

A3 Quick Start Guide

This document is the Quick Start Guide for the A3 system version 3.2.0 or higher. It includes setup and installation instructions as well as multiple demonstrations of A3 authentication.

This version of the Quick Start Guide utilizes an environment in which Registration and Isolation VLANs are NOT used. The distinction between environments that use and don't use VLANs is discussed in the following chapter. A companion guide is available which discusses the VLAN-based environment.

This Quick Start Guide contains all the information and instructions needed to obtain, install, setup, and execute client authentication using an Extreme Networks access point and a server running A3 software.

The authentication techniques available in this guide are:

- **SMS-based authentication.** Users wishing to use an organization's internet connection receive an SMS message with a PIN that they will need to enter in a captive web portal page.
- **Active Directory-based authentication.** Employees wishing to use a organization's network will enter their network credentials, which will be looked up in the local Active Directory. Employees in two specific groups will be assigned to separate VLANs, while all other employees will be assigned to a third. 802.1X and PEAP protocols will be used.

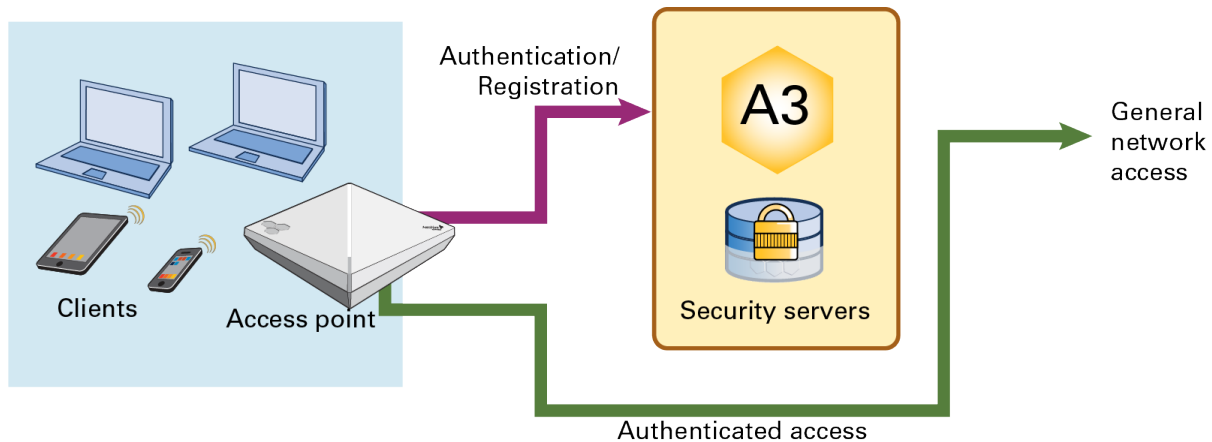
Overview

This A3 Quick Start Guide will guide you through the process of installing and configuring the A3 software for an implementation using multiple forms of external authentication.

Hybrid Out-of-Band Enforcement

This guide assumes that A3 is deployed in hybrid out-of-band mode.

In the figure below, clients use the access network (via an Extreme Networks access point in this case) to seek general network access, typically to an organization's local networks or the Internet.



In this configuration, clients are restricted to communication with the A3 server until they have been authenticated and registered in A3, at which point they are allowed access to the general network. The A3 software, with its included RADIUS server, is used to authenticate clients. A3 serves as the secure access server using information from the supporting databases and networking devices to allow or deny clients access. Clients allowed access can be further restricted by VLAN, firewall rules, and QoS settings orchestrated by A3.

Firewall rules will be used throughout this guide. During the guest authentication process clients are restricted by firewall rules in the access point that isolate them from the general network. Authorized users are then allowed free firewall-based access to the general network, albeit with possible restrictions. VLANs may be used along with firewall rules to restrict access.

Procedure

In broad strokes, the steps involved are:

1. Instantiating, installation, and initial configuration of A3.
2. Configuration of the Extreme Networks access point using ExtremeCloud IQ.
3. Implement an authentication that uses SMS messaging in conjunction with a (CWP) captive web portal. The user enters their cell phone's number. A3 causes an SMS message to be sent to the user with a PIN that is entered into the CWP page.
4. Implement an AD (Active Directory) based authentication that differentiates users based on AD information. Users in the marketing and sales security groups in the organization's AD will be assigned to VLANs that allow them access to potentially different network resources.

Equipment Requirements

To install and operate A3, you will need a computer system that meets the following requirements:

1. An x86-based VMware VSphere Hypervisor (ESXi) host with the following resources available:
 - a. Running version ESXi 6.0 or higher
 - b. 4 CPUs
 - c. 16GB RAM
 - d. 250GB storage
 - e. Access to the management VLAN.
2. An Extreme Networks access point running version 6.5 or newer software, with version 8.3r4 or higher recommended.

Access Requirements

To complete the examples in this guide, you will need logins for the following:

1. ExtremeCloud IQ - a configuration platform for your Extreme Networks access points. You may self-register for a ExtremeCloud IQ account at <https://extremecloudiq.com>.
2. Extreme Networks Community - provides access to the latest A3 software.
3. Active Directory administrative credentials.
4. Administrative access to a ESXi host. If the host is included in a vCenter domain, then access to that domain will be needed as well.

Extreme Networks related logins may be obtained from your Extreme Networks sales manager or other Extreme Networks employee.

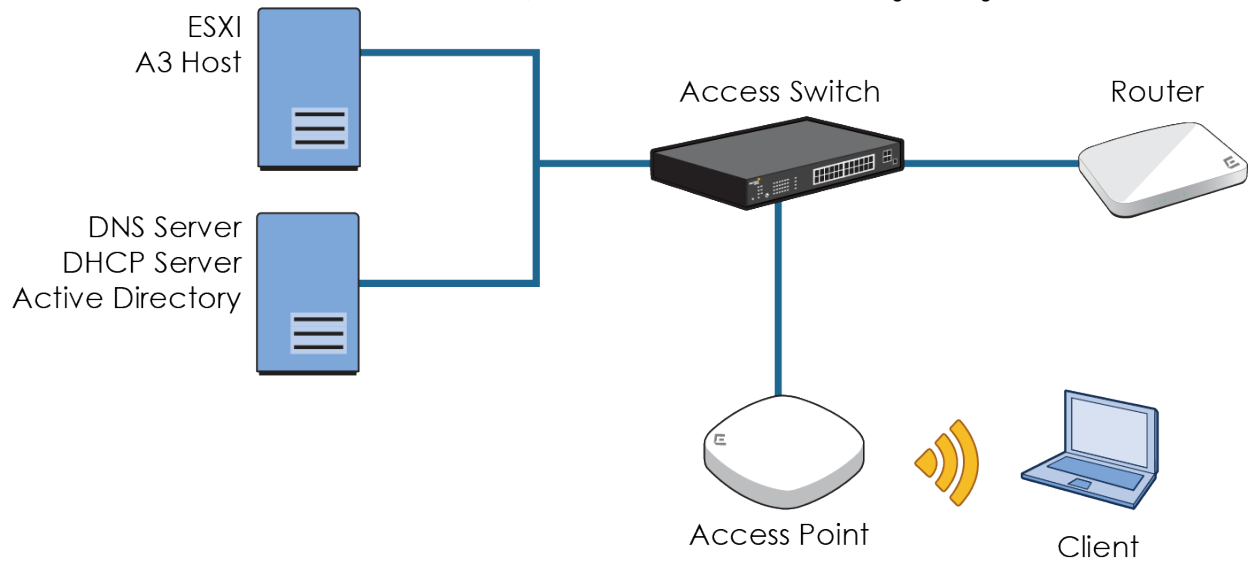
Software Requirements

An OVA file with the A3 software and Linux operating system is available at <https://thehivecommunity.aerohive.com>.

1. Log in to the site.
2. Select Downloads from the top menu bar.
3. Select A3.
4. Select the entry for the file corresponding to the V3 version of A3 ending in OVA.
5. Select Download. The file is larger than a GB; it may take some time to download. Note where you have downloaded the file to.

Network Requirements

Several computer and networking components are required and should be connected as shown below. Layer 2 connectivity is required for the examples in this guide. No VLANs are described here; it is assumed that all devices use a single management VLAN.



The required components are:

Network Component	Usage
A3	ESXi server that is the host for A3. See Equipment Requirements .
DHCP Server	A server used to supply client addresses.
Active Directory Server w/ DNS	A server used to host the local Active Directory and DNS services. It is your responsibility to configure the Active Directory and DNS components.
Access Point	See Equipment Requirements for a description of requirements.
Client	A client computer, cell phone, tablet or other device running a recent version of its operating system. The client must have wireless network connectivity.
Access Switch	
Router	A router connected to a larger network with access to the Internet.

A3 Installation and Initial Configuration

A3 Installation

The A3 software is installed on your ESXi system. Note the available resource requirement detailed in [Equipment Requirements](#). The ESXi web management interface is used to initialize a virtual machine and start A3. vSphere-based operation is similar, but not covered here. The virtual machine may be instantiated by following these instructions:

1. Log in to your ESXi web management interface.
2. Click Create/Register VM and select Deploy a virtual machine from and OVF or OVA file.
3. Click Next and name the virtual machine. This is not the name of the A3 system, only how ESXi will refer to the virtual machine.
4. Click in the box below the name to select the name of the OVA file that you downloaded. See [Software Requirements](#) for instructions on finding and downloading the appropriate OVA.
5. Click Next. Select a datastore from your system that has more than 250GB free.
6. Click Next. Select
 - a. **Network mappings:** The assigned port group may be configured to support VLAN trunking or not. The default port group, called VM Network is by default defined as an access port, with VLAN ID = 0. To configure as a trunk port, set VLAN ID = 4095.
 - b. **Disk provisioning: Thick.**
 - c. **Power on automatically.**
7. Click Next to review your settings.
8. Click Finish to start the installation.
9. When the installation is finished, you can navigate to your A3 virtual machine under Virtual Machines to view the VM settings.
10. Click the black box to open the browser console window. If the display appears as below, then A3 has not been assigned a DHCP address from your network and you must set up A3's basic networking yourself.

```
Welcome to A3.

In order to configure your A3 installation, please connect to the following URL:
https://:1443

A3 login:
```

- a. From the console, enter:
Username: **netcfg**
Password: **aerohive**
- b. Enter ? to see the basic help screen.

```
A3 login: netcfg
Password:
Welcome netcfg it is Thu May 2 21:39:08 UTC 2019
>
help      Display an overview of the CLI syntax
logout   logout console
network  some utility commands for network related details
ping     Ping
reboot   Reboot the system
show     show system related details
> -
```

- c. Enter the following commands to set up your network. Note that the (X) letters used below should not be entered; they refer to a table of suggested address assignments in the next section of this guide.

