

# A3 Installation and Usage Guide

## No Registration VLAN Version

*This document is the Installation and Configuration Guide for the A3 system. It includes installation and usage instructions for A3 version 4.1.0 or later.*

*There are two versions of this manual, one using a registration VLAN and one with no registration VLAN. This is the version for no registration VLAN. Further detailed usage instruction is included in the online help that accompanies the A3 administrative GUI.*

# Table of Contents

<b>Introduction</b> .....	<b>1</b>
Overview .....	1
Major Features of A3 .....	1
<b>Deployment Modes</b> .....	<b>3</b>
Overview .....	3
Layer 2 Hybrid Out-of-Band Deployment .....	3
Layer 3 Across a Routed Network .....	4
Layer 3 Hybrid Out-of-Band Deployment .....	5
Inline Deployment .....	6
<b>Enforcement Modes</b> .....	<b>7</b>
Firewall Enforcement .....	7
WebAuth Enforcement .....	7
RADIUS Enforcement .....	8
WebAuth (ACL) Enforcement .....	9
<b>Installation</b> .....	<b>10</b>
Equipment Requirements .....	10
VMware VSphere Hypervisor .....	10
Microsoft Windows Server 2019 .....	10
Extreme Networks Requirements .....	10
Download the Software .....	11
A3 Installation on VMware ESXi .....	11
Network Interfaces .....	11
Instantiation .....	11
A3 Installation on Windows Server 2019 Hyper-V .....	13
Network Interfaces .....	13
<b>Network Topology</b> .....	<b>17</b>
Connectivity and Security .....	17
Enforcement Devices .....	18
Infrastructure Devices .....	19
Layer 3 Topology .....	19
<b>Clustering</b> .....	<b>21</b>
Cluster Installation .....	21
Cluster Operation .....	22

---

Restarting Services .....	22
Graceful Shutdown and Restart .....	22
Cluster Backup and Recovery .....	22
<b>Table of Addresses and VLANs .....</b>	<b>23</b>
Network Implementation .....	24
.....	26
<b>Initial A3 Configuration .....</b>	<b>27</b>
Setup IP Addresses .....	27
Domain and Time Zone .....	28
Alerting .....	29
Change Admin Password .....	29
A3 Server Certificate .....	30
<b>ExtremeCloud IQ Setup .....</b>	<b>31</b>
MAC Authentication .....	31
Network Policy .....	31
Authentication .....	32
.....	33
Guest User Profile .....	33
Isolation User Profile .....	33
Deploy Policy .....	34
802.1X Authentication .....	35
Network Policy .....	35
Authentication .....	35
User Profiles .....	36
<b>Authentication Methods .....</b>	<b>38</b>
External Authentication Sources .....	38
Clickatell API Registration .....	39
Facebook API Registration .....	39
Github API Registration .....	39
Google API Registration .....	40
Instagram API Registration .....	40
Kickbox API Registration .....	40
LinkedIn API Registration .....	40
OpenID API Registration .....	41
Pinterest API Registration .....	41
Twilio API Registration .....	41
Twitter API Registration .....	41
WindowsLive API Registration .....	41
Internal Authentication Sources .....	42
Azure AD Registration .....	42
Google Workspace LDAP Registration .....	44
Exclusive Authentication Sources .....	46

Billing Authentication Sources	46
AuthorizeNet	46
Mirapay	46
PayPal	47
Stripe	47
802.1X	48
Suplicants	48
Authenticator	48
Authentication Servers	49
EAP and X.509 Certificates	49
EAP Methods	50
Social Login Authentication Technology	51
<b>A3 Configuration Flow</b>	<b>53</b>
Overview	53
Guest Access Configuration Example	54
ExtremeCloud IQ Configuration	54
A3 Configuration	54
802.1X Configuration Example	54
ExtremeCloud IQ Configuration	55
A3 Configuration	55
<b>Certificates and PKI</b>	<b>57</b>
Overview	57
Public and Private Keys	58
Public Key Infrastructure	58
A3 Certificate Usage	59
SSL Certificate	59
RADIUS Certificate	60
PKI Provider	64
Provisioner	64
<b>Portal Modules</b>	<b>66</b>
Connection Profile Settings	67
Type of Portal Modules	67
Source by Options	68
Templates	69
Example 1: Reorder Choices	70
Example 2: Two Factor Authentication	73
<b>Security Events and Scan Engines</b>	<b>75</b>
Fingerbank	75
Scan Engines	76
Nessus	76
OpenVAS	76
Rapid7	77

Rapid7 Installation	77
Rapid7 A3 User	77
A3 Configuration	78
Microsoft WMI (Windows Management Instrumentation)	79
Security Events	80
Event Triggers	80
Event Actions	80
Built-in and Sample Events	81
Scan Engine Related	81
Device Isolation	83
Miscellaneous	84
<b>Provisioning</b>	<b>85</b>
Mobile Device Managers	86
Cisco DPSK	86
Jamf	86
Microsoft Intune	86
MobileIron	87
OPSWAT	87
SentinelOne	88
SEPM (Symantec Endpoint Protection Manager)	88
<b>Firewall Integration</b>	<b>89</b>
Barracuda	89
A3 Configuration	89
Verification	90
Checkpoint	90
Setting up the Checkpoint Firewall	90
A3 Configuration	91
FortiGate	91
Setting up FortiGate Firewall	91
A3 Configuration	92
JSON-RPC	93
A3 Configuration	93
Palo Alto	94
Setting up the Palo Alto Networks Firewall	94
A3 Configuration	95
Verification	95
<b>Use Case 1: Guest Access with Captive Web Portal</b>	<b>96</b>
Roles	97
Authentication Sources	97
Null	97
Email	97
SMS	97

Devices	98
Connection Profile	98
Testing	99
SMS Test	100
Use Case 1 Complete	101
<b>Use Case 2: Active Directory Authentication</b>	<b>102</b>
Active Directory Domain Join	102
Active Directory Domain	103
Realms	103
Roles	104
Authentication Sources	104
Devices	105
Connection Profile	106
Testing Active Directory	106
Use Case 2 Example Complete	109
<b>Use Case 3: Local User Authentication</b>	<b>110</b>
User Manager	110
Local User Authentication	111
Create a Local User	111
Testing	Local User Authentication 112
Use Case 3 Example Complete	112
<b>Use Case 4: Sponsored Access</b>	<b>113</b>
Authentication Sources	113
Active Directory Source	113
Sponsor Source	114
Connection Profile	114
Testing Sponsored Access	114
Use Case 4 Example Complete	116
<b>Use Case 5: EAP-TLS Authentication</b>	<b>117</b>
EAP-TLS Authentication Source	117
Connection Profile	118
Corporate Profile	118
Guest Profile	118
Testing EAP-TLS	118
Use Case 5 Example Complete	120
<b>Use Case 6: Guest Access with External Captive Web Portal</b>	<b>121</b>
ExtremeCloud IQ Configuration	121
Network Policy	121
A3 Configuration	122
Devices	122
Connection Profile	123

---

Testing E-CWP Access .....	123
Null Authentication Test .....	124
Use Case 6 Complete .....	124
<b>Use Case 7: Headless IoT Devices .....</b>	<b>125</b>
Automatic Registration Security Event .....	126
Manual Use of Security Event .....	127
Use Case 7 Complete .....	127
<b>Use Case 8: Eduroam .....</b>	<b>128</b>
Overview .....	128
Local Users .....	129
Remote Users .....	129
Local Users at Remote Sites .....	129
ExtremeCloud IQ Configuration .....	129
A3 Configuration .....	129
Local Domain and Realm .....	130
Local Authentication Source .....	131
Eduroam Authentication Source .....	131
Local Connection Profile .....	132
Eduroam Connection Profile .....	132
Use Case 8 Complete .....	133
<b>Advanced Topics .....</b>	<b>134</b>
Best Deployment Practices .....	134
Memory and vSwap .....	134
vMotion .....	134
Fault Domains .....	134
RARP .....	134
Link Capacity .....	134
Paravirtualization .....	135
Snapshots .....	135
Administrative Access .....	135
Creating Dynamic Reports .....	135
Examples .....	137
Performance Enhancements .....	138
DHCP - IP Helpers .....	138
DHCP - Remote Sensor .....	139
Active Directory Integration .....	140
Locked Account .....	144
<b>A3 Troubleshooting .....</b>	<b>146</b>
Administration .....	146
Unable to Run A3 Administration .....	146
Browser Complains That A3 Is Unsafe .....	146
Internet Explorer Cannot Display the A3 Admin Page .....	146

---

Changes Don't Take Effect .....	146
The Auditing Tab .....	147
Getting Started .....	147
Clients Don't See Captive Web Portal .....	147
Authentication Issues .....	149
Clients No Longer See CWP .....	149
Clients Cannot Successfully Authenticate with the CWP .....	149
Clients Cannot Use Social Login Authentication .....	149
Some Clients Cannot Join with Active Directory Authentication .....	150
Post-Authentication Issues .....	150
Clients Assigned to Incorrect Role .....	150
Authenticated Clients Can't Access Internet or Local Sites .....	151
Cluster Problems .....	151
<b>Glossary .....</b>	<b>152</b>
<b>Index .....</b>	<b>160</b>



# Introduction

## Overview

---

A3 provides complete functionality for securing, managing and controlling all devices on your access network – from standard wired and wireless clients, to IoT and BYOD clients.

A3 is a mature software system for NAC (Network Access Control) used to control network access for client and IoT devices. It includes a captive portal for registration and remediation, centralized management for wireless and wired networks, and 802.1X support. A3 integrates with IDS (Intrusion Detection Systems), vulnerability scanners, and firewalls. It scales well and can be used for very large heterogeneous networks.

## Major Features of A3

---

### Web-based Management

A3's web-based management provides easy access to all of its features. No command line interface is required.

### Cloud-based Management

The A3 GUI is available in Extreme Networks's cloud management system. All A3 installations associated with a cloud account can be remotely managed.

### Clustering

Multiple A3 instances can be used as an integrated A3 cluster that provides load balancing, redundancy, and fail-over.

### Wired and Wireless Integration

Wired and wireless networks are handled uniformly by A3 using the same CWP (captive portal) and user database. APs (Access Points), wireless controllers, and switches from multiple vendors may be used in the same controlled network.

### Guest Access

Guest access is easily configured based on CWP-based authentication with a variety of techniques, including no authentication, email, SMS, and social media.

## **802.1X Support**

802.1X authentication is supported through the embedded FreeRADIUS software module.

## **Permanent Registration**

A3 automatically determines which client devices have been registered and optionally allows them continued network access without re-authentication. Such registrations can be automatically ended, for example at the end of a school term.

## **Security Events**

Abnormal network activity, including computer malware, prohibited, and exceeded limits traffic can be detected using remote sensors.

Proactive vulnerability scans can be performed on registration, scheduled, or on an ad-hoc basis. A3 correlates scan engine vulnerability IDs to the specific vulnerability, offering content-specific web pages for each found vulnerability.

A3's security event manager integrates events from multiple sources with customized alerting, reporting, isolation, and remediation actions.

## **Firewall Integration**

SSO (single sign-on) integration is supported for several model firewalls. Upon successful registration, A3 can dynamically update a firewall's IP to client association. The firewall can apply per-user or per-group filtering policies.

## **VoIP (Voice over IP) Support**

VoIP, or IPT (IP Telephony) is fully supported in heterogeneous environment for multiple switch vendors including Cisco, Avaya, and HP.

## **Virtual System Support**

A3 provides OVA and HYPERV virtual images supported by a wide variety of virtualization systems, including Microsoft HYPERV.

# Deployment Modes

## Overview

---

There are several modes of deploying A3 within a network. The deployment mode often dictates the type of A3 Enforcement Modes possible. Two classes of deployment are used with A3 depending on how unregistered clients are isolated prior to authentication:

- **Isolation through a registration VLAN.** Unregistered clients are associated with a unique VLAN that is not routed beyond the network that connects A3 to access devices. When working with a registration VLAN, two deployments are generally used:
  - [Layer 2 Hybrid Out-of-Band Deployment](#) - connects access devices to A3 within a single Layer 2 network.
  - [Layer 3 Across a Routed Network](#) - connects a remote Layer 2 set of access devices to an A3 via Layer 3 connections.
- **Isolation through firewall rules.** Unregistered clients are restricted from accessing the general network by firewall rules enforced in the access device. All authentication required devices are connected through Layer 3 networks. A single deployment mode is used:
  - [Layer 3 Hybrid Out-of-Band Deployment](#)

This version of the Installation and Usage manual discusses deployments that do not utilize a registration VLAN.

## Layer 2 Hybrid Out-of-Band Deployment

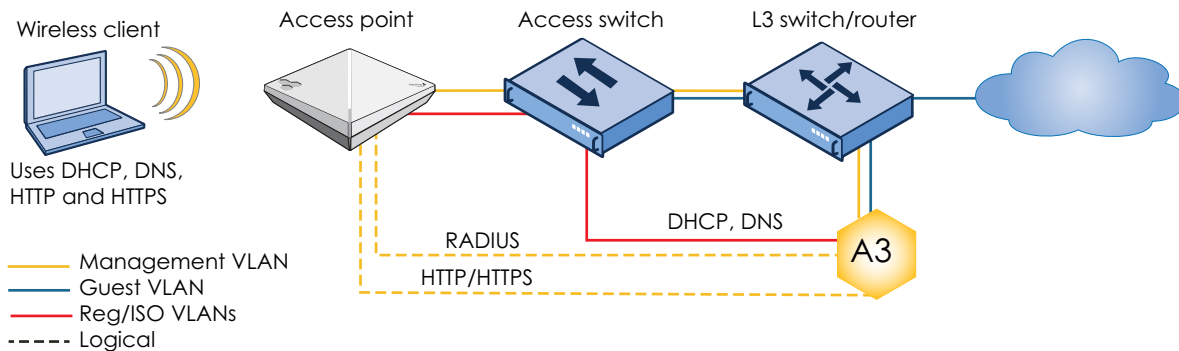
---

Layer 2 hybrid OOB (out-of-band) deployments requires that all of the elements in network access control be connected through layer 2 networks. This means that VLANs must be pushed from the core to the access networks, which can be an issue for larger network deployments. A [Layer 3 Across a Routed Network](#) deployment may be a better choice.

