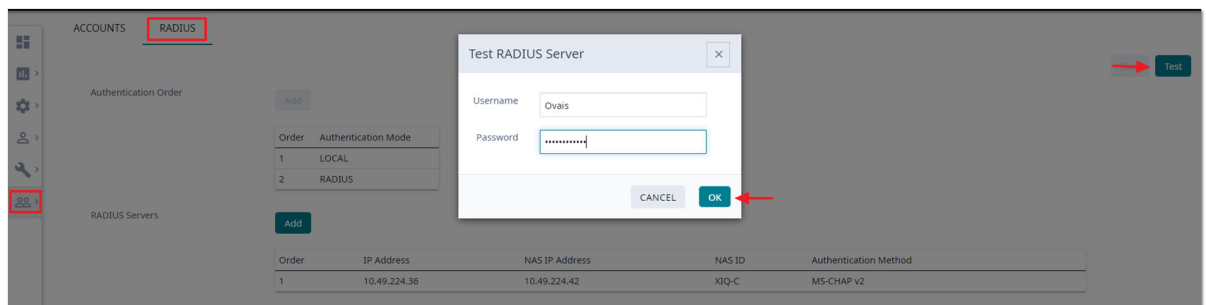


7. a. Select **Administrator NAC Profile** in the **Actions** section. This profile returns the default **Administrator** policy role which has its **Access permissions** set to **Administrator**.
- b. Save the settings to return to the **Rules** screen.
- c. If working with multiple rules to handle authentication for different User or Device Groups, make sure to move the rules UP or Down based on the rule precedence.
- d. Finally, select **Enforce** to enforce the configuration.



Testing and Validation

1. To test the configuration, log into the ExtremeCloud IQ Controller using the local admin account and go to **Administration > Accounts > RADIUS**. Select **Test** to test the login credentials.



2. If the test is successful, you can change the order of Authentication Mode to RADIUS first and Local second. This is to ensure that if the RADIUS server is not reachable, administrators can still access ExtremeCloud IQ Controller using the local admin user account.
3. Go to the event log under **Tools > Logs > Events** to verify the new RADIUS authenticated user with Administrator access permissions is mapped to the internal admin user role.

Search ☐ Exact match

From: past month

To: latest

Advanced Filtering

EVENTS STATION EVENTS AUDIT AP EVENTS

Time	Type	Component	Message
Jun 5, 2023 4:02:33 PM	Info	PAM Log Filter	Jun 5 16:02:33 XIQ-C pam_radauth[1387]: (www) User [admin] has been rejected in authentication on radius server [10.49.224.36].
Jun 5, 2023 3:45:12 PM	Info	PAM Log Filter	Jun 5 15:45:12 XIQ-C gui_s_mgr: pam_unix(www:session): session closed for user admin
Jun 5, 2023 3:44:59 PM	Info	PAM Log Filter	Jun 5 15:44:59 XIQ-C gui_s_mgr: pam_unix(www:session): session opened for user admin by (uid=0)
Jun 5, 2023 3:44:59 PM	Info	PAM Log Filter	Jun 5 15:44:59 XIQ-C pam_radauth[1387]: (www) User [admin] has been rejected in authentication on radius server [10.49.224.36].
Jun 5, 2023 3:31:12 PM	Info	PAM Log Filter	Jun 5 15:31:12 XIQ-C gui_s_mgr: pam_unix(www:session): session closed for user admin
Jun 5, 2023 3:30:50 PM	Info	PAM Log Filter	Jun 5 15:30:50 XIQ-C gui_s_mgr: pam_unix(www:session): session opened for user admin by (uid=0)
Jun 5, 2023 3:30:50 PM	Info	PAM Log Filter	Jun 5 15:30:50 XIQ-C pam_radauth[1387]: (www) User [Ovais], mapped to [admin], has been authenticated successfully. The session will be opened.

Time: Jun 5, 2023 3:30:50 PM
Type: Info
Component: PAM Log Filter
Message: Jun 5 15:30:50 XIQ-C pam_radauth[1387]: (www) User [Ovais], mapped to [admin], has been authenticated successfully. The session will be opened.