network ip 10.150.1.4 (A)

network netmask 255.255.255.0 (A)

network gateway 10.150.1.1 (F)

network dns 10.150.1.5 (D)

show network

- d. Verify your settings in the display.
- e. Enter the following commands:

reboot

y

11. The display should appear as below. Note the address shown in that window. This is the temporary (A) address in the following network diagram and table. The IP address assigned to the A3 instance was assigned by DHCP from your assigned server or manually in step 10. This may be changed during initial configuration.

```
A3
CentOS Linux release 7.4.1708 (Core)
[System ID: 2495-6204-EE05-843D-C6AA-381B-FE29-3204]
Kernel 3.10.0-693.11.6.el7.x86_64 on an x86_64
Welcome to A3.

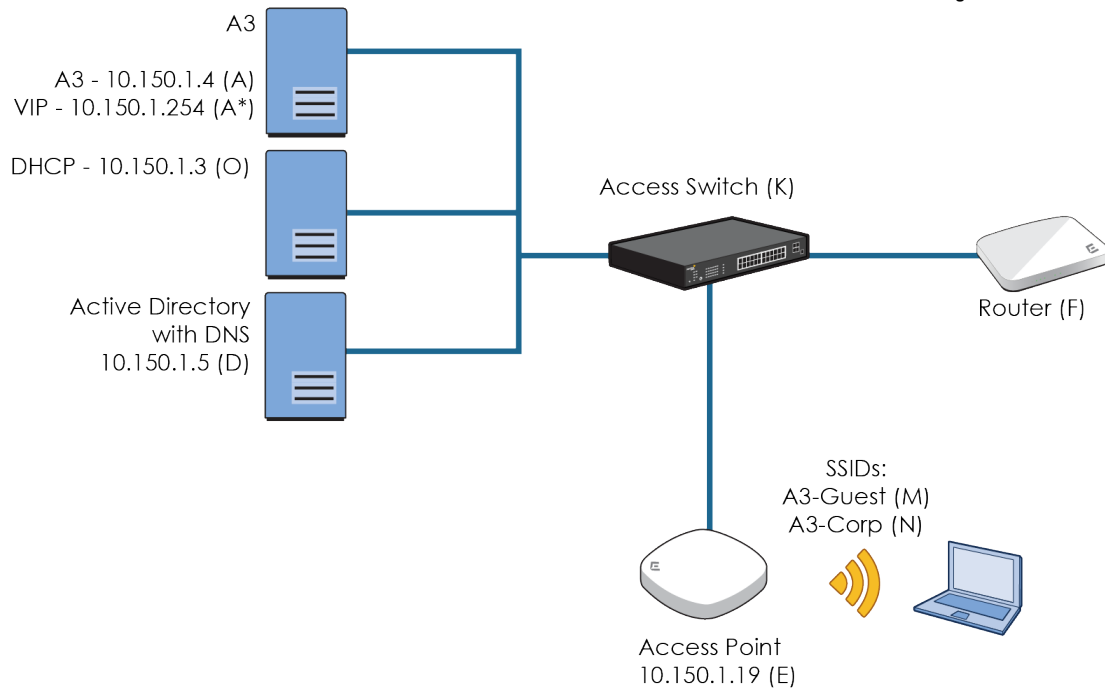
In order to configure your A3 installation, please connect to the following URL:
https://10.150.1.173:1443
```


Network Addresses, VLANs and Other Specifications

A3's initial configuration is based on the network layout shown in [Network Requirements](#). The following figure repeats the network diagram with assigned addresses.

The addresses shown below and in the following chart will be used in this guide in the form **value (X)**. (X) corresponds to the letter in the Key column of the table. The value used in the text will be those present in the Suggested Assignment column of the table. If you use different values in your network, enter them in the Actual Assignment column and use them in your configuration steps.

If you enter or change a value in the Actual Assignment column after configuration, ensure that you make corresponding changes to the elements mentioned in the Dependencies column. The Dependencies column provides references to locations in the A3 and ExtremeCloud IQ GUI where the addresses and VLANs were assigned or used.



It would be a good idea to print out this and the next page for reference.

Table 1: Table of Addresses and VLANs

Key	Usage	Suggested Assignment	Actual Assignment
A	Address of the A3 instance on the ESXi server. This address is initially assigned by DHCP, but can be changed during setup.	10.150.1.4 Netmask 255.255.255.0	
A*	Virtual IP address needed for clusters. Must be in same network as (A).	10.150.1.254	
D	Active Directory (AD) and DNS server.	10.150.1.5	
E	Access Point.	10.150.1.19	
F	Router used to connect to the rest of the network. Must route to the Internet. Should be placed on same network as (A).	Default gateway: 10.150.1.1	
K	Access Switch.		
O	DHCP Server	10.150.1.3	

The following table of other values lists items that are used in form fields.

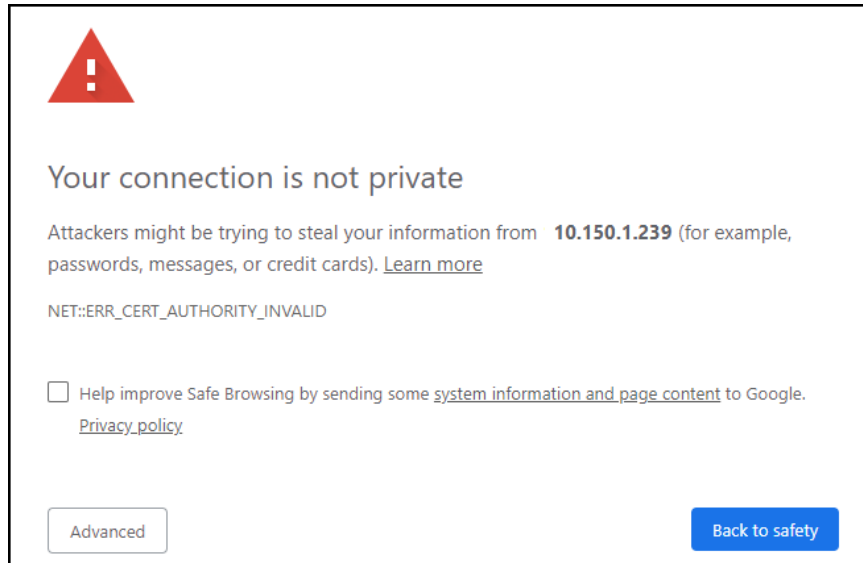
Table 2: Table of Other Values

Key	Usage	Suggested Assignment	Actual Assignment	Dependencies
a	Shared secret for RADIUS communications. This should be a strong password used to protect communications between A3 and the access point.	8AB7thkP		Authentication step , Devices step 3, Devices step 6
b	Guest SSID with Open access.	A3-Guest-NV		Connection Profile step 4
c	Corporate SSID with WPA2-Enterprise encryption.	A3-Corp-NV		Connection Profile step 6
d	Name of the A3 instance.	A3-Eval		A3 Initial Configuration step 5
e	Domain for network.	example.com		A3 Initial Configuration step 12
f	RADIUS Filter_ID for registration role.	registration		Devices step 4
g	RADIUS Filter_ID for isolation role.	isolation		Devices step 4
h	RADIUS Filter_ID for guest role.	guest		Devices step 4, Guest Assignment Rules step 3
i	RADIUS Filter_ID for sales role.	sales		Assignment Rules step 3, Devices step 5
j	RADIUS Filter_ID for marketing role.	marketing		Assignment Rules step 3, Devices step 5
k	RADIUS Filter_ID for employee	employee		Devices step 5

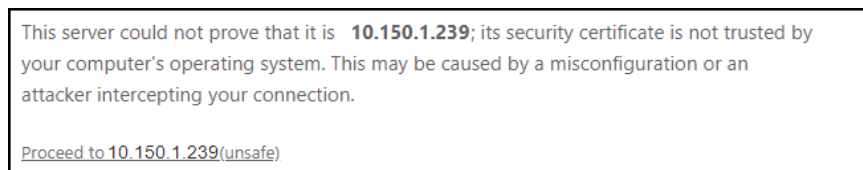
A3 Initial Configuration

The initial configuration of A3 sets up some basic networking and naming parameters. Use the following steps to complete the process.

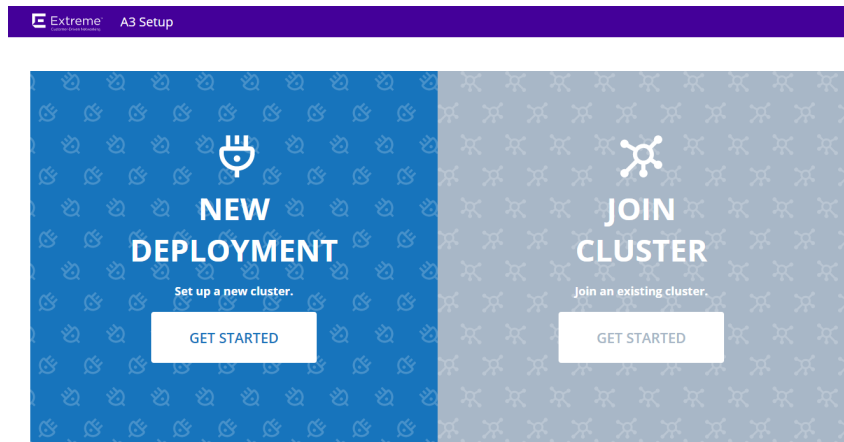
1. Using your browser enter the URL obtained from the last step of [A3 Installation](#). You may receive a warning about your connection not being private, as shown for the Chrome browser¹ below.



2. Click the Advanced button and select Proceed.



3. Select GET STARTED from the New Deployment box.



1. Other browsers may display this and other pages differently. We suggest that you use Chrome for this guide.

- The next screen will ask you for your email address and a password. The email that you enter will be your primary login name going forward. Make sure to use a valid email address that you have access to. Select Next.

- On the next screen you will set the A3's network and VIP addresses. The initial screen is shown below. Make the following changes in the indicated order.

NAME	IP ADDRESS	NETMASK	VIP	TYPE	SERVICES	VLAN
eth0	10.150.1.239 (A)	255.255.255.0	0.0.0.0 (A*)	Management	RADIUS × Portal ×	+ Add VLAN


- VIP.** In the VIP field, enter an address in the same network as the IP ADDRESS. Select an address that will not be assigned by your DHCP server. The VIP address is the main point of contact for network devices and A3. Note that the default VIP field (0.0.0.0) must be erased before entering the new address. Select the to effect the change.
 - IP Address.** Change the IP Address to something that is not in a DHCP pool or remove the address from your DHCP pool. Even though this address was obtained via DHCP, it will now become static, thus you may run into duplicate IP issues if you use an IP that is in the DHCP pool. This will become the (A) address. When is selected, A3 will change the address on the back end. Once finished the page will reload; this may take a few minutes. If for some reason it does not restart, you can refresh it with the [https://<\(A\) address>:1443](https://<(A) address>:1443).
 - Change the host name to something appropriate for your installation. In this guide, we will use **A3-Eval** (d).
- The next screen will ask you if you want to start a 30-day trial of A3. Select START A 30-DAY TRIAL PERIOD unless you have an entitlement key. A key can be entered at a later date, in any case.
 - (Optional) The next screen will ask you to link your A3 instance with ExtremeCloud IQ for monitoring. Enter the ExtremeCloud IQ specifics that you obtained in [Access Requirements](#) and select LINK WITH EXTREME CLOUD IQ ACCOUNT. If you wish to skip this step, select Continue without an ExtremeCloud IQ Account.

8. When A3 says configuration is complete, its services will start. This can take a few minutes. Wait for all services to start.
9. Enter the A3 configuration interface by selecting GO TO ADMINISTRATIVE INTERFACE or invoking the interface via [https://<\(A*\) address>:1443](https://<(A*) address>:1443).
10. Log in with the credentials that you used in step 4.
11. Go to the General Configuration page by selecting CONFIGURATION on the top menu, System Configuration from the left, and General Configuration.
12. Change the Domain to **example.com** (e) and the Time Zone to your local time zone. Note that the U.S. cities are listed under America/<city> and sometimes America/<state>/<city>. Click Save.
13. If you have changed the host name or added a domain name, please restart the haproxy-portal service using the Status > Services interface.
14. Make sure to add an A record for the A3 VIP address to your DNS service. The A record should resolve to the 10.150.1.254 (A*) address.
 - DNS zone: example.com (e)
 - Host name: A3-Eval (d)
 - IP address: 10.150.1.254 (A*)
15. Click ● haproxy-portal ▾ and then Save.

Alerting

Alerting must be set up to receive any messages from A3 and for authentication techniques that involve SMS or email.

1. Select the Alerting tab.
2. Enter the following essential changes:

- a. **Recipients:** one or more email addresses for those who will receive alert messages.
 - b. **SMTP server:** you may fill in a local SMTP server or use GMAIL or any public mail service for which you have credentials. If you wish to use GMAIL, enter **smtp.gmail.com**.
 - c. **SMTP encryption:** enter the type of encryption appropriate for your SMTP server. GMAIL uses ssl.
 - d. **SMTP port:** enter the port number appropriate for your SMTP server. GMAIL uses port 465.
 - e. **SMTP username:** enter the SMTP account name on the SMTP server.
 - f. **SMTP password:** enter the SMTP password associated with the account.
3. Click .