To ensure correct IP and VLAN assignments, A3 must receive all client DHCP and DNS requests. In layer 2 deployments, this is accomplished by connecting the A3 server to the access point via a switch. A3 receives DHCP requests and responds with an IP address on the local registration or isolation network. A3 also responds with its own IP address as the DNS server and the default gateway.

This deployment mode is shown in the figure below. An Extreme Networks AP is used in this figure, but an access switch or other intelligent network device can be used. This

deployment model may be used with VLAN, Web Auth, and RADIUS enforcement as described in [Enforcement Modes](#).

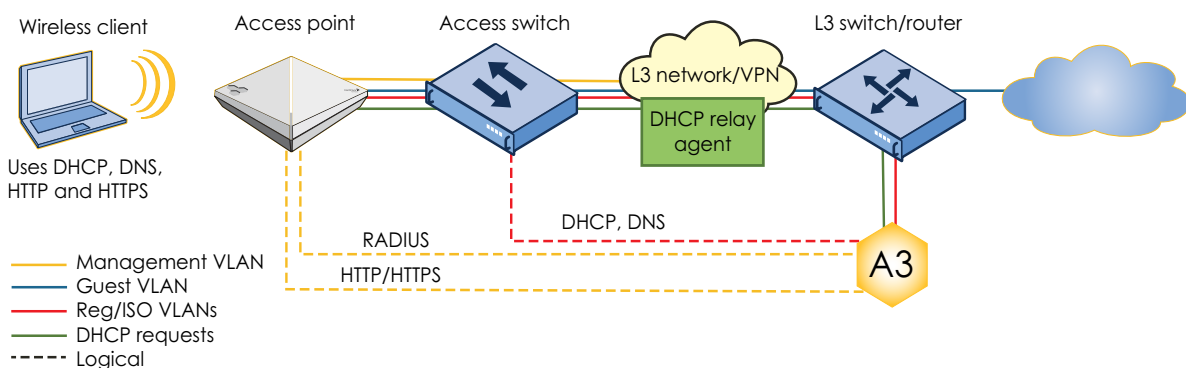


## Layer 3 Across a Routed Network

This deployment mode allows for complete, fine-grained network control and scales better than [Layer 2 Hybrid Out-of-Band Deployment](#) mode. This is the most common deployment model for A3.

A3 may be hosted in a data center in a layer 3 deployment. Clients and their access devices can be remotely located from A3 as long as the latency between clients and the A3 servers is under 5 ms. VPN access can be used between sites for added security.

This deployment mode is shown in the figure below. An Extreme Networks access point is used in this figure, but an access switch or other intelligent network device can be used. This deployment model may be used with VLAN, Web Auth, and RADIUS enforcement as described in [Enforcement Modes](#).



DHCP requests on the local registration or isolation network are forwarded to the A3 server on a remote network using a DHCP relay agent. Although DHCP relay agents may be enabled on an access point or access switch, best practice is to run it on a member of the larger layer 3 network. The relay agent receives layer 2 DHCP requests, encapsulates them in layer 3 packets and transmits them using the L3/VPN network to A3.

The steps needed to use A3 in a routed network are:

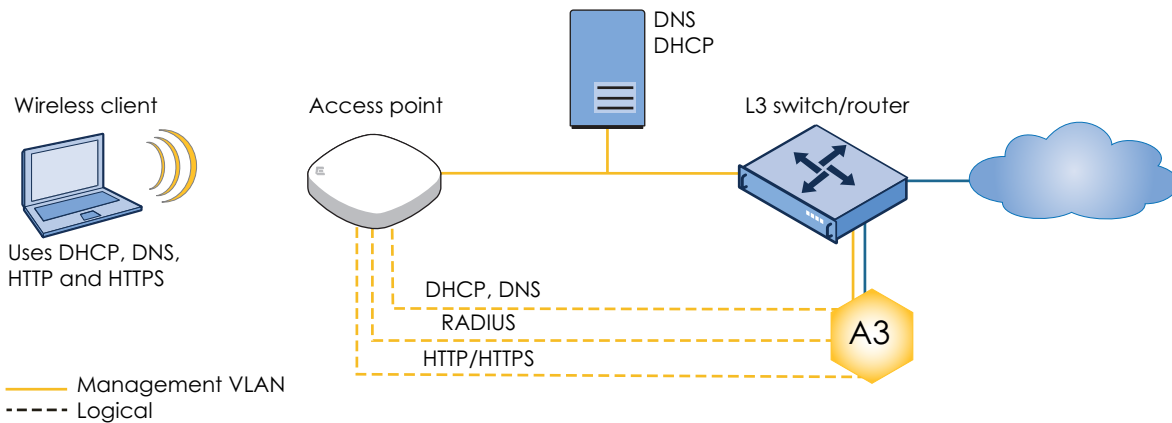
1. Define routed networks for interfaces in A3.
2. Setup up a DHCP relay on the L3 switch/router connected to A3.
3. Configure firewall rules on the access point or access switch to limit client access to A3 and required services.

An example of a Layer 3 configuration is available in the [Initial A3 Configuration](#) chapter.

## Layer 3 Hybrid Out-of-Band Deployment

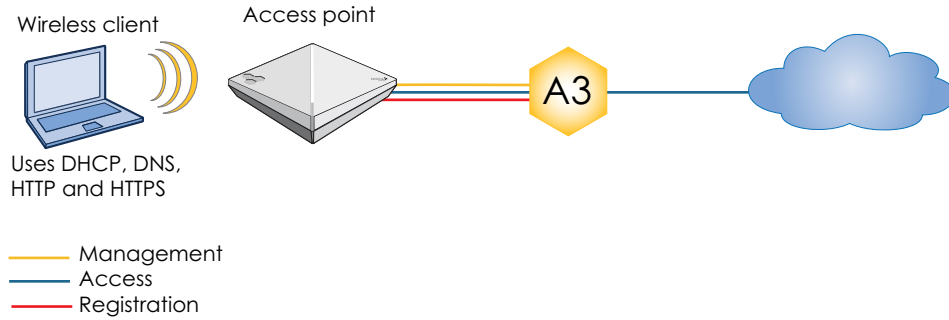
Layer 3 hybrid OOB (out-of-band) deployments are a new means of connecting authenticating clients. As opposed to earlier techniques a registration VLAN is not required and Layer 2 connectivity between clients and A3 is likewise not required. The A3 server and access point or switches need only have Layer 3 connectivity.

This deployment mode is shown in the figure below. An Extreme Networks AP is used in this figure, but an access switch or other intelligent network device can be used. This deployment model may be used with VLAN, Web Auth, and RADIUS enforcement as described in [Enforcement Modes](#).



# Inline Deployment

In an inline deployment A3 acts as the router that connects devices to the enterprise's internal networks and the internet. An inline deployment is shown below.



All devices connect through the A3 server. Unregistered devices connect to A3, which assigns an IP address. Web traffic is directed to the internal CWP while all other traffic is blocked. Clients are registered through the CWP as in other forms of enforcement, and are granted access through the internal IPtables and IPSet facilities.

This deployment mode does not scale very well, as all network traffic must go through the A3 server. Further, the A3 server becomes the single point of failure for the network as clustering is not supported. For these reasons, this deployment mode is not supported with A3.

# Enforcement Modes

A3 may be used with a number of enforcement mechanisms to implement network access control. The techniques describe here are:

- [Firewall Enforcement](#) - using access device firewall rules clients use A3's embedded web portal or other authentication mechanisms. Clients are assigned to distinct networks by the access device.
- [WebAuth Enforcement](#) - clients use a captive web portal hosted by A3, a switch or other device. Although clients can be assigned to distinct VLANs, this form of enforcement is generally used for a go/no-go access decision.
- [RADIUS Enforcement](#) - A3 acts as a RADIUS server for an access device. A3 responses are used to implement VLAN-based, ACL-based, or firewall-based access control.
- [WebAuth \(ACL\) Enforcement](#) - A3 is used as in VLAN enforcement, but A3 writes new ACL (access control list) elements to the access switch.

## Firewall Enforcement

---

In this Layer 3 mode, new clients attempting to first associate with a network are restricted by their access device via firewall rules. The firewall rules allow access to the A3 server and the local DHCP and DNS servers, but redirects any web (HTTP or HTTPS) traffic to A3's CWP.

The client steps through the registration process with A3, which provides the access device information used to assign a new set of firewall rules or VLAN to the client that implement appropriate network access.

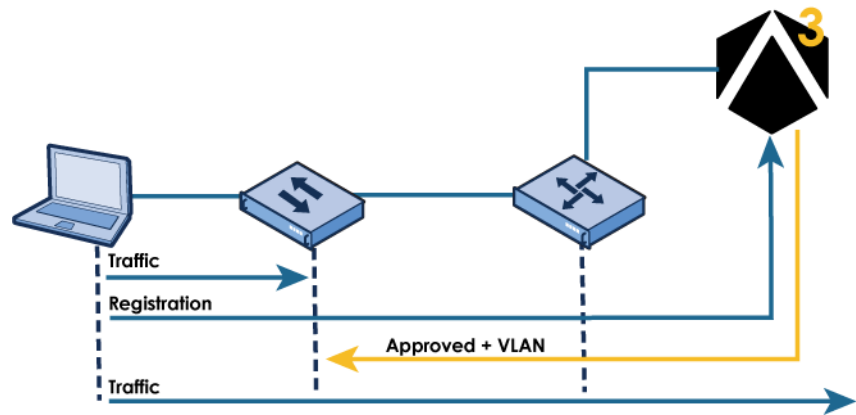
In this configuration, clients are restricted to communication with the A3 server until they have been registered and authenticated in A3, at which point they are allowed access to the general network. The A3 software, with its included RADIUS server, is used to authenticate clients. A3 serves as the 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 enforcement is used for all of the use cases in this guide.

## WebAuth Enforcement

---

WebAuth enforcement, also known as E-CWP (external captive web portal) is illustrated in the figure below.



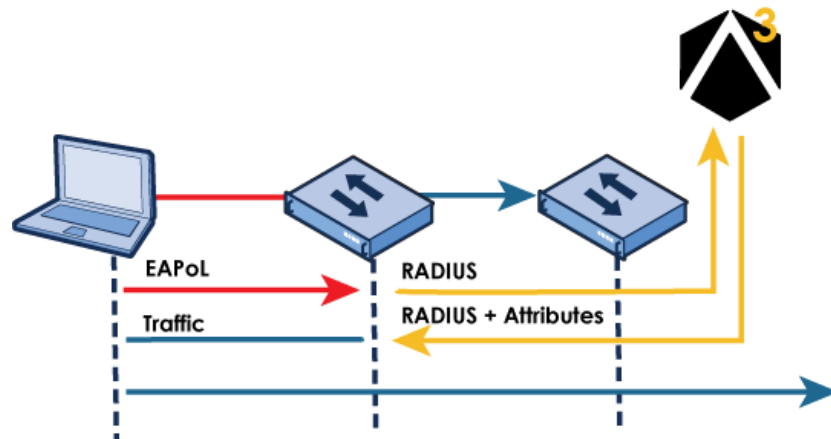
In this mode, the registration process uses A3 as an E-CWP. The client authenticates through the portal, where A3 indicates success or failure, and assigns a new VLAN. Several restrictions apply when used with Extreme Networks equipment:

1. The E-CWP is set up in an access policy in ExtremeCloud IQ. This process is described in the [Use Case 6: Guest Access with External Captive Web Portal](#).
2. Only a single ExtremeCloud IQ access policy is applied.
3. Some external A3 authentication sources may not work.
4. Role by VLAN ID must be used in Network Devices roles in A3.

An example of WebAuth enforcement usage is at [Use Case 6: Guest Access with External Captive Web Portal](#).

## RADIUS Enforcement

RADIUS enforcement is illustrated in the figure below.

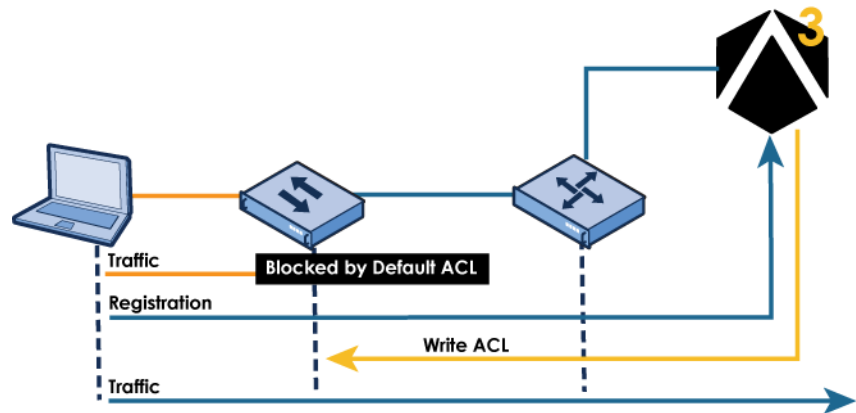


In this mode, A3 acts as a RADIUS server with and may optionally be used as a captive web portal. A3 returns roles or VLANs via RADIUS attributes, which the switch uses to allow or restrict access.