Main Configuration

General Configuration
Alerting
Advanced
Maintenance

Alerting

Recipients

A comma-separated list of email addresses to which notifications of security events with an action of "email" or any other A3-related messages will be sent.

Sender

Email address from which notifications will be sent. If empty, messages will originate from root@<server-domain-name>.

SMTP Server

Server to use for sending messages.

Subject Prefix

Subject prefix for email messages.

SMTP Encryption ssl

Encryption style when connecting to the SMTP server.

SMTP Port

The port of the SMTP server. If the port is set to 0, then the port is determined by the encryption type. none: 25, SSL: 465, StartTLS: 587.

SMTP Username

The username used to connect to the SMTP server.

SMTP Password

The password used to connect to the SMTP server.

SMTP Check SSL

Verify SSL connection.

SMTP Timeout

The email sending timeout, in seconds.

4. Test your SMTP configuration by selecting Tools from the top menu, then SMTP from the left hand menu. Click the START button; the box below will indicate the particulars of the test and its success or failure. If GMAIL is used, the settings on your account may prohibit use from "less secure apps", such as A3. Google "gmail access from less secure apps" and follow instructions to enable access.

Certificate Installation (Optional)

When A3 is installed it generates a self-signed certificate for use in the captive web portal, which will be accessed in the management portal and with URLs that begin with <https://A3-Eval.example.com/> (<https://<a>.<d>/>), corresponding to the value entered on the General Configuration page.

In a production system, you would use a domain that you own and use a public certificate authority to generate a certificate for the A3 CWP. You can do this now, modifying the domain on the General Configuration page and installing your certificate file using the Configuration > System Configuration > Certificates page on A3. All HTTP services (`httpd.aaa`, `httpd.admin`, `httpd.dispatcher`, `httpd.parking`, `httpd.portal`, and `httpd.webservices`) must be restarted after installing HTTPS certificates via A3's GUI: Status > Services.

If you choose to skip this step, when testing A3 your browser may object to the use of A3's WebUI and captive web portal. This might require that you exercise some work-arounds. These work-arounds are covered at the appropriate place.

A3 Initial Configuration Complete

This completes the initial A3 initial configuration.


SMS Authentication with Captive Web Portal

In this A3 example implementation you will perform SMS-based authentication of users desiring to obtain access to the network. Users will receive an SMS message with a PIN that they will need to enter in a captive web portal page. Their device will be registered to the phone number supplied during the registration process.

To do this, we will configure both A3 through its administration interface and the access point through ExtremeCloud IQ.

Extreme Networks ExtremeCloud IQ Configuration


This discussion assumes that you have obtained a ExtremeCloud IQ account as discussed in [Access Requirements](#), that you have logged into that account, and that you have on-boarded your access point.

If you have not yet on-boarded your device yet, select  from the sidebar.

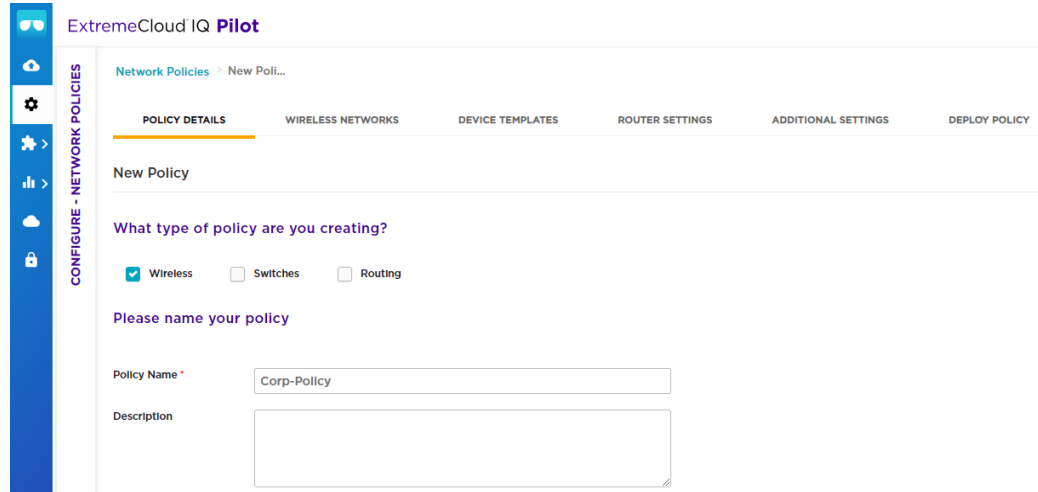
ExtremeCloud IQ will be used to program the Extreme Networks access point used in our SMS example. There are five major steps:

1. [Network Policy](#). The **A3-Guest** (b) SSID is defined.
2. [Authentication](#). Open SSID with MAC authentication is selected.
3. [Guest User Profile](#). Three user profiles to move a user through the registration process are associated with the network policy.
4. [Guest Assignment Rules](#). Rules used to place users in the correct user profile are tied to the user profile.
5. [Deploy Policy](#). The configuration is pushed to the access point.

Network Policy

A new network policy is defined by selecting  from the sidebar and then NETWORK POLICIES. Select ADD NETWORK POLICY.

1. Fill in the Policy Details: check the Wireless box only and enter **Corp-Policy** as the Policy Name.



ExtremeCloud IQ **Pilot**

Network Policies > New Poli...

POLICY DETAILS WIRELESS NETWORKS DEVICE TEMPLATES ROUTER SETTINGS ADDITIONAL SETTINGS DEPLOY POLICY

New Policy

What type of policy are you creating?

Wireless Switches Routing

Please name your policy

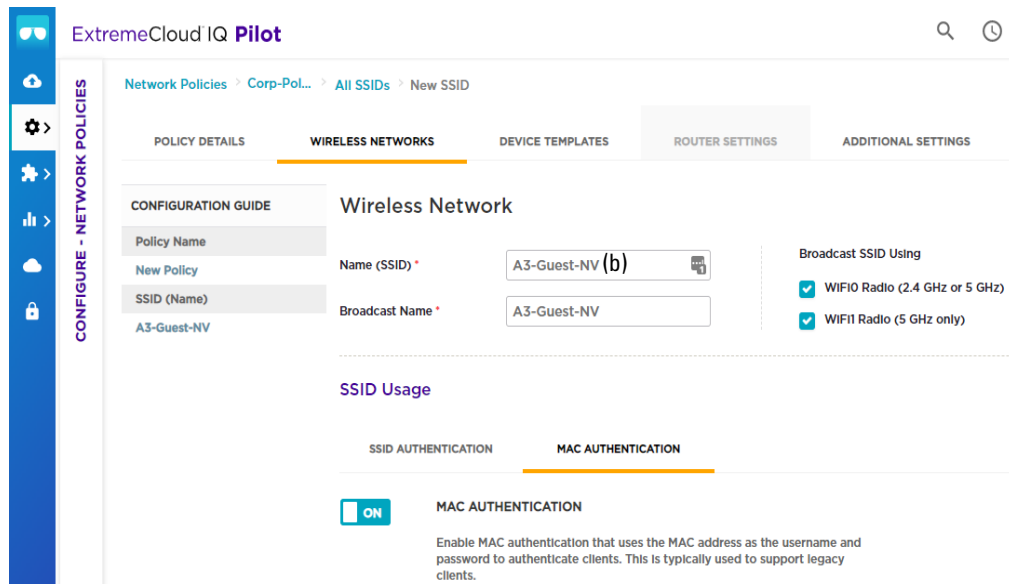
Policy Name *

Description

2. Click **SAVE** to move to the Wireless Networks tab.
3. Select ADD NETWORK and then All Standard Network.
4. Enter **A3-Guest** (b) in the Name (SSID) field. The Broadcast Name is automatically filled in as A3-Guest as well.

Authentication

1. Since the SSID will be used for guest access, select **Open Unsecured**. This means that users will not need to enter any credentials to associate with the SSID, nor will any 802.1x credentials be transmitted. Open unsecured also means that data is not encrypted over the air, which is suitable for guest access but not sensitive employee data.
2. Select the **MAC Authentication** tab and enable **MAC Authentication**. This supplies the user's device's MAC address to A3 to determine device registration status.



ExtremeCloud IQ **Pilot**

Network Policies > Corp-Pol... > All SSIDs > New SSID

POLICY DETAILS WIRELESS NETWORKS DEVICE TEMPLATES ROUTER SETTINGS ADDITIONAL SETTINGS

CONFIGURATION GUIDE

Policy Name
New Policy

SSID (Name)
A3-Guest-NV

Wireless Network

Name (SSID) *

Broadcast Name *

Broadcast SSID Using

WiFi Radio (2.4 GHz or 5 GHz)

WiFi Radio (5 GHz only)

SSID Usage

SSID AUTHENTICATION MAC AUTHENTICATION

ON **MAC AUTHENTICATION**

Enable MAC authentication that uses the MAC address as the username and password to authenticate clients. This is typically used to support legacy clients.

3. A RADIUS Server group is defined next. This is a set of RADIUS servers that can be queried by access points. In this example, we will only be adding one RADIUS server, our A3 instance. Click the **+** sign beside Default RADIUS Server Group.
4. In the Configure RADIUS Servers dialog, select **EXTREME A3 (0)** and click the **+** sign to add a new RADIUS server. Note: If you are using the on-premises version of ExtremeCloud IQ, then:
 - a. The on-premises version of ExtremeCloud IQ does not offer an EXTREME A3 category, select EXTERNAL RADIUS SERVER (0) instead.
 - b. Select the gear icon (⚙️). In the dialog presented ensure that CoA (RFC3576) is enabled.

Configure RADIUS Servers

RADIUS Server Group Name * RADIUS Server Group Description ⚙️

EXTERNAL RADIUS SERVER (0) | EXTREME NETWORKS A3 (0) | EXTREME NETWORKS RADIUS SERVER (0)

⚙️ **+** 🗑️

Name	IP/Host Name
------	--------------

1 Do not change the Server Type Authentication or Accounting ports from 1812 and 1813, respectively.

5. Fill in the Extreme Networks A3 Server dialog:
 - a. **Name:** **A3-RADIUS**.
 - b. **Description:** as desired.
 - c. **IP/Host Name:** use the **+** sign to add the A3 VIP address **10.150.1.254 (A*)** as the Name and IP Address.
 - d. **Shared Secret:** **8AB7tHkP (a)**. This is used to hash and unhash information exchanged with the A3 server. Remember this setting; it must be used during A3 configuration.
 - e. Click SAVE EXTREME A3.
 - f. Enter **A3-RADIUS-SERVER-GROUP** in the RADIUS Server Group Name field, check the box next to **A3-RADIUS** and click SAVE RADIUS.

Aerohive A3 Server

Aerohive A3 Server


Name *

Description

IP/Host Name * ⚙️ **+** 🗑️

Server Type * Authentication Port: *
 Accounting Port: *

Shared Secret Show Password



6. The means by which A3 ensures proper guest access by sending RADIUS attributes to the access point upon MAC authentication. The access point uses these attributes to assign user profiles. To start authentication, every user must register with A3. The default profile is used when no RADIUS attribute rules have been satisfied, placing the user in the Registration state. Continue down the screen past Authenticate via RADIUS Server to User Access Settings.
7. Select the **+** sign on the line containing Default User Profile to access the Create User Profile dialog.
 - a. Enter **Registration-NV** in the User Profile Name.
 - b. If the VLAN number listed is not your management VLAN, then select  sign.
 - i. If your management VLAN is in the list, select it.
 - ii. If not, select **New**, and then define your new VLAN number. Enter the number in both the Name and VLAN ID fields.
 - c. Select **SAVE VLAN**.
8. Turn on Firewall Rules and then name the IP Firewall **Registration-NV-FW**.

Create User Profile

User Profile

User Profile Name *

Connect to * VLAN VLAN Group




 **+** 



SECURITY TRAFFIC TUNNELING QoS AVAILA

ON Firewall Rules

IP Firewall MAC Firewall



IP Firewall Name *

+   




9. Firewall rules must now be defined to ensure that users in the registration state can only access the services and places that are needed for registration.
 - a. Press the **+** sign to define the first firewall rule.
 - b. The first rule allows the client to communicate with the A3 server using any protocol.
 - i. Select the , select any from the list, and then select **ADD SERVICE**.
 - ii. Select the  beside Destination IP, and then the IP address of the A3 server, 10.150.1.254 (A*).