## WebAuth (ACL) Enforcement

WebAuth (ACL) enforcement is illustrated in the figure below.



In this mode, the switch ACLs (access control lists) restrict initial traffic through the switch and redirect the client to A3 for authentication using a captive web portal. If the authentication is successful A3, writes new ACLs to the switch that allow appropriate traffic based on the client's role.

# Installation

## Equipment Requirements

---

A computer system that meets the following requirements is needed to install and operate A3. The virtual machine resources listed below must be dedicated to A3 operation. Sharing resources with other applications may lead to system instability and bad user experience or even loss of service.

### VMware vSphere Hypervisor

VMware vSphere Hypervisor (ESXi) may be used with an x86-based host. ESXi requirements include a host:

1. Running ESXi version 6.0 or higher
2. 4 or more cores
3. 16GB or more RAM
4. 250GB or more storage

Administrative access to an ESXi host is also required. If the host is included in a vCenter domain, then access to that domain will be needed as well.

### Microsoft Windows Server 2019

An x86-based host running Microsoft Windows Server 2019 with a Hyper-V role may be used. The host requirements include:

1. Running Microsoft Windows Server 2019 with a Hyper-V role defined.
2. 4 or more cores
3. 16GB or more RAM
4. 250GB or more storage

## Extreme Networks Requirements

---


If Extreme Networks APs are used in the network then the following is also needed:

1. Extreme Networks APs must run version 10.41 software or higher.
2. ExtremeCloud IQ is a configuration platform for Extreme Networks access points. Self-registration for a ExtremeCloud IQ account is available at <https://extremecloudiq.com>.
3. An Extreme Networks Community login provides access to the latest A3 software.

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

## Download the Software

---

An OVA file with the A3 software and Linux operating system is available through the Extreme Networks Support Portal. Search for "A3". Versions of A3 will be highlighted by a  symbol.

## A3 Installation on VMware ESXi

---

Note the ESXi 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.

### Network Interfaces

There are two basic choices for the registration and isolation VLAN interfaces. These choices affect the virtual interfaces that are presented to the guest OS, and not the physical ports on the actual VMware host.

- **One virtual Ethernet interface.** In this instance, all VLANs are connected to A3 on one virtual interface inside the VM. This deployment is more common in smaller networks, or labs. A LAN port group is defined in vswitch0 as a trunk that allows trunking of the VLANs associated with management, registration, and isolation in A3.
- **Multiple virtual Ethernet interfaces.** This deployment option is more common in larger VMware environments where a management port group has already been established and new VLANs will avoid affecting other VMs that are also using that same port group. For example:
  - An A3ManagementNetwork port group can be defined in vswitch0, tagged with the management VLAN. Referring to [Table of Addresses and VLANs](#), this guide uses VLAN 1 (V1).

### Instantiation

The virtual machine may be instantiated by following these instructions:

1. Log in to the 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 [Equipment Requirements](#) for instructions on finding and downloading the appropriate OVA.
5. Click Next. Select a datastore from your system that has at least 250GB free.
6. Click Next. Select:
  - a. **Network mappings:** Check that your assigned port group(s) are configured as discussed in [Network Interfaces](#) above.

- 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: arohive
```

- 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
> _
```

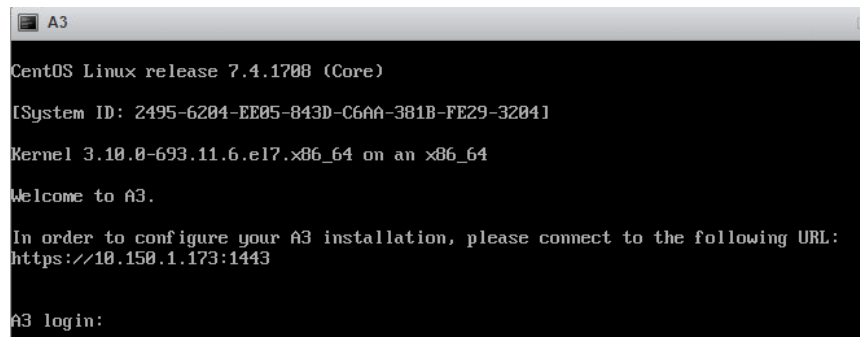
- c. Enter the following commands to set up your network using parameters applicable to the network that A3 is installed in.

```
network ip 10.150.1.4
network netmask 255.255.255.0
network gateway 10.150.1.1
network dns 10.150.1.5
show network
```

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

```
reboot
y
```

- The display should appear as below. Note the address shown in that window. This is the IP address assigned to the A3 instance by DHCP from your assigned server or manually in step 10. This will 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

A3 login:

```

## A3 Installation on Windows Server 2019 Hyper-V

Note the Hyper-V resource requirement detailed in [Equipment Requirements](#). The Hyper-V Manager is used to install A3.

### Network Interfaces

A3 must be attached to an “External” type of virtual switch. An external virtual switch binds to the physical network adapter so that the virtual machine can access a physical network.

A3 may be installed by following these instructions:

- Download an A3 Hyper-V release image, for example **A3-HYPERV-4.0.0-6.zip**, from the Extreme Networks support site. Unzip the file into a folder, for example **C:\tmp\A3-HYPERV.temp**.
- Invoke the Hyper-V Manager.
- Select **Import Virtual Machine** from the **Actions** panel.
- Select **Next >**.
- Select a folder with the virtual machine to import. For example **C:\tmp\A3-HYPERV.temp**.
- Select **Next >**.
- In the **Select Virtual Machine** step, select the virtual machine to import, which must have been previously created. For example, **A3-HYPERV**.
- Select **Next >**.
- In the **Choose Import Type** step, select *Copy the virtual machine (create a new unique ID)*.
- Select **Next >**.
- In the **Choose Folder for Virtual Machine Files** step, check the *Store the virtual machine in a different location* check box.
- Select the first **Browse...** button, and then navigate to a folder for use in holding the VM files. For example, **c:\tmp\hyper-v\**. Copy and past this value into all three fields.
- Select **Next >**.

14. In the **Choose Folder to Store Virtual Hard Disks** step, select the **Browse...** button and navigate to a folder to hold the disks. For example, `c:\tmp\hyper-v\disks\`
15. Select **Next >**.
16. In the **Completing Import Wizard** step, review the settings.
17. Select **Finish**.
18. The Hyper-V Manager will import the image.
19. When complete, the virtual machine will appear on the main Hyper-V Manager display.
20. Select **Edit Disk...** from the **Actions** panel.
21. Select **Next >**.
22. In the **Locate Virtual Hard Disk** step, select **Browse...**
23. Navigate to `a3-disk2.vhd` in the folder where disks were specified in step 14.
24. Select **Open**.
25. Back in the **Locate Virtual Hard Disk** step, select **Next >**.
26. In the **Choose Action** step, select **Convert**.
27. Select **Next >**.
28. In the **Convert Virtual Hard Disk, Choose Disk Format** step, verify that **VHD** is selected.
29. Select **Next >**.
30. In the **Convert Virtual Hard Disk, Choose Disk Type** step, select *Fixed size*.
31. Select **Next >**.
32. In the **Convert Virtual Hard Disk, Configure Disk** step, select **Browse...**
33. Navigate to the folder with the disks (`c:\tmp\hyper-v\disks\` in this example) and select `a3-disk2.vhd`.
34. In the **File name** field at the bottom of the dialog, change the name to `a3-disk2-fix.vhd`.
35. Select **Save**.
36. Back in the **Convert Virtual Hard Disk, Configure Disk** step, verify that the Name: field contains the renamed disk (`c:\tmp\hyper-v\disks\va3-disk2.vhd`).
37. Select **Next >**.
38. In the **Completing the Edit Virtual Hard Disk Wizard, Summary step**, verify the conversion from a VHD dynamically expanding disk to a VHD, fixed size disk.
39. Select **Finish**.
40. The wizard will now convert the disk. This can take several minutes.
41. When the process is complete, the main page for the Hyper-V Manager will be displayed.
42. Select the **A3-HYPERV** virtual machine in the top list. The details for the VM will be displayed in a panel entitled with its name.
43. In the **Actions** panel, under the **A3-HYPERV** title. Select **Settings...**
44. In the **Hardware** section of the **Settings** page, under **SCSI Controller**, select the Hard Drive named `a3-disk2.vhd`.
45. Select **Remove**. There should be no change in the display.
46. Under **Virtual hard disk:**, select the **Browse...** button. Select the `a3-disk2-fix.vhd` disk.
47. Select **OK**.

48. Back in the main Hyper-V Manager window, right-click on the **A3-HYPERV** machine and select **Connect...**
49. In the **A3-HYPERV on ... - Virtual Machine Connection** window, select **Start** from the **Action** menu.
50. The A3 instance will start.
51. 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: arohive
```

- 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
> _
```

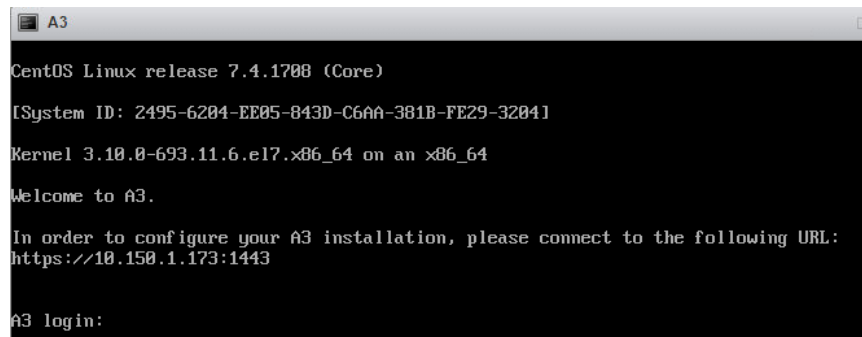
- c. Enter the following commands to set up your network using parameters applicable to the network that A3 is installed in.

```
network ip 10.150.1.4
network netmask 255.255.255.0
network gateway 10.150.1.1
network dns 10.150.1.5
show network
```

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

```
reboot
y
```

52. The display should appear as below. Note the address shown in that window. This is the IP address assigned to the A3 instance by DHCP from your assigned server or manually in step 10. This will 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

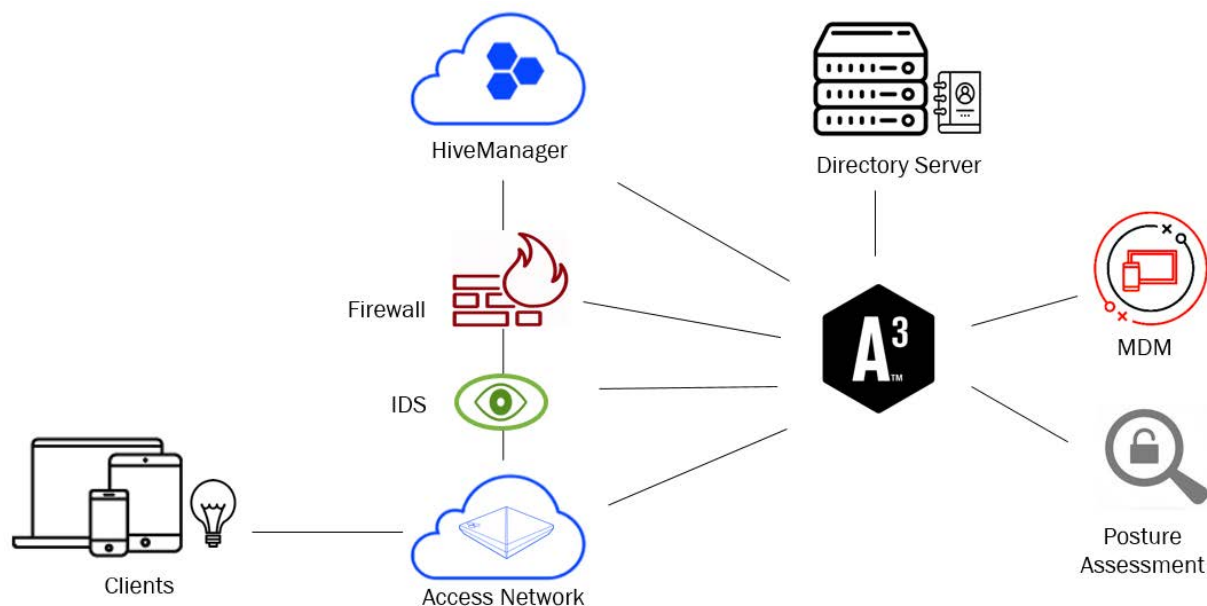
A3 login:
```



# Network Topology

## Connectivity and Security

A3 interfaces with many connectivity and security devices, as shown below.



The pictured components are:

1. **Clients** - networked devices, including computers, phones, tables, and headless IoT (Internet of Things) devices. Clients access an organization's networks through the access network.
2. **Access network** - one or more devices that serve to connect clients to networks. Access networks enforce security policies governing who is able to connect to what. The devices used in this capacity are discussed below in [Enforcement Devices](#).
3. **Extreme Networks A3** - software that works with other components to enforce access and security policy. Of critical importance in the manner in which A3 connects to and controls the access network.
4. **IDS** - intrusion detection systems watch clients and network traffic to detect unusual network activity. A3 uses alerts from IDS systems to trigger security events that can isolate clients and send alerts.