New Firewall Rule (Outbound Traffic)


New Firewall Rule (Outbound Traffic)


Service  

Any x

Source IP *   

Destination IP *   

Action 

Logging 

- iii. Select SAVE FIREWALL RULE to save the rule.
- d. Similarly define additional rules as per the table below in the order indicated.

Services	Source IP	Destination IP	Action
DHCP-Client, DHCP-Server, DNS	any	any	Permit
HTTP, HTTPS	any	any	Redirect
any	any	any	Deny

- e. Set the Redirecting URL to **https://A3-Eval.example.com/Aerohive::AP**. This invokes A3 when a registering user attempts to reach any web page.
- f. The resulting User Profile should now appear as show below.

Create User Profile



User Profile

User Profile Name * Connect to * VLAN VLAN Group
 +

SECURITY

TRAFFIC TUNNELING

QoS

AVAILABILITY SCHEDULE

CLIENT SLA

DATA/TIME LIMIT

 ON

Firewall Rules

IP Firewall

MAC Firewall

IP Firewall Name * Redirecting URL * Prevent Apple CNA (Captive Network Assistant) application from requesting credentials

Outbound Traffic

Permit

SOURCE IP	DESTINATION IP	SERVICE	ACTION	LOGGING	ORDER
<input type="checkbox"/> Any	10.150.1.254	Any	PERMIT	OFF	↑ ↓
<input type="checkbox"/> Any	Any	DHCP-Client	PERMIT	OFF	↑ ↓
<input type="checkbox"/> Any	Any	DHCP-Server	PERMIT	OFF	↑ ↓
<input type="checkbox"/> Any	Any	DNS	PERMIT	OFF	↑ ↓
<input type="checkbox"/> Any	Any	HTTP	REDIRECT	OFF	↑ ↓
<input type="checkbox"/> Any	Any	HTTPS	REDIRECT	OFF	↑ ↓
<input type="checkbox"/> Any	Any	Any	DENY	OFF	↑ ↓






10. Select **SAVE USER PROFILE** to save the new user profile.
11. Back at the Wireless Network definition page, select **Apply a different user profile to various clients and user groups**. This enables the use of multiple user profiles on a single SSID.
12. Select **Allow user profile assignment using RADIUS attributes in addition to three tunnel RADIUS attributes**. This results in a selection of Standard RADIUS Attribute and a value of 11_Filter-Id. This means that the access point's profile assignment will key off of the value of the 11_Filter-Id RADIUS attribute received from A3.

User Access Settings



Configure your QoS, VLAN, Firewall policies, and Traffic Tunneling

Default User Profile **Registration-NV**
VLAN : 1 + Apply a different user profile to various clients and user groups. Allow user profiles assignment using RADIUS attributes in addition to three tunnel RADIUS attributes. Standard RADIUS Attribute Vendor specific RADIUS Attribute

Guest User Profile

1. Select  above User Profile Name to obtain create a Guest User Profile with a different set of firewall rules. The management VLAN (VLAN1) will continue to be used. Enter **Guest-NV** into the User Profile Name.
2. If your management VLAN is not displayed, select the  icon to select the correct VLAN.
3. Turn on Firewall Rules.
4. Name the IP Firewall **Guest-NV-FW**.
5. Select the  icon beneath the IP Firewall Name, select Guest-Internet-Access-Only, and then . This denies access to any internal networks.
6. Select .

Guest Assignment Rules




1. After the Guest-NV-FW profile have been created, it is necessary to tell the access point to assign the profile when A3 sends back the proper RADIUS attribute. Select the  on the Guest line in the Assignment Rules column.
2. Enter the name **Guest-Rule-NV** in the Name field, click the  symbol, and select RADIUS Attribute.

User Profile Assignment

Name
Guest-Rule-NV

Description
Allow guest access

Assign user profiles to clients or users connecting to an SSID according to authentic assignment.

RADIUS Attribute	Value
Client OS Type	
Client MAC Address	No rules four
Client Location	
Schedule	

3. Note that 11_Filter-Id has been preselected. Fill in the Attribute Values field with **guest(h)**. It is important that the value be entered in this way, since the field is case sensitive and it must match an entry we will make in A3. Click OK and then SAVE.





A single standard RADIUS Attribute Value Pair




RADIUS Attribute 11_Filter-Id

Attribute Values

Isolation User Profile

An isolation user profile is necessary to handle exception cases signaled by A3. A3 will send the access point a isolation RADIUS attribute in that case, which will be treated as a return to registration state.


1. Select  above User Profile Name and select **Registration-NV**.
2. Select the  on the Guest line in the Assignment Rules column.
3. Enter the name **Isolation-Rule-NV** in the Name field, click the  symbol, and select RADIUS Attribute.
4. Note that 11_Filter-Id has been preselected. Fill in the Attribute Values field with **isolation (g)**. It is important that the value be entered in this way, since the field is case sensitive and it must match an entry we will make in A3. Click OK and then SAVE.
5. Under Assignment Description click the  button to expand both descriptions. The display should appear as below. Click SAVE.

   The IQ Engine with version prior to 8.1r1 only support 16 user profile policy rules.

USER PROFILE NAME	VLAN/VLAN GROUP	ASSIGNMENT RULES	ASSIGNMENT DESCRIPTION	ORDER				
<input type="checkbox"/> Guest-NV	1	  Guest-Rule-NV	▼ Allow guest access <table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>RADIUS Attribute</td> <td>guest(h)</td> </tr> </tbody> </table>	Type	Value	RADIUS Attribute	guest(h)	↑ ↓
Type	Value							
RADIUS Attribute	guest(h)							
<input checked="" type="checkbox"/> Registration-NV	1	  Isolation-Rule-NV	▼ For isolation, move back to Registration state <table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>RADIUS Attribute</td> <td>isolation (g)</td> </tr> </tbody> </table>	Type	Value	RADIUS Attribute	isolation (g)	↑ ↓
Type	Value							
RADIUS Attribute	isolation (g)							

Deploy Policy

Before continuing, note the IP Address of your access point, this corresponds to the (E) address in table.

Select the Deploy Policy tab, then check the box for your access point, and then . Check Update Network Policy and Configuration and select Complete Configuration Update. Click PERFORM UPDATE.

Device Update
✕

1 device will be updated

Update Network Policy and Configuration

Delta Configuration Update
Update device with changed configuration.




Complete Configuration Update
Update device with all configurations. Used to reset device to ExtremeCloud IQ configuration settings.

Upgrade IQ Engine and Extreme Network Switch Images

Activation Time for Extreme Networks Devices Running Images

Activate at next reboot (requires rebooting manually)

Activate after seconds

This completes the ExtremeCloud IQ configuration.

A3 Configuration

A3 configuration requires definition or modification of several A3 settings:

1. [Roles](#) - classifies the type of user and the number of concurrent devices a user with this label can have. In this case, a predefined guest role will be used.
2. [Authentication Sources](#) - defines how user information is to be gathered and ties users to roles. The predefined sms authentication source will be used.
3. [Devices](#) - defines the network devices that authenticate clients against A3, in this case the Extreme Networks access point.
4. [Connection Profile](#) - ties together the authentication source with a connection source, in this case an access point's A3-Guest SSID.

When configuration is completed, an SMS-based authentication will be tested, and audit logs will be examined.

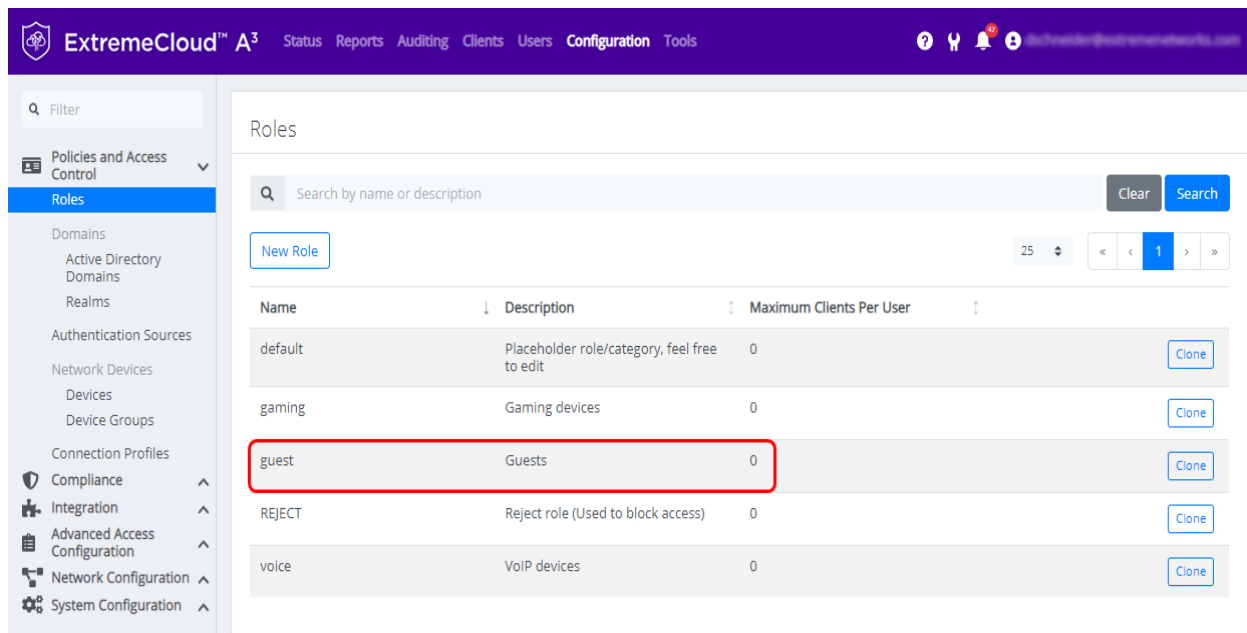
Start by entering the A3 configuration interface, either continuing from the initial installation or invoking the interface via [https://<\(A\) address>:1443](https://<(A) address>:1443).

Roles

Roles are accessed through the following steps:

1. Select Configuration at the top of the page.
2. Select Policies and Access Control.
3. Select Roles.

The list of predefined roles is shown. Verify that the guest role is visible.



The screenshot displays the 'Roles' configuration page in the ExtremeCloud A3 interface. The page features a search bar at the top with the text 'Search by name or description' and buttons for 'Clear' and 'Search'. Below the search bar is a 'New Role' button and a pagination control showing '25' items per page and a page number '1'. The main content is a table with the following data:

Name	Description	Maximum Clients Per User	
default	Placeholder role/category, feel free to edit	0	Clone
gaming	Gaming devices	0	Clone
guest	Guests	0	Clone
REJECT	Reject role (Used to block access)	0	Clone
voice	VoIP devices	0	Clone

Authentication Sources

The next steps involve selection and modification of the SMS authentication source.

1. Select Authentication Source from the list on the left, below Roles.
2. Click the **sms** source in the External Sources box.

The screenshot shows the 'External Sources' configuration page in the ExtremeCloud A3 interface. A sidebar on the left contains navigation options like 'Policies and Access Control', 'Roles', 'Domains', and 'Authentication Sources'. The main area displays a table of external sources:

	Name	Description	Type
1	sms	SMS-based registration	SMS
2	email	Email-based registration	Email
3	sponsor	Sponsor-based registration	SponsorEmail
4	null	Null Source	Null

3. The sms dialog is displayed. The SMS Carriers box is pre-populated with a large number of supported carriers. You may leave the list alone, or pare it down. In the screen shot below, the list has been reduced to a few US carriers.
4. Scroll to Authentication Rules > Rule - catchall () at the bottom of the page.