5. **Firewall** - firewalls control connections between networks. They can be used to limit client access to parts of the internal network through VLAN assignment, IP address restriction, or other means. A3 can send user identity information to firewalls to implement single sign-on.
6. **Cloud control (ExtremeCloud IQ)** - cloud-based control of network devices has become the gold standard for network administration. Most network device vendors offer a cloud and web based system. Pictured here, Extreme Networks's ExtremeCloud IQ is used to configure all Extreme Networks devices.
7. **Directory server** - one or more servers that are used to hold user and device identity information. LDAP (Lightweight Directory Access Protocol) compatible servers, including Microsoft's Active Directory, are the most common type.
8. **MDM (Mobile Device Management)** - central management systems used to configure, update, and control client devices. These are responsible for ensuring that the correct, updated software is installed on clients. A3 can request client status from such system, restricting client access.
9. **Posture assessment** - scanning tools that evaluate client acceptability for network access. Posture assessment tools can ensure that up-to-date software is installed and whether client systems manifest any security vulnerabilities.

## Enforcement Devices

---

A3 registers and authenticates clients, but enforcement devices ensure that clients are allowed or denied network access with appropriate restrictions. For example, a facility guest may be granted Wi-Fi access to the internet. An organization's employees may be assigned to networks appropriate for their jobs: engineering, management, finance, etc.

A3 inter-operates with different classes of enforcement devices:

- **Wi-Fi access points with integrated controller.** These devices allow Wi-Fi enabled devices to connect to a wired network while controlling that access. Extreme Networks access points fit in this category; their usage with A3 is described in this guide and in the ExtremeCloud IQ documentation.
- **Wi-Fi access points using a separate controller.** The access points provide connectivity and control access using the controller for decision making. A3 communicates with the controller to perform its functions.
- **Intelligent switches.** These devices enforce access on wired connections. Multiple clients connected to switch ports can be individually controlled. Wi-Fi clients connected to access points that have no controller function can be individually registered and authenticated.
- **Other devices.** Security appliances such as Cisco ASA can perform registration and authentication in conjunction with A3.

Extreme Networks access point usage with A3 is described in this guide and in the ExtremeCloud IQ documentation. All other supported devices are describe in the A3 Network Devices Configuration Guide.

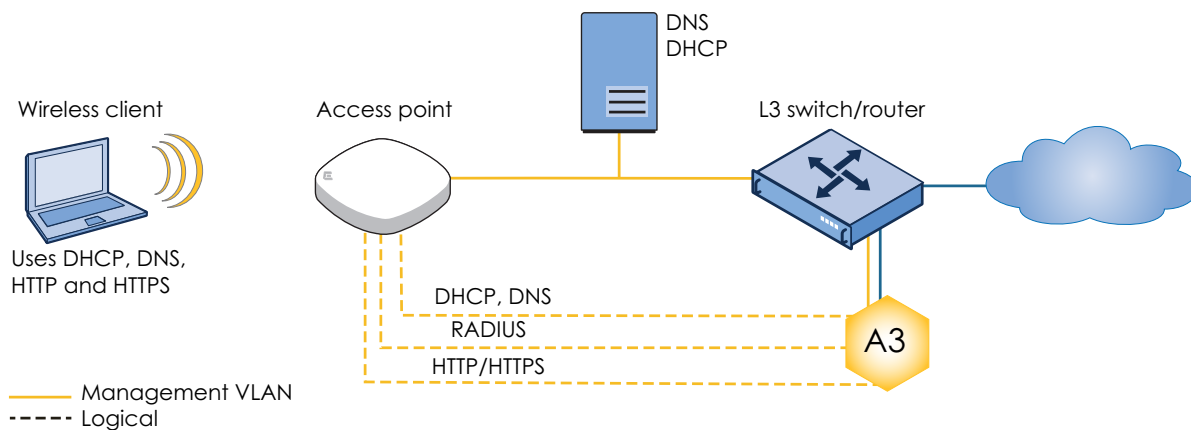
## Infrastructure Devices

Several other infrastructure devices are critical components of an A3-based system:

- **Switches.** Switches connect the various network components. Unmanaged switches can be used to connect A3 to other network components, but managed switches are preferred. A managed switch can be used to isolate clients on the registration and isolation networks from any elements that they should not be accessing.
- **Routers.** Routers connect networks together. When used with A3 they are used to connect the registration, isolation, and other networks used during authentication with the larger network. Routers can also be used as managed switches in smaller networks.
- **DHCP Servers.** DHCP servers provide clients with network addresses during client startup. Unless a client has been assigned a static address, they will broadcast a request to any available DHCP server. During registration A3 serves as the DHCP server, providing an IP address, gateway, and DNS server address(es).
- **DNS Servers.** DNS servers provide name to IP address mapping. During registration clients use A3's DNS server, which redirects them to the captive web portal and allow them access to limited external servers used for authentication.
- **Email.** Email messages are sent from A3 for administration, security events, and several types of registration. Email servers can be external or internal, but must always be publicly accessible.

## Layer 3 Topology

The A3 Layer 3 topology is straightforward and is shown below.



The figure uses a wireless client and Extreme Networks AP, but the concepts apply equally well with Wi-Fi access points and wireless controllers or wired computers and an intelligent switch. Physical connections are pictured as solid lines, while logical connections are shown as dashed lines.

A single management VLAN is used to register clients. The access device is configured to work with a local DNS and DHCP server. The access device and the A3 server have Layer

3 connectivity. Following authentication, one or more other VLANs or firewall rule sets may be used to provide appropriate client access.

A3 contains the web-based captive web portal and RADIUS server used during authentication. The client accesses these services using Layer 3 (IP) addressing.

Initial configuration of A3 requires the following addresses:

- **A3 permanent IP address** - as discussed in [Installation](#), the address that A3 is initially assigned may come from a DHCP pool defined in DHCP server for the network that A3 is attached to. This DHCP server is the organization's responsibility. During initial configuration, a permanent address will be assigned to the A3 server. This address must be statically assigned to an address not in the DHCP pool.
- **A3 permanent virtual IP address** - another IP address is required in the same network as the A3 permanent IP address to be used to access a cluster of A3 instances. This address must likewise be a static address not included in the DHCP pool. This address should be used in all cases when an A3 server address is required.
- **Domain name of the A3 server** - the domain in which the A3 server resides.
- **Access network enforcement device** - pictured as an Extreme Networks AP, it could be a Wi-Fi controller or switch. This address must likewise use a static address. It is needed even if the device is managed by a cloud management system.
- **Email information** - A3's alerting should be set up as part of initial configuration. This requires an administrator's email address and access to a publicly accessible email server. The latter item requires a email server name, protocol information, and email account and password.

**Optional server certificate** - although an SSL certificate can be later installed, if one exists for the server then initial configuration is a good time to install it.

# Clustering

A3 clusters provide load balancing and failover. There are some basic rules when using A3 clustering:

- Servers that form a cluster should always be installed using odd numbers, that is 3, 5, 7.
- Servers should not be installed on the same platform. Where possible they should use separate independent power sources and be connected to separate switches.
- Servers must all be on the same LAN segment (layer 2 connectivity).

## Cluster Installation

---

Each server in a cluster is referred to as a member. Cluster installation is straightforward:

1. Install the first member using the **New Deployment** option during A3 installation. This member is referred to as the master, or primary.
2. Install subsequent members using the **Join Cluster** option (instead of **New Deployment**).
  - a. Provide the address of the primary, and the administrator name and password used to install the master.
  - b. Clusters must be managed using the VIP (B) address instead of individual member addresses. The VIP address is the IP address assigned to the first A3 server installed in the cluster.
  - c. Configure network devices, including Extreme Networks AP configured through ExtremeCloud IQ, to use the VIP address of the cluster as their RADIUS server.

You can monitor and manage clusters from multiple A3 administration pages:

- The **Status** page displays informational graphs for each member.
- The **Cluster > Services** option on the **Configuration > System Configuration > Status** page displays a column for each member's services.
- The **Configuration > System Configuration > Cluster** option page shows the cluster members and their states.

## Cluster Operation

---

During normal operation network devices send their RADIUS requests to the VIP address of the cluster. The acting A3 master distributes the requests to one of the members.

If a cluster member fails, the master stops using that member and sends an alert to the administrator.

If the cluster master fails, one of the other members is automatically elected as the new master. When the original master again becomes active on the network, it thinks that it is still the master. The other cluster members then vote on which of these two will become the new master.

## Restarting Services

---

When advised to restart any A3 service, the administrative interface for each cluster member must be used individually to perform the operation. Restart services in each member one at a time, waiting for all services to completely restart.

## Graceful Shutdown and Restart

---

The best way to shut down all members is to shut down the non-master members first, and the master last. Restart the cluster devices using the opposite process (start the master first, then the cluster members). For example, if there are three members named 1, 2, and 3 with 1 as the master, then you should shut down using the order 3, 2, 1, and restart should in the order 1, 2, 3.

For each shutdown or restart step, make sure that operation has completed before starting the next step.

## Cluster Backup and Recovery

---

*Do not take a snapshot of a running member. This will temporarily cause it to halt and result in service disruption and a corrupt snapshot. To make an appropriate snapshot, stop the VM first.*

To guard against unexpected shutdowns, Extreme Networks recommends that you take snapshots of all the members of a cluster. Shut down the clusters as described in [Graceful Shutdown and Restart](#). Take snapshots of all members, then restart the members in reverse order. In the event of an ungraceful shutdown, restore the snapshots, then restart the members in the reverse order of the snapshot order.

When a snapshot is restored changes to the A3 configuration after the snapshots will be lost.

# Table of Addresses and VLANs

<sup>(1)</sup> *Ensure that none of the permanent addresses used are covered by a DHCP range.*

There are many components involved in a robust A3 implementation. Components are characterized by network names, real and virtual IP addresses, netmasks, gateways, VLANs, passwords, and configurations. A3 and many of the other components require configuration by IP addresses rather than symbolic names.

The tables in this chapter of the guide can be used to keep track of addresses, VLANs, and other values. The table keys are labeled with upper and lower case letters (A..Z, a..z) and V followed by a number for VLANs. The table items and are used throughout this guide, within parenthesis. For example,

## **10.150.1.254 (B)**

Refers to row B in the Addresses and VLANs table, which corresponds to the virtual address of the A3 server. The address 10.150.1.254 is one of the set of addresses used in this guide and corresponds to the value in the Example Assignment column of the table.

The tables include example values as a consistent set; an additional column is provided for administrators to insert their own values. Extreme suggests that you print out and use the tables for A3 configuration and maintenance.

If there should ever be a need to change any of the addresses or other values in an implementation, this guide can provide a handy reference for the locations in A3 where the address or values is used. The PDF for this guide can be used to searched for the corresponding (X) value.

Most use cases in this guide use [Firewall Enforcement](#). Other forms of enforcement use addressing that is similar or identical.

---

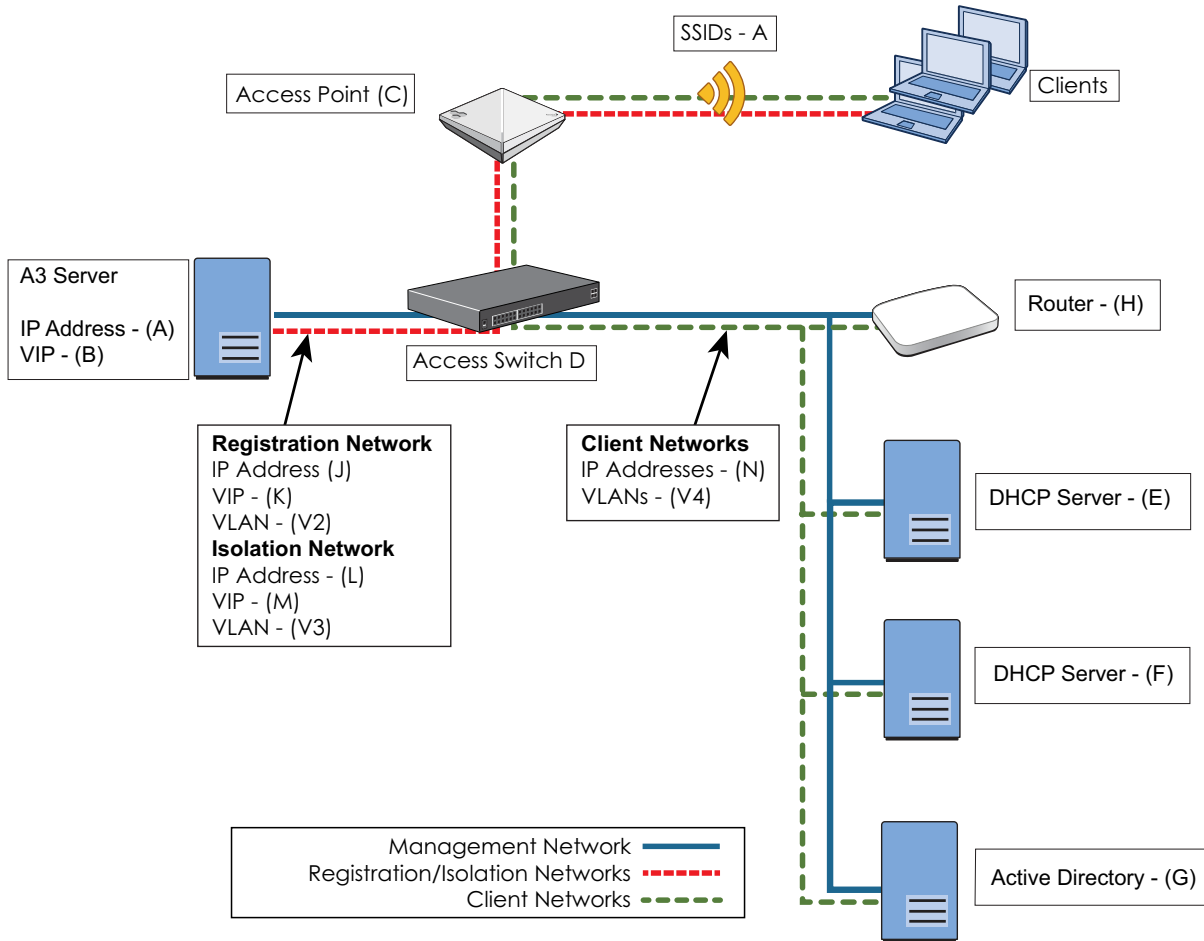
# Network Implementation

---

Refer to the following figures when referencing the [Addresses and VLANs](#) and [Other Values](#) tables. Separate figures are provided for Layer 2 and Layer 3 network topologies.