The screenshot shows the 'Authentication Source sms' configuration dialog. The 'SMS Carriers' field is highlighted with a red box and contains a list of carriers: AT&T Wireless, T-Mobile, US Cellular, Verizon, and Google Project Fi. Below this, the 'Authentication Rules' section shows a single rule named 'catchall' selected with a red box. The rule configuration includes:

- Name: catchall
- Description: (empty)
- Matches: All
- Conditions: Add Condition
- Actions:

1	Role	guest
2	Access duration	1 day

- The **catchall** Authentication Rule states that anyone authenticating against this source will be assigned to the role of guest and allowed to use the network for 1 day before needing to re-register. No modification to this rule is required.
- Click **Save** to save the authentication source.

Devices

Device configuration is next:

- Click Devices beneath Network Devices. The list of predefined entries is displayed.

The screenshot shows the 'Network Devices' configuration page in ExtremeCloud IQ. The 'Devices' tab is active, displaying a table of predefined entries. A 'New Device' dropdown menu is open, showing 'Aerohive_AP' selected. The table contains two entries:

Description	Group	Type	Mode	Actions
Test Access Point	Aerohive_AP	Aerohive::AP	production	Delete Clone
Test Range of Access Points	Aerohive_AP	Aerohive::AP	production	Delete Clone

- A device for our access point must be defined. Click the New Device drop down control and then select **Aerohive_AP**.
- In the New Device form, enter the IP address of your access point **10.150.1.19** (E) or an entire subnet using CIDR format in the IP Address/MAC Address/Range (CIDR) field, enter a Description, and ensure that the Use CoA box is checked.

The screenshot shows the 'Device 10.150.1.19' configuration form. The 'Definition' tab is active. The 'IP Address/MAC Address/Range (CIDR)' field is set to '10.150.1.19 (E)'. The 'Description' is 'QSG AP', 'Type' is 'Aerohive::AP', 'Mode' is 'production', and 'Device Group' is 'Aerohive Access Points'. The 'Deauthentication Method' is 'RADIUS'. The 'Use CoA' checkbox is checked.

- Select the Roles tab, enabling **Advanced**.
- Disable all but **Role by Device Role**.

6. Enter **registration** (f), **isolation** (g), and **guest** (h) next to the same-named entries. This dictates which RADIUS value will be returned to the access point for each A3 role and must match what was entered in [Guest Assignment Rules](#) step 3. Values are case sensitive.

Role Mapping by VLAN ID

Role by VLAN ID

Role Mapping by Device Role

Role by Device Role

registration	registration	(f)
isolation	isolation	(g)
macDetection		
inline	inline	
default		
guest	guest	(h)
gaming		
voice	voice	
REJECT		

Role Mapping by Access List

Role by Access List

Role Mapping by Web Auth URL

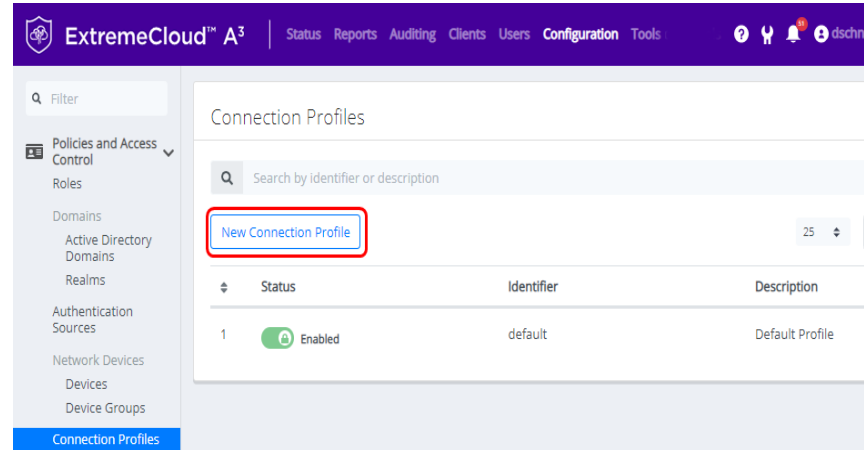
Role by Web Auth URL

7. Select the RADIUS tab. Enter **8AB7tHkP** (a) into the Secret Passphrase field. This matches the setting entered in the ExtremeCloud IQ in [Authentication](#). Click [Create](#).

Connection Profile

The connection profile ties together the access point's SSID with authentication sources. To define a new profile:

1. Select Configuration > Connection Profiles > New Connection Profile.



2. Fill in a profile name and description.

The screenshot shows the configuration form for a new connection profile. The 'Profile Name' field is set to 'Guest-Connection-NV' with a note that profile IDs may only contain alphanumeric characters. The 'Profile Description' field is set to 'Guest access using SMS, no reg vlan'. The 'Enable Profile' toggle is turned on. The 'Root Portal Module' is set to 'Default portal policy' with a note that it is the root portal module to use.

3. Uncheck **802.1X Recompute Role from Portal** since we are not using **802.1x authentication** in this example.
4. Under Filters, click **Add Filter**, select SSID from the list, and enter **A3-Guest (b)** next to SSID. This tells A3 to use this connection profile when anyone connects to the access point using the **A3-Guest (b)** SSID.
5. Under Sources, select **Add Source**, and then select sms as the authentication source. This tells A3 to authenticate users against the sms authentication source.

The screenshot shows the filter and source configuration sections. The 'Filter' section has one filter with the name '1', the field 'SSID', and the value 'A3-Guest-NV (b)'. The 'Sources' section has one source with the name '1' and the value 'sms'.

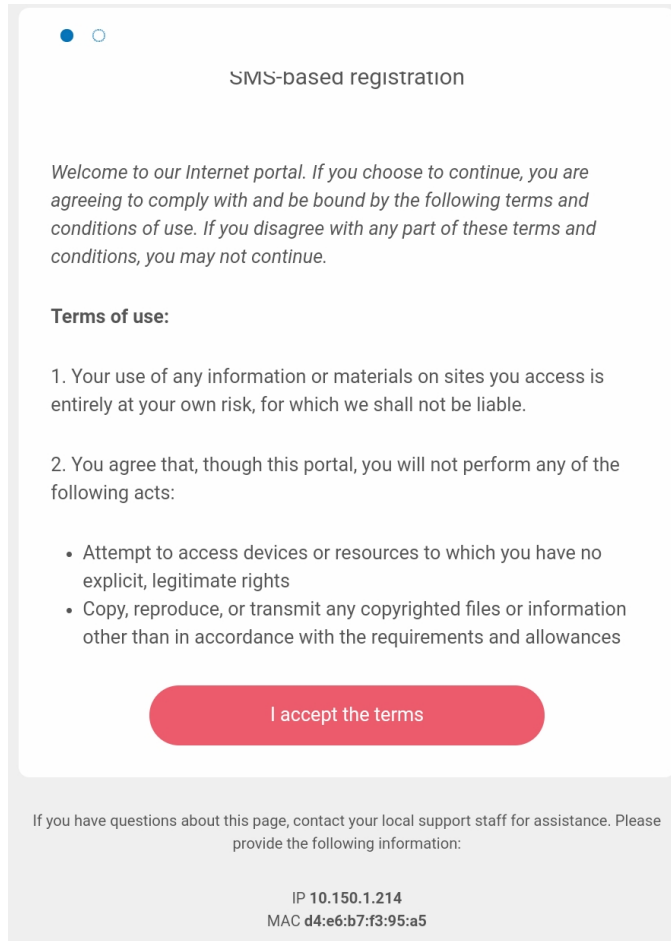
6. Click **Create**.

Testing the SMS Example

To test the A3 and ExtremeCloud IQ configurations for SMS authentication, use a laptop, smart phone, or tablet to connect to the **A3-Guest** (b) SSID.

Depending on your configuration, your default browser might automatically open with a reference to the URL <https://A3-Eval.example.com/> (`https://<a>.<d>/`), or it may be necessary for you to reference a popular web site such as <http://aerohive.com> (note that `http://` must be used and **not** `https://`).

If your browser complains about the site or certificates, please reread the [Certificate Installation \(Optional\)](#) section of this guide. The browser warnings relate to the use of a default self-signed certificate on A3. If you persist¹, you should be able to obtain a web page that begins with:



SMS-based registration

Welcome to our Internet portal. If you choose to continue, you are agreeing to comply with and be bound by the following terms and conditions of use. If you disagree with any part of these terms and conditions, you may not continue.

Terms of use:

1. Your use of any information or materials on sites you access is entirely at your own risk, for which we shall not be liable.
2. You agree that, though this portal, you will not perform any of the following acts:
 - Attempt to access devices or resources to which you have no explicit, legitimate rights
 - Copy, reproduce, or transmit any copyrighted files or information other than in accordance with the requirements and allowances

[I accept the terms](#)

If you have questions about this page, contact your local support staff for assistance. Please provide the following information:

IP 10.150.1.214
MAC d4:e6:b7:f3:95:a5

Looking at the bottom of the page, the IP address is from the management network (VLAN 1): 10.150.1.214.

1. This might involve selecting Advanced or Details and then accepting warnings. In some Chrome versions it is necessary to disable a check by entering a URL of <chrome://flags/#allow-insecure-localhost> and then Enable that option.

Scrolling the web page down you will be asked to accept the use policy. Select that to receive a screen that asks you for your phone number and choice of mobile carrier.

SMS-based registration

TELEPHONE
1234567890

MOBILE PROVIDER
AT&T Wireless

Continue

When you click Continue, A3 will email your mobile number at your carrier and the SMS will come through with a PIN. The PIN is then entered into the web page, followed by Continue.

↻

PIN
9 2 5 0 4 2 | ×

Continue

[I don't have a PIN](#)

A success page is displayed with a progress bar letting you know you are being moved to the user VLAN.

When the progress bar has finished, you will be in the guest VLAN. Your browser is redirected to the site that is predefined in the Captive Portal section of the [Connection Profile](#). You can also test this by selecting extremenetworks.com or other site in your browser address bar.

Verifying Operation

In addition to successful authentication and network access, you can use A3's auditing function to check on the status of the authentication. Select Auditing from the top menu bar and use the Search facility to look for the client device; in this case the search was for the last component of the client's device (:a5). Items are displayed in reverse order. You should see an Unregistered status for your client followed in time by a Registered status.

The screenshot shows a search bar with ':a5' entered and 'Search' button. Below the search bar is a table with columns: Created At, ID, Auth Status, Server IP, MAC Address, Client Status, User Name, NAS IP Address, and NAS Port Type. The table contains three rows of data, with the most recent entry at the top.

Created At	ID	Auth Status	Server IP	MAC Address	Client Status	User Name	NAS IP Address	NAS Port Type
07/15/2020 06:33 PM	7	Accept	10.150.1.4	d4:e6:b7:f3:95:a5	Registered	d4e6b7f395a5	10.150.1.19	Wireless-802.11
07/15/2020 05:50 PM	6	Accept	10.150.1.4	d4:e6:b7:f3:95:a5	Unregistered	d4e6b7f395a5	10.150.1.19	Wireless-802.11
07/15/2020 12:13 AM	1	Accept	10.150.1.4	d4:e6:b7:f3:95:a5	Unregistered	d4e6b7f395a5	10.150.1.19	Wireless-802.11

If you click the MAC Address for the row (00:08:ca:e1:da:21 in this case), you can see the status of the node associated with the client device.

MAC d4:e6:b7:f3:95:a5

The screenshot shows a details page for the MAC address d4:e6:b7:f3:95:a5. It has tabs for Edit, Info, Fingerbank, Timeline, IPv4, IPv6. The IPv4 tab is active, showing fields for Owner, Status, and Role.

Field	Value
Owner	[Redacted]
Status	Registered
Role	guest - Guests

The Owner will be the phone number used to obtain the PIN, the Status will be Registered and the Role will be guest.

If you intend to retest with the same client, then you need to ask A3 to forget the device registration. In the same dialog as above, erase Owner, change Status to Unregistered, change Role to No Role and click the small 'x' in Role to reset it to No role. Click SAVE.

SMS Example Complete

This completes the SMS Authentication example for A3.


Active Directory Authentication

In this A3 example you will perform differentiated authentication based on Active Directory information. Users in marketing and sales security groups in the organization's Active Directory will be assigned to user profiles that allow them access to potentially different network resources. Users in neither group will be assigned to a third VLAN.

In this chapter, you will configure both the access point through ExtremeCloud IQ and A3 through its administration interface.

ExtremeCloud IQ Configuration

This discussion assumes that you have obtained a ExtremeCloud IQ account as discussed in [Access Requirements](#), that you have logged into that account, and that you have on-boarded your access point.

If you have not yet on-boarded your device yet, select  from the sidebar.

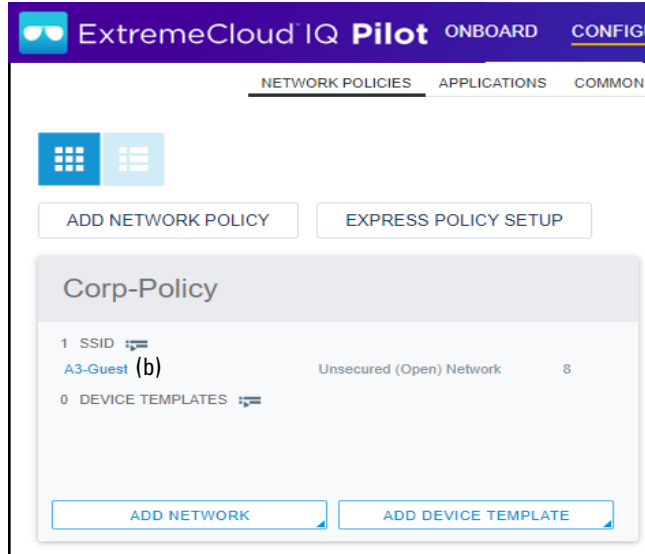
The ExtremeCloud IQ will be used to program the Extreme Networks access point used in this Active Directory example. There are five major steps:

1. [Network Policy](#). The **A3-Corp-NV** (c) SSID is defined.
2. [Authentication](#). Enterprise authentication is selected.
3. [User Profiles](#). Three user profiles that move a user through the authentication process are associated with the network policy.
4. [Assignment Rules](#). Rules used to place users in the correct VLAN are tied to the user profile.
5. [Deploy Policy](#). The configuration is pushed to the access point.

Network Policy

A new network policy is defined by selecting CONFIGURE from the top menu and NETWORK POLICIES just below it.

1. If a network policy has previously been defined, as would be the case if you followed the instructions for the [SMS Authentication with Captive Web Portal](#) example, then you will see the CONFIGURE page to that shown below.



2. If a network policy is displayed, then:
 - a. Click within the network policy name box (Corp-Policy (c) in the figure above).
 - b. Select .
3. If no existing network policy is displayed, then:
 - a. Select .
 - b. Fill in the Policy Details: check the Wireless box only and enter **Corp-Policy** as the Policy Name.
 - c. Click SAVE to move to the Wireless Networks tab.
 - d. In the Wireless Networks tab, select and then .
 - e. Enter **A3-Corp-NV** (c) in the Name (SSID) field. The Broadcast Name is automatically filled in as A3-Corp-NV as well.

Authentication

1. Since the SSID will be used for employee access, select **Enterprise** below SSID Authentication.

Network Policies > Corp-Pol... > All SSIDs > New SSID

POLICY DETAILS WIRELESS NETWORKS DEVICE TEMPLATES ROUTER SETTINGS ADDITIONAL SETTINGS DEPLOY POLICY

CONFIGURATION GUIDE

Wireless Network

Policy Name
New Policy

SSID (Name)
A3-Corp-NV

RADIUS Server Group
+ Add Radius Server Group

Name (SSID) *
A3-Corp-NV (c)

Broadcast Name *
A3-Corp-NV

Broadcast SSID Using

WIFIO Radio (2.4 GHz or 5 GHz)

WIF1I Radio (5 GHz only)

SSID Usage

SSID AUTHENTICATION MAC AUTHENTICATION


Enterprise WPA / WPA2 / WPA3

Personal WPA / WPA2 / WPA3


Private Pre-Shared Key

WEP

Open Unsecured

2. A RADIUS Server group is a set of RADIUS servers that can be queried by access points. If you have previously defined a RADIUS server group in a previous example, you can reuse it.
 - a. Click the  icon beside Default RADIUS Server Group.
 - b. Place a check mark beside the previously defined server group name.
 - c. Click **SELECT**.

RADIUS Server Groups



Name

A3-RADIUS-SERVER-GROUP

CANCEL **SELECT** COPY

3. If a server group has not been defined yet.
 - a. In this example, we will only be adding one RADIUS server, our A3 instance. Click the **+** sign beside **Default RADIUS Server Group**.
 - b. In the Configure RADIUS Servers dialog, select **AEROHIVE A3 (0)** and click the **+** sign to add a new group. Note: If you are using the on-premises version of ExtremeCloud IQ, then:
 - i. The on-premises version of ExtremeCloud IQ does not offer an EXTREME A3 category, select EXTERNAL RADIUS SERVER (0) instead.

- ii. Select the gear icon (⚙️). In the dialog presented ensure that CoA (RFC3576) is enabled.

Configure RADIUS Servers

RADIUS Server Group Name * RADIUS Server Group Description ⚙️

EXTERNAL RADIUS SERVER (0) EXTREME NETWORKS A3 (0) EXTREME NETWORKS RADIUS SERVER (0)

✎️ + 🗑️

Name	IP/Host Name
------	--------------

ⓘ Do not change the Server Type Authentication or Accounting ports from 1812 and 1813, respectively.

- c. Fill in the Extreme Networks A3 Server dialog:
 - i. **Name: A3-RADIUS.**
 - ii. **Description:** as desired.
 - iii. **IP/Host Name:** use the + sign to add the A3 VIP address **10.150.1.254 (A*)** as the Host Name and IP Address.
 - iv. **Shared Secret: 8AB7tHkP (a).** This is used to hash and unhash information exchanged with the A3 server. Remember this setting; it must be used during A3 configuration.
 - v. Click SAVE EXTREME A3.
 - vi. Enter **A3-RADIUS-SERVER-GROUP** in the RADIUS Server Group Name field, check the box next to A3-RADIUS and click SAVE RADIUS.

Aerohive A3 Server

Aerohive A3 Server

Name *

Description

IP/Host Name * (A*) + 🗑️

Server Type * Authentication Port: 1812
 Accounting Port: 1813

Shared Secret (a) Show Password

4. A3 ensures proper employee access by sending RADIUS attributes to the access point upon authentication. The access point uses these attributes to assign appropriate user profiles. The default profile is used when no RADIUS attribute rules have been satisfied, placing the user in the registration state. Continue down the screen to Authenticate via RADIUS Server, User Access Settings.
5. If you have completed the SMS example, then:
 - a. Click on the 🗑️ icon to the right of **Default User Profile**.
 - b. Select **Registration-NV** from the list.
 - c. If you have not completed the SMS example, please execute steps 7 through 10 in [SMS Authentication with Captive Web Portal](#).
 - d. Click **SELECT USER PROFILE**
6. Select the **Apply a different user profile to various clients and user groups** check box. This enables the use of multiple user profiles on a single SSID.

7. Select the **Allow user profile assignment using RADIUS attributes in addition to three tunnel RADIUS attributes** check box. This results in a selection of Standard RADIUS Attribute and a value of 11_Filter-Id. This means that the access point's profile assignment will key off of the value of the 11_Filter-Id RADIUS attribute received from A3.

User Access Settings

Configure your QoS, VLAN, Firewall policies, and Traffic Tunneling

Default User Profile Registration-NV
VLAN : 1 + ≡

Apply a different user profile to various clients and user groups.

Allow user profiles assignment using RADIUS attributes in addition to three tunnel RADIUS attributes.

Standard RADIUS Attribute 11_Filter-Id ▾

Vendor specific RADIUS Attribute

User Profiles

1. Select **+** above User Profile Name to obtain create a Sales User Profiles with VLAN 2 (H); the VLAN setting will server to provide Sales members with appropriate access rather than firewall settings. Enter **Sales** into the User Profile Name. The VLAN to Connect to is either selected from a list of those already defined with the **≡**, or if the VLAN number is not found in the list, use the **+** icon to view the New VLAN Object dialog to create VLAN 2 (H). Select SAVE.

User Profile

User Profile Name * Sales ≡

Connect to * VLAN VLAN Group

2 (H) ≡ + ≡



New VLAN Object

Name * 2

VLAN ID * 2 (H)

2. Select **+** again to obtain a **Marketing** User Profiles with VLAN 5 (l) using the same procedure as in the previous step.
3. Select **+** again to obtain a **Employee** User Profiles with VLAN 8 (k) using the same procedure as in the previous step.

Assignment Rules

1. After the profiles have been created, it is necessary to tell the access point to assign these profiles when A3 sends back the proper RADIUS attribute. Select the  on the **Sales** line in the Assignment Rules column.
2. Enter the name **A3-Sales-Rule-NV** in the Name field, click the  symbol, and select RADIUS Attribute.

User Profile Assignment

Name
A3-Sales-Rule-NV

Description
Send sales to VLAN 2

Assign user profiles to clients or users connecting to an SSID according to authentication assignment.


RADIUS Attribute	VALUE
Client OS Type	No rules found
Client MAC Address	
Client Location	
Schedule	


3. Note that 11_Filter-Id has been preselected. Fill in the Attribute Values field with *sales* (i). It is important that the value be entered in this way, since the field is case sensitive and it must match an entry we will make in A3. Click OK and then SAVE.

A single standard RADIUS Attribute Value Pair

RADIUS Attribute 11_Filter-Id

Attribute Values

4. Repeat the procedure for the **Marketing** profile, using the name **A3-Marketing-Rule-NV** and attribute value of **marketing** (j).
5. Repeat the procedure for the **Employee** profile, using the name **A3-Employee-Rule-NV** and attribute value of **employee** (k).
6. Under Assignment Description click the  button to expand both descriptions. The display should appear as below. Click SAVE.

+   The IQ Engine with version prior to 8.1r1 only support 16 user profile policy rules.

USER PROFILE NAME	VLAN/VLAN GROUP	ASSIGNMENT RULES	ASSIGNMENT DESCRIPTION	ORDER				
<input checked="" type="checkbox"/> Sales	2	  A3-Sales-Rule-NV	▼ Send sales to VLAN 2 <table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>RADIUS Attribute</td> <td>sales</td> </tr> </tbody> </table>	Type	Value	RADIUS Attribute	sales	↑ ↓
Type	Value							
RADIUS Attribute	sales							
<input type="checkbox"/> Marketing	5	  A3-Marketing-Rule-NV	▼ Send marketing to VLAN 5 <table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>RADIUS Attribute</td> <td>marketing</td> </tr> </tbody> </table>	Type	Value	RADIUS Attribute	marketing	↑ ↓
Type	Value							
RADIUS Attribute	marketing							
<input checked="" type="checkbox"/> Employee	8	  A3-Employee-Rule-NV	▼ Send all other employees to VLAN 8 <table border="1"> <thead> <tr> <th>Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>RADIUS Attribute</td> <td>employee</td> </tr> </tbody> </table>	Type	Value	RADIUS Attribute	employee	↑ ↓
Type	Value							
RADIUS Attribute	employee							

Deploy Policy

Select the **Deploy Policy** tab, then check the box for your access point, and then

UPLOAD

UPLOAD. Check **Update Network Policy and Configuration**. Click

PERFORM UPDATE.

Before continuing, note the IP Address of your access point, this corresponds to the (E) address in table.

This completes the ExtremeCloud IQ configuration.

A3 Configuration

Authentication setup then requires definition or modification of several A3 settings:

1. [Active Directory Domain Join](#) - adds the A3 server to the Active Directory used for authentication.
2. [Roles](#) - classifies the type of user, in this case three roles for employees, sales group members, and marketing group members will be used.
3. [Authentication Sources](#) - defines how user information is to be gathered and ties users to roles. The internal AD authentication source will be used.
4. [Devices](#) - defines the network devices that authenticate clients against A3, in this case the Extreme Networks access point.
5. [Connection Profile](#) - ties together the authentication source with a connection source, in this case an access point's A3-Corp SSID.