Refer to the following figures when referencing the [Addresses and VLANs](#) and [Other Values](#) tables. Separate figures are provided for Layer 2 and Layer 3 network topologies.



**Table 1: Addresses and VLANs**

Key	Usage	Example Assignment	Actual Assignment
A	Address of the A3 server instance. The A3 server must be assigned to the management VLAN. This address is initially assigned by DHCP or manually during installation and initial configuration. The VIP address (B) is normally used for A3 administration, unless a cluster is in place and the specific server must be accessed.	10.150.1.4/24	
B	Virtual IP address of the A3 cluster. This address is assigned as part of the initial configuration of the master A3 server. It is the address used by all other components, even when the cluster only has one member.	10.150.1.254	
C	Access Point address. This is used only once in ExtremeCloud IQ when bringing the access point under management and once in A3 to define an access control device.	10.150.1.19	
D	Access switch. This switch is used to connect A3 to all other network components.		
E	DHCP server for the network.	10.150.1.3	
F	DNS server for the network. In this example, it is hosted on the Active Directory server.	10.150.1.5	
G	Active Directory server. User and computer information used for several types of authentication.	10.150.1.5	
H	Router. The router is used to connect to the rest of the organization's network or to a remote site.	10.5.1.240	
N	Client networks. One or more networks used for authenticated clients. A3 associates the clients with a VLAN (V4) and the DHCP server (E) assigns them an address in that network.	10.150.10.0/24	
V1	VLAN 1, the management VLAN is connected to all components.	1	
V4	One or more client networks assigned after successful authentication. Connected to clients, access point (C), access switch (D), router (G), and infrastructure servers (D, E, and F).	2, 5, 8	

**Table 2: Other Values**

Key	Usage	Example Assignment	Actual Assignment
a	SSIDs defined in the access point (C).	A3-Guest, A3-Corp, A3-WA, A3-IoT	
b	Shared secret for RADIUS communications. This should be a strong password used to protect communications between A3 and the access point.	8AB7tHkP	
c	Name of the A3 server. This name is configured during <a href="#">Initial A3 Configuration</a> .	A3-Main	
d	Domain for network.	example.com	
g	RADIUS Filter_ID for guest role.	guest	
h	RADIUS Filter_ID for sales role.	sales	
i	RADIUS Filter_ID for marketing role.	marketing	
j	RADIUS Filter_ID for employee role.	employee	
k	ExtremeCloud IQ policy name for corporate access.	Corp-Policy	

# Initial A3 Configuration

## Setup IP Addresses

---

The initial configuration of A3 sets up some basic networking and naming parameters. In most cases, this guide uses tables and descriptive text to describe configuration. Two different Quick Start Guide performs the same functions, for registration VLAN and no registration VLAN configurations. Here are the steps for initial A3 configuration.

1. **Get started.** Access A3 with a browser using the URL obtained from the last step of [Installation](#). This is not the (A) or (B) address; those will be defined in this chapter.
2. **Warning.** A warning about your connection not being private will likely be displayed. This is due to the fact that A3 generates its own SSL certificate at installation time. Certificate generation to handle this problem is discussed in [A3 Server Certificate](#). Click the Advanced/Details button and select the appropriate button to proceed anyway.
3. **New Deployment.** For the first or only server in a cluster select GET STARTED from the New Deployment box.
4. **Clusters.** For the second and subsequent servers in a cluster, select GET STARTED from the Join Cluster box. Rules for non-primary cluster members is discussed in [Clustering](#).
5. **Email.** The next screen asks for the administrator's email address and a password. The email address will be your primary login name for all cluster members. Make sure to use a valid email address that you have access to. Select **Next**.
6. **License.** Agree to the licensing terms. Select **SUBMIT**.
- 7.
8. **Addressing.** The next screen is used to set IP addresses for A3. Use the following steps in order.
  - a. **VIP.** In the VIP field, enter the (B) address. The VIP address is the main point of contact for network devices and A3 for all cluster members. All cluster members use the same VIP address. Erase all the characters in the field and type in your new address. Press the check box to accept the setting.
  - b. **IP Address.** Change the IP Address to the (A) address. Press the check box to accept the setting. A3 will change the address reload the page at the new address. This may take a few minutes. If for some reason it does not restart, you can refresh it with the <https://<new IP address>:1443>.
  - c. **Host name.** Change the host name to something appropriate for your installation. A3-Main (c) is used in this guide.
  - d. Select **Next**.

<sup>(1)</sup> All A3 instances default to "A3" as their host name. Only one member in a cluster can use the "A3" name.

9. **Link to Cloud.** (Highly suggested) The next screen links your A3 instance with ExtremeCloud IQ for configuration and monitoring. Extreme Networks strongly suggests that an account be established and linked to the A3 instance. Beginning with A3 version 4.0.0, licenses are distributed from your cloud account. **The use of NAC entitlements is mandatory for all production environments.** If you skip this step, you will only have a limited time to link with ExtremeCloud IQ.

Enter the ExtremeCloud IQ specifics that you obtained in [Extreme Networks Requirements](#) and select LINK WITH CLOUD ACCOUNT. Once this A3 instance is registered with ExtremeCloud IQ, you will be able to distribute NAC Entitlements between installations. Further, accessing A3 from ExtremeCloud IQ will automatically pass down authentication information so that administrative login will not be required.

A3 automatically generates a device certificate to authenticate the A3 server to ExtremeCloud IQ. The status of the certificate can be found at **Configuration > System Configuration > Cloud Integration**.

When the cloud link is active, after upgrading to a 4.0 version from a 3.x version, the XIQ Cloud Admin password previously used to connect to the cloud must be re-entered.

To skip this step, select Continue without a Cloud Account.

10. **License.** The next screen offers a choice for a 30-day trial of A3. Select START A 30-DAY TRIAL PERIOD unless you have a legacy entitlement key. A key can be entered at a later date unless you have linked to ExtremeCloud IQ and configured ExtremeCloud IQ to distribute NAC entitlements as part of the new licensing model.
11. **Startup.** When A3 says configuration is complete, its services will start.
  - a. This may take up to 10 minutes. Wait for all services to start.
  - b. Enter the A3 configuration interface by selecting GO TO ADMINISTRATIVE INTERFACE or invoking the interface via [https://<VIP address \(B\)>:1443](https://<VIP address (B)>:1443).
  - c. Log in with the administrator's credentials.

## Domain and Time Zone

---

The domain and time zone are best configured next.

1. **General Configuration.** Select Configuration > System Configuration > General Configuration.
2. **Domain and host name.** The domain and host name configured on this page are only used for the captive web portal URL offered to clients. For example, if the Domain is set to example.com (d) and the Host Name is set to A3-Main (c), then the CWP will be invoked as A3-Main.example.com.
3. **DHCP Servers.** Comma-separated list of DHCP servers on the network. These are used after A3 releases a user from the isolation and registration networks.
4. **Time zone.** Set the Time Zone to your local time zone. Note that the U.S. cities are listed under America/<city> and sometimes America/<state>/<city>.

**(1)** *Services must be individually restarted on each member of a cluster. Restarting services will disable authentication for a period of time.*

5. **Press Save.** If you have changed the host name or added a domain name, a warning message will prompt you to restart the haproxy-portal service. Press **Save** again after haproxy-portal has restarted.
6. **DNS setup (external configuration).** Add an A record for the A3 VIP address to the network's DNS service. The A record should resolve to the VIP address.
  - DNS zone: example.com (d)
  - Host name: A3-Main (c)
  - IP address: 10.150.1.254 (B)

## Alerting

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

1. **Alert Configuration.** Select Configuration > System Configuration > Alerting.
2. **SMTP.** Enter the following essential changes:.


Entry	Example Value	Notes
Recipients	admin@example.com	One or more email addresses for those who will receive alert messages.
SMTP server	smtp.gmail.com	Either a local SMTP server, a public web server such as gmail or any public mail service for which you have credentials. Gmail's mail server is smtp.gmail.com.
SMTP encryption	ssl	The type of encryption appropriate for your SMTP server. Gmail's uses ssl.
SMTP port	465	The port number appropriate for your SMTP server. Gmail's uses port 465.
SMTP user name	example-admin@gmail.com	The SMTP account name on the SMTP server.
SMTP password	bigsecret	The SMTP password associated with the account.

3. **Test.** The SMTP configuration can be tested by selecting Tools > SMTP. Enter one or more email addresses and select **Test**; 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.

## Change Admin Password

The administrator name and password entered during installation stays with the A3 data forever. It is most common to use the form <user-name>@<company.com> for the user name. Names of that form are convenient because alert email is sent to that address and the address may be used for Active Directory lookup. In fact, as soon as a join to an active directory is performed (as in [Use Case 2: Active Directory Authentication](#)), the active directory is queried when it is used for administrative access.

If the Active Directory should ever fail, it will be impossible for the administrator to login. To provide a backup A3 in the form of an **Admin** user in the **Users** tab of the GUI. The password was automatically generated, but can and should be changed at this juncture:

1. Navigate to **Users**.
2. Select **Admin**
3. Select the **Password** tab.
4. Enter a new password in the **Password** field. The same password used during installation might make it easier to remember.
5. Press .

To provide an alternative account that you can use to access A3, update the password for the **admin** user in the **Users** GUI tab.

## A3 Server Certificate

---

The browser warnings encountered in the first step of [Initial A3 Configuration](#) are due to the fact that the web administration page uses HTTPS. During the initial handshake between the browser and A3 administrative server, A3 sends its SSL certificate to the browser.

A3's initial certificate is generated during installation and is a self-signed certificate. That is, the certificate is for the server and is signed by the server. All modern browsers will generate warnings when they see self-signed certificates. If the certificate is not replaced, then administrators and clients will continue to receive these warnings.

To resolve this, a new certificate generated by a well-trusted certificate authority should be installed. A3 provides the means to request a certificate and install it in the appropriate place in A3. These techniques are covered in [Certificates and PKI](#).

# ExtremeCloud IQ Setup

This chapter covers two common configurations of ExtremeCloud IQ for use with A3. Other access devices are configured in similar ways, especially intelligent access points and access controllers.

The two configurations covered in this chapter are:

- [MAC Authentication](#)
- [802.1X Authentication](#)

This discussion assumes that ExtremeCloud IQ account discussed in [Extreme Networks Requirements](#) has been used to log in to ExtremeCloud IQ. The access points to be used must have been on-boarded.

Devices are on-boarded by selecting the  in the menu bar at the top and entering the device's serial number when requested.

## MAC Authentication

---

The instructions in this section of the guide explain how to set up ExtremeCloud IQ for MAC authentication for use in guest access to a Wi-Fi network. This chapter is essentially the same as the Quick Start Guides that cover registration VLAN and no registration VLAN environments.

There are four major steps in setting up access points for MAC authentication:

1. [Network Policy](#). The **A3-Guest (a)** SSID is defined.
2. [Authentication](#). Open SSID with MAC authentication is selected.
3. [Guest User Profile](#). A user profile is defined that uses a firewall rule sets to restrict network access for registration.
4. [Isolation User Profile](#). A user profile is defined to handle cases when A3 determines a client violation has occurred.
5. [Deploy Policy](#). The configuration is pushed to the access point.















## Network Policy

A new network policy is defined by selecting CONFIGURE > NETWORK POLICIES. Select

.

1. **Policy Details**. Check the Wireless box only and enter **Corp-Policy (k)** as the Policy Name. Click SAVE; the Wireless Networks tab is displayed.
2. **Network**. Select  and then All Other Networks (Standard). Enter **A3-Guest (a)** in the Name (SSID) field. The Broadcast Name is automatically filled in as **A3-Guest** as well.