When configuration is completed, a directory-based authentication will be tested and audit logs will be examined.

Start by entering the A3 configuration interface, either continuing from the initial installation or invoking the interface via [https://<\(A\) address>:1443](https://<(A) address>:1443).

Active Directory Domain Join

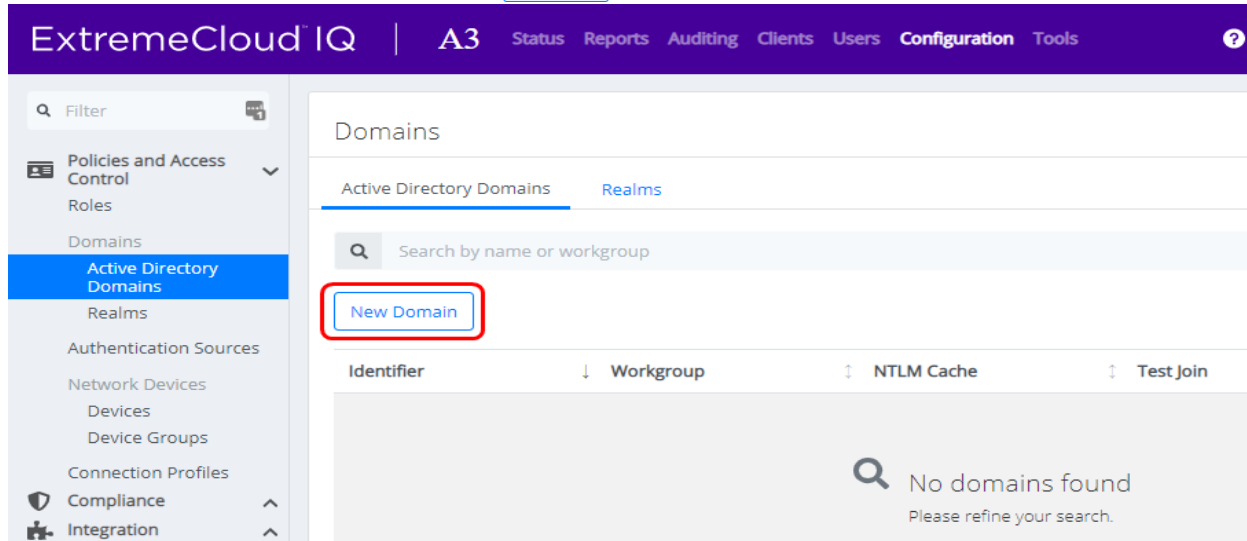
Requirements

The following pieces of information will be needed:

- Domain name of the AD Domain. E.g. **example.com**.
- NETBIOS name of the AD Domain. E.g **example**.
- Domain Controller IP Address. This is the **10.150.1.5** (D) address.
- Domain DNS Server IP Address. This is the **10.150.1.5** (D) address.
- Administrator account (name and password) with the necessary privilege to join a computer to the AD. This will only be used once during this configuration step.
- The OU of the AD node where the A3 computer is to be added, usually **COMPUTERS**.
- The Base DN is the base location in the directory where search queries will be performed. E.g. **CN=Users,DC=example,DC=com**.
- The Bind DN is the distinguished name for the user account that A3 will use to conduct user lookups. This does not need to be the Administrator's account. E.g. **CN=jstaff,CN=Users,DC=example,DC=com**.

Follow these steps to add the A3 server to your Active Directory domain:

1. Select Configuration > Policies and Access Control > Active Directory Domains.
2. Select [New Domain](#).



3. Enter the information as shown below, based on the information gathered earlier:

The screenshot shows the 'New Domain' configuration form. The 'Settings' tab is selected. The fields are as follows:

Identifier	CorpAD (e)	Specify a unique identifier for your configuration. This does not have to be related to your domain.
Workgroup	example	
DNS Name of the Domain	example.com	The DNS name (FQDN) of the domain.
Sticky Domain Controller	*	This is used to specify a sticky domain controller to connect to.
Active Directory Server	10.150.1.5 (D)	The IP address or DNS name of your Active Directory server.
DNS Server(s)	10.150.1.5 (D)	The IP address(es) of the DNS server(s) for this domain.
Organizational Unit	Computers	Create the computer account in advance in this OU. The characters. (e.g., "Computers/Servers/Unix")

4. Click [Create and Join](#).
5. Enter the administrator account and password that has privileges to join the domain.

Join CorpAD Domain

Please enter administrative credentials to connect to the domain.

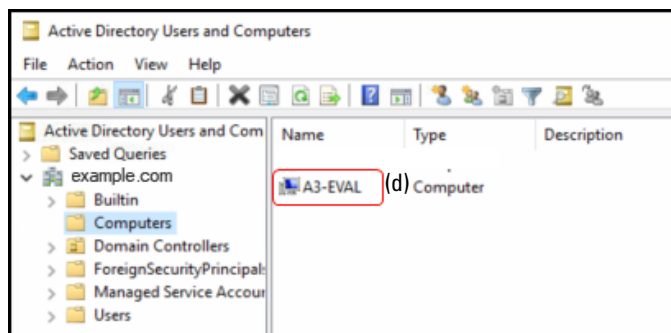
User Name: admin

Password:

Buttons: Cancel, Join CorpAD

6. If the Join fails, you can try again using the same credentials using the Try Again button, or try again by using the Cancel button and then the Join button on the Domains page.
7. You may receive an error indicating that a DNS record for the AD server could not be defined. If this is the case, please add an A-record for your A3 server (A3-Eval) to your DNS server.

The success of the operation can be checked by using the Active Directory Users and Computers snap-in on the Windows server hosting the AD. Check the location in your AD tree where the OU for computer accounts is located (Computers in the example above) to ensure that your computer has been added.



Next REALMS must be modified to use the Active Directory that you just defined.

1. Select Configuration > Policies and Access Control > Realms.
2. Three realms are pre-defined:
 - **DEFAULT** - defines the realm used when no others realm applies.
 - **LOCAL** - a realm for use with local lookups, instead of forwarding to another server.
 - **NULL** - the realm to use when no domain information is provided by user. For example, user instead of user@domain.
3. Select **DEFAULT**. In the Realm DEFAULT titled dialog, under NTLM Auth Configuration, select **CorpAD** from the Domain drop-down. Click **Save**.
4. Repeat the previous step for **NULL**.

Roles

Roles are accessed through the following steps:

1. Select Configuration > Policies and Access Control > Roles.
2. Select [New Role](#).
3. Create a Sales role by entering **Sales** into the Name field. Click [Create](#).

New Role

Name

Description

Maximum Clients Per User
The maximum number of clients a user having this role can register. A number of means unlimited number of clients.

[Create](#) [Reset](#)

4. Repeat the last step for the **Marketing** role.
5. Do the same for the **Employee** role.

Authentication Sources

The next steps involve creation of the **CorpAD** authentication source.

1. Select Authentication Source from the list on the left.
2. Inside the Internal Sources box, click New Internal Source, and choose Active Directory.

Authentication Sources

Define the authentication sources for access to the captive portal or the admin web interface.

Each connection profile must be associated with one or multiple authentication sources while 802.1X connections use the ordered internal sources to determine which role to use. External sources are never used with 802.1X connections.

Internal Sources

[New Internal Source](#)

- Active Directory**
- Authorization
- EAP-TLS
- Htpasswd
- HTTP
- Kerberos
- LDAP
- Password of the Day
- RADIUS

Description	Type
0 internal sources defined	

Click the button to define a new source.

3. Fill in the form as shown below, with:
 - a. **Name: CorpAD.**
 - b. **Description:** as desired.
 - c. **Host: 10.150.1.5 (D)** - the Active Directory server.
 - d. **Base DN: CN=Users,DC=EXAMPLE,DC=COM.** This is the base AD tree location to start a user search from.
 - e. **Scope: Subtree.** This allows the search to progress to the entire tree beneath the Base DN.
 - f. **User Name Attribute: sAMAccountName.** This is the normal AD entry for the user's name.
 - g. **Email Attribute: mail.** This is the normal AD entry for the user's email. This is used for sponsored access.
 - h. **Bind DN: CN=jstaff,CN=Users,DC=example,DC=com.** The Bind DN is the distinguished name for the user account that A3 will use to conduct user lookups. This does not need to be the Administrator's account.
 - i. **Password:** the Bind DN user's password. At this point you should use the TEST button beside the password. This will check for a working connection to the AD server.
 - j. **Associated Realms:** include **default** and **null**.

New Authentication Source AD ✕

Name

Description

Host : 389 None ▼ (D)

Connection Timeout
LDAP connection timeout.

Request Timeout
LDAP request timeout.

Response Timeout
LDAP response timeout.

Base DN

Scope

Username Attribute
Main reference attribute that contains the username.

Username Attribute
Other attributes that can be used as the username (requires restarting the radiusd service to be effective).

Email Attribute
LDAP attribute name that stores the email address against which the filter will match.

Bind DN
If empty, an anonymous bind will be performed.

Password 👁

Cache Match
Cache results of a rule match.

Monitor
Monitor this source.

Shuffle
Randomly choose LDAP server to query.

Associated Realms

4. Click Authentication Rules at the bottom of the page.
5. Add a **Sales** rule that matches Sales group membership in Active Directory. Enter:
 - a. Name as **Sales**.
 - b. Description as desired.
 - c. Click on .
 - d. Select Conditions to match the user's AD membership:
 - i. Drop down the first field to **memberOf**.
 - ii. Drop down the second field to **equals**.

- iii. Enter **CN=Sales,CN=Users,DC=EXAMPLE,DC=COM**. LDAP distinguished names must be used as the search string.
 - d. In the field beside Role, under Actions, select **Sales**.
 - e. Click the plus sign next to **Sales**. In the new action,
 - i. Change Role to **Access Duration**.
 - ii. Change the period to **2 days**.
6. Click the plus sign to the right of **Sales** adjacent to **Authentication Rules**. Repeat step 3 for the **Marketing** role, changing **Sales** to **Marketing** in all cases and Access Duration to **12 hours**.
7. Click the plus sign again to create a **catchall** rule that will place all users not in either the Sales or Marketing role into the Employee role:
 - a. Name as **catchall**.
 - b. Role beneath Actions as **Employee**.
 - c. Set Access Duration to **3 days**.

The screenshot displays the 'Authentication Rules' configuration page. It shows three rules, each with its own configuration panel. Red boxes highlight specific fields in each rule's configuration.

- Rule 1: Sales (Sales department members)**
 - Name: Sales
 - Description: Sales department members
 - Matches: All
 - Conditions: 1. memberOf, equals, CN=Sales,CN=Users,DC=
 - Actions: 1. Role, Sales; 2. Access duration, 2 days
- Rule 2: Marketing (Marketing department members)**
 - Name: Marketing
 - Description: Marketing department members
 - Matches: All
 - Conditions: 1. memberOf, equals, CN=Marketing,CN=Users
 - Actions: 1. Role, Marketing; 2. Access duration, 12 hours
- Rule 3: catchall**
 - Name: catchall
 - Description: (empty)
 - Matches: All
 - Conditions: Add Condition
 - Actions: 1. Role, Employee; 2. Access duration, 3 days

8. Click [Create](#) to save the authentication source.

Devices

Device configuration is next:

1. Click Devices beneath Network Devices. The list of defined entries is displayed.
2. If the list includes the highlighted device, i.e. the address of your access point 10.150.1.19 (E), then select that entry and skip to step 5.

Identifier	Description	Group	Type	Mode	
10.150.1.19	QSG AP (E)	Aerohive_AP	Aerohive::AP	production	Delete Clone
192.168.0.1	Test Access Point	Aerohive_AP	Aerohive::AP	production	Delete Clone
192.168.1.0/24	Test Range of Access Points	Aerohive_AP	Aerohive::AP	production	Delete Clone

3. A device for our access point must be defined. Select [New Device](#) and then select **Aerohive_AP**.
4. In the New Device form, enter the IP address of your access point **10.150.1.19 (E)** in the IP Address/MAC Address/Range (CIDR) field, enter a Description, and ensure that the Use CoA box is checked.