## Authentication

1. **Open Unsecured.** Since the SSID will be used for guest access, select . Clients 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. **MAC Authentication.** Select the MAC Authentication tab and enable MAC Authentication.
3. **RADIUS Server.** A RADIUS Server group is defined next. This is a set of RADIUS servers that can be queried by access points.
  - a. Click the  sign beside Default RADIUS Server Group.
  - b. In the Configure RADIUS Servers dialog, select Extreme Networks A3 and click the  sign to add a new RADIUS server.
  - c. Fill in the Extreme Networks A3 Server dialog:
    - i. Name as **A3-RADIUS**. Description as desired.
    - ii. IP/Host Name: use the  sign to add the A3 VIP address 10.150.1.254 (B) as the Name and IP Address.
    - iii. Shared Secret as **8AB7tHkP** (b). This is used to hash and unhash information exchanged with the A3 server.
    - iv. Click .
    - v. Enter **A3-RADIUS-SERVER-GROUP** in the RADIUS Server Group Name field, check the box next to A3-RADIUS and click .
4. **Default User Profile.** The means by which A3 ensures proper guest access is 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. A set of firewall rules are used that restrict client access. Clients may access A3, use DNS and DHCP on their network, but are redirected to A3 when they try any http: or https: access.
  - a. Select the  sign on the line containing Default User Profile to access the Create User Profile dialog.
  - b. Enter **Registration-NV** in the User Profile Name.
  - c. If the VLAN number listed is not your management VLAN, then select  sign. If your management VLAN is in the list, select it. If not, select **New**, and then define your new VLAN number. Enter the number in both the Name and VLAN ID fields.
  - d. Select .
  - e. Turn on Firewall Rules and then name the IP Firewall **Registration-NV-FW**.
  - f. 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.
  - g. Press the  sign to define the first firewall rule.
  - h. 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 .
    - ii. Select the  beside Destination IP, and then the IP address of the A3 server, 10.150.1.254 (B).
    - iii. Select  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-Main.example.com/Aerohive::AP**. This invokes A3 when a registering user attempts to reach any web page.
5. Select **SAVE USER PROFILE** to save the new user profile.



## Guest User Profile

- Select "Allow a different user profile to various clients and user groups".
- Guest Profile.** Select **ADD** above User Profile Name to create a Guest User Profile with VLAN 2 (V4).
  - Enter **Guest** 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 VLAN**.
- Assignment Rule.** 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. Before adding an assignment rule based on a filter ID, the "Allow user profile assignment using RADIUS attributes in addition to the three tunnel RADIUS attributes" must be set.
  - Select the  on the Guest line in the Assignment Rules column.
  - Enter the name **A3-Guest-Rule** in the Name field
  - Select the **+** symbol, and select RADIUS Attribute.
  - Note that 11\_Filter-Id has been preselected. Fill in the Attribute Values field with **guest** (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**.
- Click **SAVE**.

## 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 an isolation state.

- Select  above User Profile Name and select **Registration-NV**.
- Select the  on the **Registration-NV** line in the Assignment Rules column.

3. Enter the name **Isolation-Rule** 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. Click  .

## Deploy Policy

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

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

This completes ExtremeCloud IQ configuration for MAC authentication.

## 802.1X Authentication

---

The instructions in this section of the guide explain how to set up ExtremeCloud IQ for 802.1X authentication for use in employee access to a Wi-Fi network.

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




1. [Network Policy](#). The **A3-Corp** (a) SSID is defined.
2. [Authentication](#). Enterprise authentication is selected.
3. [User Profiles](#). Three user profiles are associated with the network policy.
4. [Deploy Policy](#). The configuration is pushed to the access point.

### Network Policy

A new network policy is defined by selecting CONFIGURE > NETWORK POLICIES. Select ADD NETWORK POLICY.

1. **Policy details**. If a network policy has previously been defined, as would be the case if you followed the instructions for the [MAC Authentication](#) example, then the CONFIGURE page with a listing for the Corp-Policy network policy will be displayed.
  - a. If a network policy is displayed, then:
    - i. Click the network policy name (**Corp-Policy**).
    - ii. Select the Wireless Networks tab.
  - b. If no existing network policy is displayed, then:
    - i. Select ADD NETWORK POLICY.
    - ii. Fill in the Policy Details: check the Wireless box only and enter **Corp-Policy** as the Policy Name.
    - iii. Click SAVE to move to the Wireless Networks tab.
2. **Network**. Select ADD and then All Other Networks (Standard). Enter **A3-Corp** (c) in the Name (SSID) field. The Broadcast Name is automatically filled in as A3-Corp as well.

### Authentication



1. **Enterprise**. Since the SSID will be used for employee access, select **Enterprise** below SSID Authentication.
2. **RADIUS Server**. A RADIUS Server group is a set of RADIUS servers that can be queried by access points.
  - a. If you have previously defined a RADIUS server group in a previous example, you can reuse it.
    - i. Click the  icon beside Default RADIUS Server Group.
    - ii. Place a check mark beside the previously defined server group name.
    - iii. Click SELECT.
  - b. If a server group has not been defined yet.
    - i. In this example, only one RADIUS server will be used. Click the  sign beside Default RADIUS Server Group.
    - ii. In the Configure RADIUS Servers dialog, select **Extreme Networks A3** and click the  sign to add a new group.

**NOTE:** 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 as **A3-RADIUS**. Description as desired.
  - ii. IP/Host Name: use the **+** sign to add the A3 VIP address 10.150.1.254 (B) as the Host Name and IP Address.
  - iii. Shared Secret as **8AB7tHkP** (b). This is used to hash and unhash information exchanged with the A3 server.
  - iv. Click SAVE Extreme Networks A3.
  - v. Enter **A3-RADIUS-SERVER-GROUP** in the RADIUS Server Group Name field, check the box next to A3-RADIUS and click SAVE RADIUS.
3. **Default User Profile.** 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 VLAN associated with the default-profile.
  - a. Continue down the screen to Authenticate via RADIUS Server, User Access Settings.
  - b. Select the **+** sign on the line containing Default User Profile to access the Create User Profile dialog.
    - a. Enter **Employee** in the User Profile Name.
    - b. Select the **+** icon and choose 8 if it is in the list, otherwise select plus sign to add VLAN 8 (V4).
      - i. Enter **8** (V4) in both the Name and VLAN ID fields.
      - ii. Select SAVE to save the VLAN object.
      - iii. Select SAVE USER PROFILE to save the new user profile.
4. 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.
5. 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. The access point's profile assignment will key off of the value of the 11\_Filter-Id RADIUS attribute received from A3.

## User Profiles

1. **Sales Profile.** Select ADD above User Profile Name to obtain create a Sales User Profiles with VLAN 2 (H).
  - a. Enter **Sales** into the User Profile Name.
  - b. The VLAN to Connect to is either selected from a list of those already defined with the **+** icon, 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.
2. **Marketing Profile.** Select ADD again to obtain a **Marketing** User Profile with VLAN 5 (I) using the same procedure as in the previous step.
3. **Assignment Rules.** 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.
  - a. Select the **+** icon on the **Sales** line in the Assignment Rules column.

- b. Enter the name **A3-Sales-Rule** in the Name field, click the + symbol, and select RADIUS Attribute.
- c. Note that 11\_Filter-Id has been preselected. Fill in the Attribute Values field with *sales* (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.
- d. Repeat the procedure for the **Marketing** profile, using the name **A3-Marketing-Rule** and attribute value of **marketing** (i).
- e. Under Assignment Description click the  button to expand both descriptions. The display should appear as below. Click .

## Deploy Policy

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

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

This completes ExtremeCloud IQ configuration for 802.1X authentication.

# Authentication Methods

A3 using a number of technologies to authenticate users. Its authentication methods are divided in four broad categories:

- [External Authentication Sources](#)
- [Internal Authentication Sources](#)
- [Exclusive Authentication Sources](#)
- [Billing Authentication Sources](#)

Description of authentication technologies is included at the end of the chapter.

This chapter also discusses:

- [802.1X](#)
- [EAP and X.509 Certificates](#)
- [Social Login Authentication Technology](#)

## External Authentication Sources

---

External authentication sources utilize identity information obtained either directly or indirectly from the client. An identity confirmation is used in all cases except for the null authentication source. All external authentication sources work in conjunction with the CWP (captive web portal), customization of which is discussed in [Portal Modules](#). The CWP can require the client to agree to a Terms of Service/Acceptable Use Policy agreement before being allowed access.

A wide range of social media authentication mechanisms are used.

The external authentication sources are:

- **Null** - no identification is required.
- **Email** - the client enters their email address, which A3 uses to send a message. The message that the client receives includes a link that will complete the authentication. This form of authentication requires that [Alerting](#) be set up during [Initial A3 Configuration](#).
- **SMS** - the client enters their cell phone number, which A3 uses to send an SMS message. The message that the client receives includes a PIN (personal identification number) that is entered into the CWP page to complete the authentication. This form of authentication requires that [Alerting](#) be set up during [Initial A3 Configuration](#).
- **Sponsor** - the client enters their name and the email address of a sponsor within the organization authorized to allow sponsored access. The sponsor receives an email that includes a link that will complete the users authentication. This form of authentication requires that [Alerting](#) be set up during [Initial A3 Configuration](#).

- **Social login** - any of a number of social media sites are used to authenticate the client. Social media technology is described in [Social Login Authentication Technology](#). Clients are directed to log in to the social media site if they have not already done so. Their authentication information is returned to A3.

The A3 administrator must pre-configure access on the social media site to obtain several security parameters. These parameters are entered into A3 as part of the definition of a social media authentication source.

The registration for social media authentication methods supported by A3 are:

- [Clickatell API Registration](#)
- [Facebook API Registration](#)
- [Github API Registration](#)
- [Google API Registration](#)
- [Instagram API Registration](#)
- [Kickbox API Registration](#)
- [LinkedIn API Registration](#)
- [OpenID API Registration](#)
- [Pinterest API Registration](#)
- [Twilio API Registration](#)
- [Twitter API Registration](#)
- [WindowsLive API Registration](#)

Note that the registration process for each of the sites is maintained by the social media vendor and may change without notice.

## Clickatell API Registration

To use Clickatell as an SMS source:

1. Register at <https://www.clickatell.com> to get an API Key for the SMS integration.
2. Add it as an authentication source the same way as for SMS, except choosing 'Clickatell' instead of 'SMS' in 'Add source ? External'.
3. Enter a name, description and your Clickatell API key in the source configuration, then add the authentication rule.

## Facebook API Registration

The Facebook API registration is located at <https://developers.facebook.com/apps>.

1. Create an App; the URI for the **Website URL** field should be **https://<hostname>/oauth2/callback**, where **<hostname>** should be the A3's CWP, or other location if it is hosted elsewhere. This same value is entered into the **Portal URL** field in A3. This should be the same name as found in Configuration > System Configuration > General.
2. The Facebook API site will provide the **App ID** and **App Secret** fields at **Settings > Basic**.

## Github API Registration

The Github API registration is located at <https://github.com/settings/applications>.

1. Create an App; the URI for the **Callback URL** field should be **https://<hostname>/oauth2/callback**, where **<hostname>** should be the A3's CWP, or other location if it is hosted elsewhere. This same value is entered into the **Portal URL** field in A3. This should be the same name as found in Configuration > System Configuration > General.
2. The Github API site will provide the **App ID** and **App Secret** fields.

## Google API Registration

The Google API registration is located at <https://console.developers.google.com/>.

1. In the Google APIs Console, select Credentials > Create Credentials > Oauth client ID.
2. Select Configure consent screen.
  - a. Fill in the Application name as **A3**.
  - b. Enter **example.com** (d) in the Authorized domains field and press ENTER.
  - c. Click Save.
3. Select Web application, enter Name as **A3**, and then select Create.
4. Enter a name; the URI for the **Authorized redirect URI** field should be **https://<hostname>/oauth2/callback**, where **<hostname>** should be the A3's CWP, or other location if it is hosted elsewhere. This same value is entered into the **Portal URL** field in A3. This should be the same name as found in **Configuration > System Configuration > General**.
5. The Google API site will provide the **App ID** (Client ID) and **App Secret** (Client Secret) fields.

## Instagram API Registration

The Instagram API registration is located at <https://www.instagram.com/developer/clients/manage/>.

1. Create an App; the URI for the **Website URL** field should be **https://<hostname>/oauth2/callback**, where **<hostname>** should be the A3's CWP, or other location if it is hosted elsewhere. This same value is entered into the **Portal URL** field in A3. This should be the same name as found in Configuration > System Configuration > General.
2. The Instagram API site will provide the **App ID** and **App Secret** fields.

## Kickbox API Registration

An API key is required to use Kickbox. Use the following guidelines:

1. Create an account on <https://kickbox.io>.
2. Navigate to <https://app.kickbox.com/settings/keys>. Select **API Keys > Create Key**. Select a name and choose **Production mode** and **Single verification**.
3. The website will provide the API Key.

## LinkedIn API Registration

The LinkedIn API registration is located at <https://developer.linkedin.com/>.

1. Create an App; the URI for the **Callback URL** field should be **https://<hostname>/oauth2/callback**, where **<hostname>** should be the A3's CWP, or other location if it is hosted elsewhere. This same value is entered into the **Portal URL** field in A3. This should be the same name as found in Configuration > System Configuration > General.



2. The LinkedIn API site will provide the **App ID** and **App Secret** fields

## OpenID API Registration

The OpenID API registration is located at <http://openid.net/connect> along with information on how to create your own host or get one from a provider.

1. Create your App; the URI for the **Portal URL** field should be **https://<hostname>/oauth2/callback**, where **<hostname>** should be the A3's CWP, or other location if it is hosted elsewhere. This same value is entered into the **Portal URL** field in A3. This should be the same name as found in Configuration > System Configuration > General.
2. The OpenID API site will provide the **App ID** and **App Secret** fields.

## Pinterest API Registration

The Pinterest API registration is located at <https://developers.pinterest.com/apps>.

1. Create your App; the URI for the **Redirect URL** field should be **https://<hostname>/oauth2/callback**, where **<hostname>** should be the A3's CWP, or other location if it is hosted elsewhere. This same value is entered into the **Portal URL** field in A3. This should be the same name as found in Configuration > System Configuration > General.
2. The OpenID API site will provide the **App ID** and **App Secret** fields.

## Twilio API Registration

1. Create an account at <https://www.twilio.com>.
2. From the console (dashboard) at <https://www.twilio.com/console> create a 3rd Party Integration. Note the **Account SID** and **Auth Token** for later use.
3. From the Phone Manager <https://www.twilio.com/console/phone-numbers/incoming>, click the "+" button to **Buy a number with SMS capability** - no payment is needed to start using this phone number right away.

## Twitter API Registration

The Twitter API registration is located at <http://apps.twitter.com>.

1. Create an App; the URI for the **Redirect URI** field should be **https://<hostname>/oauth2/callback**, where **<hostname>** should be the A3's CWP, or other location if it is hosted elsewhere. This same value is entered into the **Portal URL** field in A3. This should be the same name as found in Configuration > System Configuration > General.
2. The Twitter API site will provide the **App ID** and **App Secret** fields.

## WindowsLive API Registration

The Twitter API registration is located at <https://developers.pinterest.com/apps>.

1. Create an App; the URI for the **Redirect URI** field should be **https://<hostname>/oauth2/callback**, where **<hostname>** should be the A3's CWP, or other location if it is hosted elsewhere. This same value is entered into the **Portal URL** field in A3. This should be the same name as found in Configuration > System Configuration > General.
2. Check **Live SDK support**.
3. The Twitter API site will provide the **App ID** and **App Secret** fields.

# Internal Authentication Sources

---

Internal authentication sources are methods for which the organization deploying A3 has control. Only internal authentication sources may be used for 802.1x/EAP authentication. The sources that are available are:

- **Active Directory (AD) / LDAP** - uses an LDAP compatible directory, including Window's Active Directory, for identity and group information. The Associated Realm parameter in the LDAP Authentication definition ties the definition to particular domain controllers.
- **Authorization** - performs authorization without client input.
- **Azure AD** - performs authentication using Azure's Active Directory service. It can be used for user authentication on the captive portal, administrator authentication, and for 802.1X users using EAP-TTLS PAP. The OpenID implementation of Azure AD is an easier alternative if only user authentication is required. Azure registration is required and is discussed in [Azure AD Registration](#).
- **EAP-TLS** - uses the EAP-TLS protocol for LDAP access. Requiring client certificates, EAP-TLS is a common EAP method used. The client and server perform mutual authentication and form encryption keys based on certificate contents. The Associated Realm parameter in the LDAP Authentication definition ties the definition to particular domain controllers. EAP technology is discussed in [EAP and X.509 Certificates](#).
- **Edirectory** - uses a NetIQ Edirectory for authentication.
- **Google Workspace LDAP** - an LDAP integration what works in conjunction with Google Workspaces.
- **Htpasswd** - uses a flat file with name and password commonly used in basic authentication on Apache HTTP servers.
- **HTTP** - permits access to A3 via an API that uses basic authentication. It is used, for example, to allow AD servers to send notice of user changes. See [Active Directory Integration](#).
- **Kerberos** - uses a Kerberos server. A Kerberos server is embedded within the A3 server and may be referenced with an IP address of 127.0.0.1. A list of users may be maintained in the Users top level menu option.
- **Password of the Day** - generates a password regularly that is mailed to an administrator. The administrator then distributes it to clients who use the password for authentication.
- **RADIUS** - uses a RADIUS server. A FreeRADIUS is embedded within the A3 server and may be referenced with an IP address of 127.0.0.1. A list of users may be maintained in the Users top level menu option.
- **SAML** - SAML (Security Assertion Markup Language) is an open standard based on XML for exchanging authentication and authorization data. It was initially designed to support single sign-on for web browsers.

## Azure AD Registration

1. Open the **Azure Active Directory** in your Azure portal.
2. Select **Manage > Application registrations > New registration**.
3. Enter the following settings for the application:
  - a. Name: **A3**

- b. Supported account types: **Accounts in this organizational directory only - (Single tenant)**
  - c. Redirect URI: leave blank
4. Select **Save**.
5. Note the displayed **Application (client) ID** and **Directory (tenant) ID** for later use.
6. Still within the application, select **Certificates & secrets > New client secret**.
7. Make the following entries:
  - a. Description: **A3**.
  - b. Note the expiration date so that it can be renewed when necessary. Failure to renew will cause A3 to stop working for Azure AD authentication.
  - c. Select **Save** to save the secret.
8. Note the **Value** of the **client secret**.
9. Select **API permissions > Add a permission**.
  - a. Select the **Microsoft APIs** tab
  - b. Select **Microsoft Graph > Application permissions**.
  - c. Add the **Directory.Read.All** permission.
  - d. Select **Grant admin consent**.
  - e. Confirm that **User.Read** is selected as a delegated permission.

## Disabling Multi-Factor Authentication

At the present time, A3 requires that multi-factor authentication (MFA) be disabled for the A3 application. If you are using Azure AD Premium, you can create a rule to exclude MFA for the A3 application. If not, MFA must be disabled for all users.

### Disabling MFA On Azure AD Premium

1. Open the **Azure Active Directory** in your Azure portal.
2. Select **Manage > Properties > Manage Security defaults**.
3. Disable **Enable Security defaults**.
4. Select **Save**.
5. Select **Manage > Security > Conditional Access**.
6. Select **New Policy** and make the following entries:
  - a. Name: **2FA policy**.
  - b. Under **Users and groups**, select **All users**.
  - c. Under **Cloud apps or actions**:
    - a. Select the **Exclude** section.
    - b. Within the **Select excluded cloud apps** section, select the **A3** application created earlier.
    - c. Within the **Grant** section, select **Grant access**.
    - d. Check **Require multi-factor authentication** and any other settings that your organization requires.
    - e. At the bottom of the dialog, ensure that **Enable policy** is set to **On**.
    - f. Select **Save**.

### Disabling MFA On Azure AD Non-Premium

Note: the following steps will disable common Microsoft recommended settings. This option is only suggested for testing or when it is impossible to use Azure AD Premium.

1. Open the **Azure Active Directory** in your Azure portal.
2. Under **Manage**, select **Properties**.
3. Select **Manage Security defaults**.
4. Disable the **Enable Security defaults** toggle.
5. Select **Save**.

### Setting Up a Realm for Azure AD

1. Under **Configuration > Policies and Access Control > Realms**, create a new realm with the following characteristics:
  - a. **Realm**: enter the realm of your Azure AD users. For example, if the user names have the format **box@example.onmicrosoft.com**, then the realm should be set to **example.onmicrosoft.com**.
  - b. In the **Stripping** tab of the realm, select your Azure AD source under **Azure AD Source for TTLS PAP**. Uncheck the following settings:
    - Strip on the portal
    - Strip on the admin
    - Strip on RADIUS authorization
2. Save the realm.
3. Restart the **radiusd** service on the **Status > Services** page.

All the users matching this realm will authenticate against Azure AD. Ensure that you also have a connection profile with auto-registration enabled with the Azure AD source.

## Google Workspace LDAP Registration

1. Open <https://admin.google.com/> and sign in as a Google Workspace domain administrator.
2. Navigate to **Apps > LDAP > Add Client**.
3. Enter an **LDAP client name** and an optional **Description**. For example, the name could be **A3** and the description could be **A3 LDAP Client**.
4. Select **Continue**.
5. Set **Access Permissions** for your organization. You must choose either:
  - **Entire domain (A3)**
  - **Selected organizational units** for both **Verify user credentials** and **Read user information**.
6. Select **Add LDAP Client**.
7. Download the generated certificate. This is required for A3 to communication with the Google Secure LDAP service. Save the certificate for later use.
8. Select **Continue to Client Details**.
9. Expand the **Service Status** section. For the **LDAP client** choice, select **On for everyone**.
10. Select **Save** and select the Service Status bar again to collapse it.

11. Expand the **Authentication** section and choose **Generate New Credentials**. Note these credentials for later use.
12. Select **Close** and click on the **Authentication** bar again to collapse it.
13. This completes the registration process on the Google Workspace site.

### Configuring A3

1. Select **Configuration > Policies and Access Control > Authentication Sources**.
2. Create a new **Google Workspace LDAP** internal source.
3. Enter the following values saved from the registration process above:
  - a. **BIND DN**: the access credentials username.
  - b. **Password**: the access credentials password.
  - c. **Client Certificate**: the *.crt* file text from the downloaded certificate.
  - d. **Client Key**: the *.key* file text from the downloaded certificate.
4. This completes the A3 setup for Google Workspace LDAP.

---

## Exclusive Authentication Sources

---

When used, exclusive authentication sources must be the only authentication source used in a connection profile. Several authentication sources are included in the exclusive category:

- **AdminProxy** - an authentication mechanism used in Microsoft systems for administrator single sign-on.
- **Blackhole** - an authentication mechanism that denies authentication for the client. This can be used to deny clients access that would otherwise be granted.
- **Eduroam** (education roaming) - a global example of realm-based authentication. The technology behind Eduroam is based on the IEEE 802.1X standard and a hierarchy of RADIUS proxy servers. Eduroam is a secure, worldwide roaming access service developed for the international research and higher education community. [Use Case 8: Eduroam](#) describes how to configure A3 to work with eduroam.

---

## Billing Authentication Sources

---

Billing authentication sources provide authentication following successful payment. The A3 administrator must pre-configure access on the billing site to obtain several security parameters. These parameters are entered into A3 as part of the definition of a billing authentication source.

Billing tiers are defined in Configuration > Advanced Configuration > Billing Tiers. The means by which each is pre-configured is described below. Note that the registration process for each of the sites is maintained by the vendor and may change without notice.

The sources that are available are described in:

- [AuthorizeNet](#)
- [Mirapay](#)
- [PayPal](#)
- [Stripe](#)

### AuthorizeNet

Registration for the AuthorizeNet authentication API is located at <https://account.authorize.net>. (A sandbox account may be set up at <https://developer.authorize.net/>).

1. When you create the account, the AuthorizeNet API site will provide an **API login ID** and **Transaction Key** which should be used in the authentication definition.
2. Login into your new account. Click **Settings** under **Account**.
3. In the Security settings of that page click MD5-Hash. Enter a shared secret in the Hash Value field.

### Mirapay

Mirapay account and API registration is available at <https://www.eigenpayments.com/>.

## PayPal

Use the following guidelines to create a Sandbox account:

1. Registration for use of the PayPal authentication API is located at <https://developer.PayPal.com/>.
2. Click Accounts in the Sandbox menu.
3. Create an account that has the type Personal and one that has the type Business.
4. Go back to Accounts and expand the Business account, then click Profile.
5. Change the password and make a note of it.
6. Repeat steps 4 and 5 for the Personal account.

Use the following guidelines to create a Merchant account:

1. Registration for use of the PayPal authentication API is at <https://PayPal.com/>.
2. Go to **My Account > Profile** to access your profile configuration.
3. Next, in **Selling Preferences**, select **Website Payment Preferences**.
4. Set **Auto Return** to **On**.
5. Set **Return URL** to <https://<hostname>/billing/PayPal/verify>, where **<hostname>** is the A3.
6. Note the **Identity Token** in the form.
7. Submit the form and note the **Cert ID**.
8. Go back to **My Account > Profile** and select **Encrypted Payment Settings**.
9. Select the A3 public certificate in the **Your Public Certificates** section.
10. **Download** the **PayPal Public Certificate** and put it in the A3 server at </usr/local/A3/conf/ssl/PayPal.pem>.

## Stripe

Registration for use of the Stripe authentication API is located at <https://dashboard.stripe.com>. Use the following guidelines:

1. Click on **Your account** then **Account settings**.
2. Navigate to the API keys tab and note your key and secret. Two sets of keys and secrets are provided for testing and live operation.

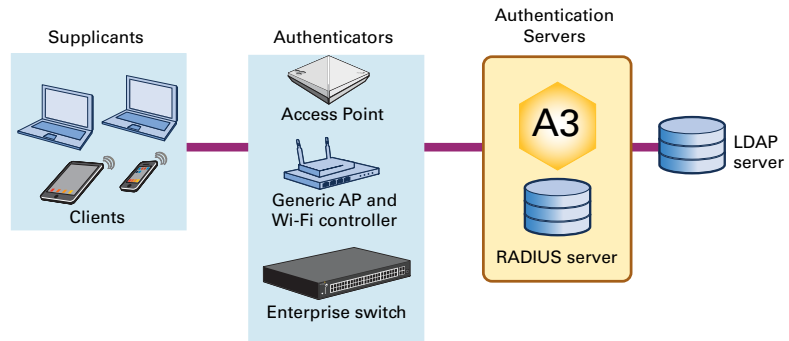
A subscription-based service is available with Stripe. Configure a billing tier for each subscription plan to be made available to the client. Configure a very long Access Duration in this case since Stripe will contact A3 when the subscription has expired. In order to receive subscription expiration or cancellation notices:

1. A3 must be publicly available through a FQDN that resolves to the server. Port 80 must be open.
2. In Stripe, configure a Webhook that Stripe will use to inform A3 of events. Go to **Your Account > Account Settings > Webhooks** and click **Add endpoint**.
3. Enter the URL as <http://<hostname>/hook/billing/stripe>, where **<hostname>** should be the A3's CWP.
4. **Mode** can be set for testing or live mode.