Device 10.150.1.19 ✕

Definition [Roles](#) [RADIUS](#) [SNMP](#) [CLI](#) [Web Services](#)

IP Address/MAC Address/Range (CIDR) 🔒

Description

Type

Mode

Device Group

Deauthentication Method

Use CoA

Use CoA when available to deauthenticate the user. When disabled, RADIUS Disconnect will be used instead, if it is available.

5. Select the Roles tab, ensure that only Role by Device Role is enabled.
 - a. Next to isolation, enter **isolation (g)**.
 - b. Next to **Sales**, enter **sales (i)**. Note that the entry is all lower case. This matches what the access point is expecting from A3.
 - c. Next to **Marketing**, enter **marketing (j)**.

Role by Device Role

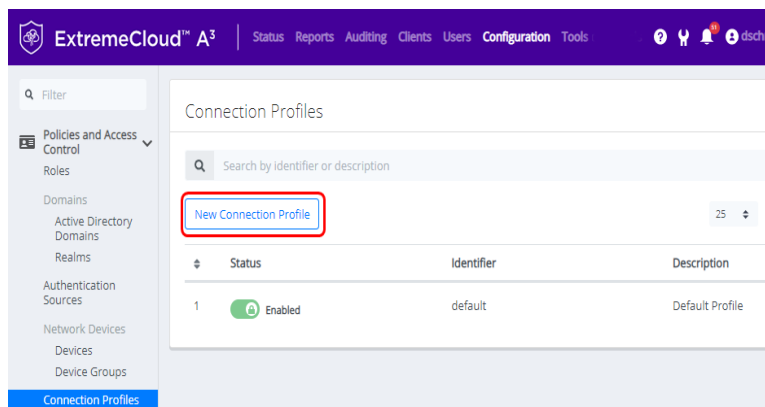
registration	registration
isolation	isolation (g)
macDetection	
inline	inline
default	
guest	guest
gaming	
voice	voice
REJECT	
Sales	sales (i)
Marketing	marketing (j)

6. Select the RADIUS tab. Enter **8AB7tHkP** (a) into the Secret Passphrase field. This matches the setting entered in the ExtremeCloud IQ in [Authentication](#). Click Create.

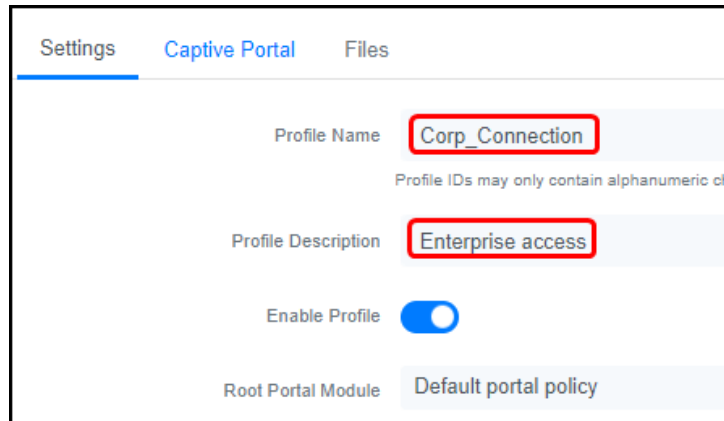
Connection Profile

The connection profile ties together the access point's SSID with authentication sources. To define a new profile:

1. Select Configuration from the top level menu, Connection Profiles from the left menu, and click the New Connection Profile button.

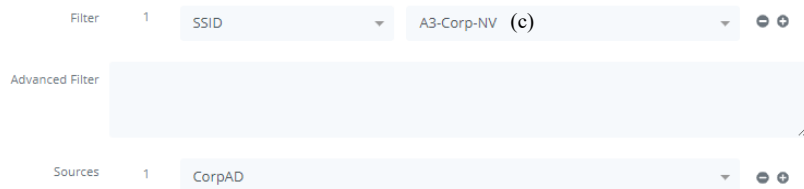


2. Fill in a Profile Name and Profile Description as shown below.



The screenshot shows the 'Captive Portal' settings page. The 'Profile Name' field is highlighted with a red box and contains the text 'Corp_Connection'. Below it, a note states 'Profile IDs may only contain alphanumeric characters'. The 'Profile Description' field is also highlighted with a red box and contains the text 'Enterprise access'. The 'Enable Profile' toggle is turned on. The 'Root Portal Module' is set to 'Default portal policy'.

3. Check Automatically Register Clients. This ensures the device is registered to A3 and allowed to connect to the 802.1X-secured SSID.
4. Uncheck 802.1X Recompute Role from Portal.
5. Under Filters, click Add a filter and enter **A3-Corp-NV (c)** next to SSID. This tells A3 to use this connection profile when anyone connects to the access point using the **A3-Corp-NV (c)** SSID.
6. Under Sources, select Add a source and then select **CorpAD** as the authentication source. This tells A3 to authenticate users against the **CorpAD** Authentication Source.



The screenshot shows the configuration for filters and sources. Under 'Filter', there is one filter with the type 'SSID' and the value 'A3-Corp-NV (c)'. Below this is an 'Advanced Filter' field which is currently empty. Under 'Sources', there is one source with the value 'CorpAD'.

7. Click [Create](#).

Testing the Active Directory Example

To test the A3 and ExtremeCloud IQ configurations for Active Directory authentication, use a laptop, smart phone, or tablet to connect to the **A3-Corp-NV** (c) SSID.

Active Directory Contents

The testing in this guide section depends on a particular configuration of your Active Directory server. In particular, the following users and groups are required:

User	Login Name	Group Membership
A3User	A3User	
Jane Staff	jstaff	Employees
Joe Sales	jsales	Employees, Sales
Mike Marketing	mmarketing	Employees, Marketing

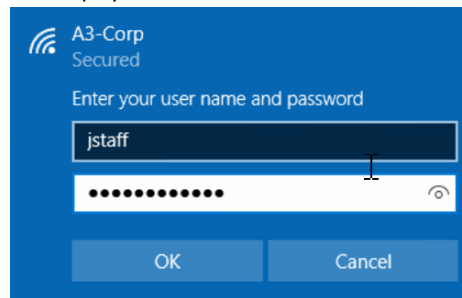
Testing

The following screen shots were taken using a Windows 10 client. Similar steps will be required for other clients.

1. If you intend to test with a client that has previously authenticated, then you need to ask A3 to forget the device registration. Select Clients from the top menu bar, find your Computer Name, and click its MAC Address. Erase Owner, change Status to Unregistered, and set the Role to No role. Click SAVE.

You also need to direct your client to forget the current login credentials. For a Windows 10 client:

- a. Disconnect from the WiFi network.
 - b. Find your Network & Internet settings. Select WiFi, then Manage known networks, select **A3-Corp-NV** (c), and then Forget.
2. Connect to the **A3-Corp-NV** (c) SSID and enter credentials for **jstaff**, who is an employee but not a member of either the **Sales** or **Marketing** AD security groups:

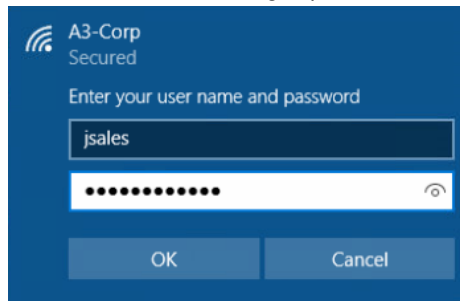


3. After the successful connection, look at the properties for the WiFi connection:

Properties

SSID:	A3-Corp
Protocol:	802.11n
Security type:	WPA2-Enterprise
Type of sign-in info:	Microsoft: Protected EAP (PEAP)
Network band:	2.4 GHz
Network channel:	6
IPv4 address:	10.150.8.10
IPv4 DNS servers:	10.150.8.1

4. Connect to the **A3-Corp-NV (c)** SSID and enter credentials for **jsales**, who is a member of either the **Sales AD** group:



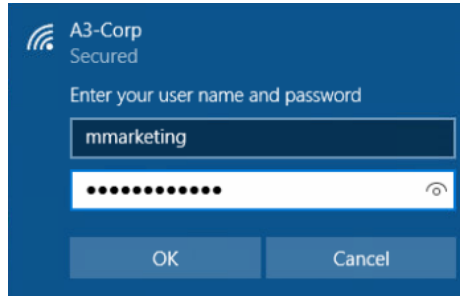
5. After the successful connection, look at the properties for the WiFi connection:

Properties

SSID:	A3-Corp
Protocol:	802.11n
Security type:	WPA2-Enterprise
Type of sign-in info:	Microsoft: Protected EAP (PEAP)
Network band:	2.4 GHz
Network channel:	6
IPv4 address:	10.150.2.10
IPv4 DNS servers:	10.150.2.1

Note that the address assigned is from the Sales User Profile configured in ExtremeCloud IQ.

6. Repeat step 4 if you intent to reuse the same client for further testing.
7. Connect to the **A3-Corp-NV (c)** SSID and enter credentials for **mmarketing**, who is a member of the **Marketing AD** group:



8. After the successful connection, look at the properties for the WiFi connection:

Properties

SSID:	A3-Corp
Protocol:	802.11n
Security type:	WPA2-Enterprise
Type of sign-in info:	Microsoft: Protected EAP (PEAP)
Network band:	2.4 GHz
Network channel:	6
IPv4 address:	10.150.5.11
IPv4 DNS servers:	10.150.5.1

Note that the address assigned is from the Marketing User Profile configured in ExtremeCloud IQ.

Verifying Operation

In addition to successful authentication and network access, you can use A3's auditing function to check on the status of the authentication. Select AUDITING from the top menu bar and then RESET SEARCH from the page. Items are displayed in reverse order. You should see an Accept Auth Status for your client.

Created At	ID	Auth Status	MAC Address	IP Address	Is a Phone	Client Status	User Name	Unique ID	NAS IP Address
2019-12-06 02:04:08	7	Accept	00:08:ca:e1:da:21		0	reg	mmarketing		10.150.1.19
2019-12-06 02:03:35	6	Accept	00:08:ca:e1:da:21		0	reg	jsales		10.150.1.19
2019-12-06 02:01:50	5	Accept	00:08:ca:e1:da:21		0	reg	jstaff		10.150.1.19

If you click the Accept button for any entry and select the RADIUS tab, you can see the RADIUS messages exchanged between A3 to the access point.

RADIUS Audit Log Entry 13

Node Information Device Information **RADIUS**

request_time 0

RADIUS Request

- User-Name = "mmarketing"
- NAS-IP-Address = 10.150.1.19
- NAS-Port = 0
- Service-Type = Framed-User
- Framed-MTU = 1500
- State = 0xe94e5fc7e8cb45af692015b5be178365
- Called-Station-Id = "88:5b:dd:00:85:14:A3-Corp"
- Calling-Station-Id = "00:08:ca:e1:da:21"
- NAS-Identifier = "AH-008500"
- NAS-Port-Type = Wireless-802.11
- Acct-Session-Id = "C1A24EA8E5F6BE7B"
- Acct-Multi-Session-Id = "908E843857937ADD"
- Event-Timestamp = "Apr 23 2019 00:24:50 UTC"
- Connect-Info = "11ng"
- EAP-Message = 0x028500061a03
- WLAN-Pairwise-Cipher = 1027076

- WLAN-AKM-Suite = 1027073
- FreeRADIUS-Proxied-To = 127.0.0.1
- EAP-Type = MSCHAPv2
- Stripped-User-Name = "mmarketing"
- Realm = "null"
- Called-Station-SSID = "A3-Corp"
- PacketFence-Domain = "CorpAD"
- Attr-26.26928.6 = 0x00000004
- Attr-26.26928.1 = 0x00000000
- User-Password = "*****"
- SQL-User-Name = "mmarketing"

RADIUS Reply

- EAP-Message = 0x03850004
- Message-Authenticator = 0x00000000000000000000000000000000
- User-Name = "mmarketing"
- Filter-Id = "marketing"

Active Directory Example Complete

This completes the Active Directory Authentication example for A3.