## 802.1X

RBAC (Role-based Access Control) authenticates users and their devices with information provided by device-resident supplicant software. This information is matched against internal databases such as AD. 802.1X protocols define the way in which the components talk to each other. A variety of encryption techniques are used to ensure the security of 802.1X protocol messages, including the EAP (Extensible Access Protocol). EAP variants are covered in [EAP and X.509 Certificates](#). EAP requires X.509 digital certificates, which are covered in [Certificates and PKI](#).

The figure below illustrates the components involved in RBAC.



## Supplicants

Supplicants are client devices that seek access to the network. They run device-resident supplicant software that supplies credential information to the authentication server.

Some common credentials include:

- User name and password
- MAC address
- Digital certificates
- Dynamic and one-time passwords
- Smart cards or credentials stored on USB devices
- Machine credentials
- Pre-shared keys

One or more credentials may be required by the authenticator. Supplicants can be integrated with the client OS, or supplied by third parties. Installing and configuring supplicants can be a time-consuming and complex task. You can automate this and other configuration tasks using automation and MDM (mobile device managers), which are described in [Provisioning](#).

## Authenticator

An authenticator is a device that blocks or allows traffic to pass through its ports. Many types of devices can serve as authenticators:

- **Extreme Networks access points:** APs provide both wireless access and authentication.



- **Generic APs:** APs may require the use of a separate Wi-Fi controller that performs authentication in addition to AP control.
- **Enterprise switches:** An advanced wired network switch can also be an authenticator.

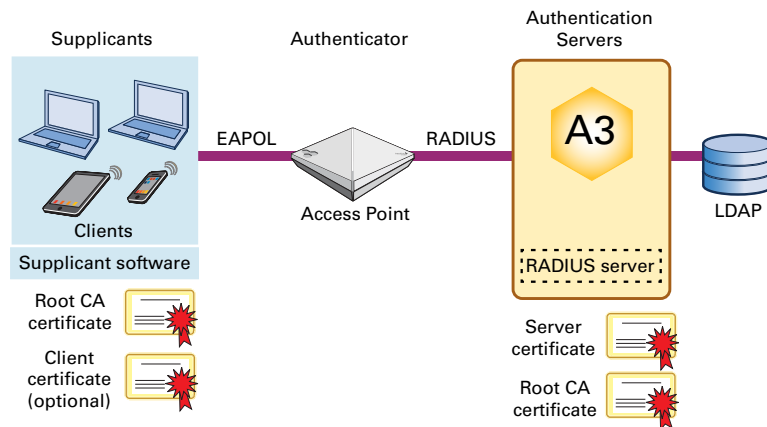
## Authentication Servers

Depending on the type of authentication you use, a number of servers may be involved. At a minimum they include:

- **A3:** the A3 server acts as a proxy for access to the other authentication servers. It matches information returned from these servers for extensive control over access control. A3 uses a built-in RADIUS server.
- **RADIUS Server:** RADIUS is the key protocol used for authentication. The RADIUS server may contain its own database of users and roles, and works with additional authentication servers. A3 uses a built-in FreeRADIUS server.
- **LDAP Server:** LDAP (lightweight directory access protocol) is used to access databases that contain user, machine, roles, and other information organized in multiple hierarchies. Microsoft's AD and OpenLDAP are two of a number of LDAP servers in common use.

## EAP and X.509 Certificates

EAP is an authentication framework that facilitates secure communications between clients and authentication servers. The figure below is a simplified network diagram featuring Extreme Networks components.



An access point serves as the Authenticator. Messages from clients to the AP are sent using the EAPoL (EAP over LAN) protocol. They are then encapsulated in RADIUS messages and sent to A3.

Most EAP methods use X.509 digital certificates to ensure identity and to set up encryption. Three possible certificates are required:

- **Server Certificate:** uniquely identifies the RADIUS server as an authorized part of an entity. Server certificates also provide the public key used to encrypt communications with the authentication server. Clients request this certificate as part of an EAP exchange to ensure that they are talking to the correct server. The server certificate is signed by a Root CA (Certificate Authority), described below.
- **Root CA Certificate:** identifies the authority that generates certificates. Clients and others use these certificates to further validate server certificates. Root CA certificates must be pre-loaded into clients. Most client operating systems contain an extensive list of Root CA certificates in their certificate store that have been validated by the OS vendor. Enterprises may choose to be their own certificate provider, in which case they must generate their own Root CA certificate and arrange to download it to clients. Windows environments that use AD can accomplish this using the GPO (Group Policy Object). Provisioners (see [Provisioning](#)) may also be used to download Root CA certificates to users.
- **Client Certificate:** Identifies individual clients. Certificate data is used in lieu of other credentials that the client might have. When a client certificate is used, the server must have the corresponding Root CA certificate.

X.509 certificates are generated and maintained as part of a Public Key Infrastructure (PKI), which is covered in [Certificates and PKI](#).

## EAP Methods

The EAP framework makes possible a number of methods for the secure exchange of identity. The client dictates which EAP methods are acceptable. The client and server negotiate which of the acceptable methods they have in common will be used. The EAP methods that are available in A3 are shown below. You can select more supported methods using the administrative interface.

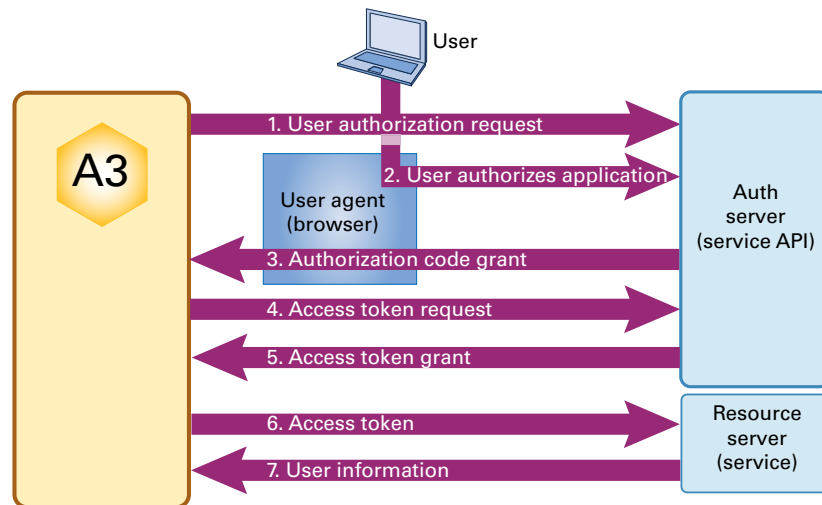
- **EAP-TLS:** this is one of the most common method used, and requires client certificates. TLS (transport layer security) is the same protocol used for secure web pages, although client certificates are not required in most TLS cases. The client and server perform mutual authentication and form encryption keys based on certificate contents.
- **PEAP:** the PEAP (protected extensible authentication protocol) encapsulates EAP within a potentially encrypted and authenticated TLS tunnel. Any of the other methods listed may be used within the tunnel.
- **EAP-TTLS:** the TTL (tunneled transport layer security) protocol extends TLS. The client need not be authenticated initially by the server using a certificate, although the server's certificate is used by the client. Once this occurs a secure tunnel is established for user authentication. User authentication may use any of a number of methods, including legacy credentials or certificates.
- **EAP-GTC:** this technique is used in conjunction with GTC (generic token cards). In this method, the RADIUS server sends a challenge to the security token on the client. The response is sent back and validated by the server.
- **EAP-MD5:** an older technique that uses an MD5 hash to authenticate the client to the RADIUS server, but not vice versa. It is currently deprecated.
- **EAP-FAST:** the FAST (Flexible Authentication via Secure Tunneling) protocol establishes a tunnel without the need for client or server certificates. The tunnel is established using PAC (Protected Access Credentials), either dynamically generated or pre-stored. Once a tunnel is established any of a number of mechanisms can be used, as in EAP-TTLS.

# Social Login Authentication Technology

A3 works with a number of social media web sites using the OAuth2 protocol defined in [RFP 6749 - The OAuth 2.0 Authorization Framework](#).

These social media sites include Facebook, Github, Google, Instagram, Kickbox, LinkedIn, OpenID, Pinterest, Twilio, Twitter, and WindowsLive. To use any of these sites in a web-based authentication, the A3 administrator must register with the OAuth provider to obtain two pieces of information: an API ID that identifies the site or sites, and an API Secret that authenticates the site or sites. During the registration process the administrator provides identification information and a callback URL into A3, which is used at run-time.

The figure below describes the run-time steps associated with social media authentication. The definition of a social media authentication source requires a number of pieces of information that are highlighted in the table below the illustration. These terms, with slight naming variations, are used in the definition of social media authentication sources.



The steps in the process are described in this table:

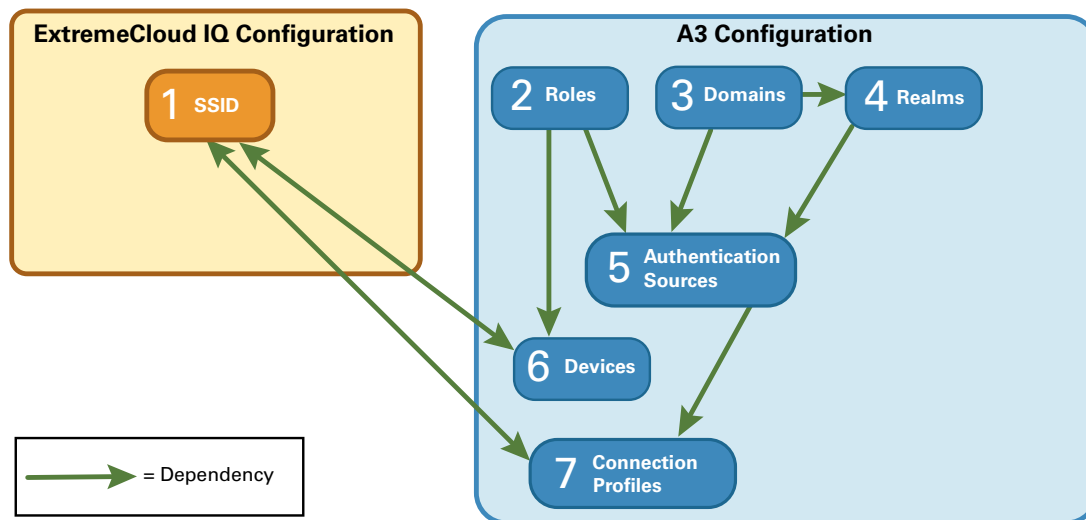
Key	Usage	Example Assignment
1	<b>User Authorization Request.</b> The user chooses a social media authentication from a captive web portal.	<ul style="list-style-type: none"> <li>• <b>API URL:</b> The URL of the social media OAuth2 site.</li> <li>• <b>API Auth Path:</b> A sub-location within the API URL used for authorization.</li> <li>• <b>API ID:</b> The ID of A3 obtained during registration.</li> <li>• <b>Portal URL:</b> The callback URL on the A3 to which to return an authorization.</li> <li>• <b>Scope:</b> A description of the information that A3 will require from the social media database</li> </ul>
2	<b>User Authorizes Application.</b> The user is asked to log in to the social media site, if necessary, and is then asked to grant A3 access to their identification information.	
3	<b>Authorization Code Grant.</b> The social media site responds to the A3 callback URL, providing an authorization code.	<ul style="list-style-type: none"> <li>• <b>Portal URL</b></li> </ul>

Key	Usage	Example Assignment
4	<b>Access Token Request.</b> A3 requests an access token that is used to retrieve the user's information.	<ul style="list-style-type: none"><li>• <b>API URL</b></li><li>• <b>API Token Path:</b> A sub-location within the API URL used for token access</li><li>• <b>API ID</b></li><li>• <b>API Secret:</b> The shared secret that allows A3 to access the social media site.</li></ul>
5	<b>Access Token Grant.</b> The response to the access token request containing the access token.	<b>Access Token Parameter:</b> The label associated with the received access token
6	<b>Access Token.</b> A3 presents the access token along with a request for user information.	
7	<b>User Information.</b> User identification information is returned to A3.	

# A3 Configuration Flow

## Overview

There are seven key elements to a working A3 authentication configuration. The figure below illustrates the general layout and suggested configuration order of ExtremeCloud IQ and A3 elements.



Either five or seven steps are required to configure ExtremeCloud IQ and A3 for authentication. Seven steps are required if AD (Active Directory) lookups are required, and other devices may also need to be configured. Use the following steps:

1. **ExtremeCloud IQ Network Policy:** define the network SSID and the network connections to be made based on A3 role identification.
2. **Roles:** define distinct role names for categorizing users.
3. **Domains:** define A3 domains only when you need AD or LDAP domains to identify users. Domains and domain controllers are identified in this step.
4. **Realms:** define realms to dictate which network regions apply.
5. **Authentication Sources:** define the ways in which users are authenticated and assigned to roles.
6. **Devices:** define the manner in which access points and switches will receive A3 information.
7. **Connection Profiles:** tie ExtremeCloud IQ SSIDs and network policy to authentication sources.

---

## Guest Access Configuration Example

---

This example uses an Extreme Networks AP connected to an A3 server to allow guest access to the internet, but not internal networks. The authentication methods in this example are supported by the captive web portal hosted on the A3 server:

1. Null (no user authentication, presents the user with an Acceptable Use Policy)
2. SMS message
3. Email message

The configured elements are pictured below.

The colors in this illustration correlate configured items. Text on a colored background designates configured items that are used in multiple elements. Black text indicates a setting name.

### ExtremeCloud IQ Configuration

ExtremeCloud IQ is configured in the following manner:

1. **MAC Authentication.** Clients are authorized based on their MAC address.
2. **User Access Settings.** A default user profile is defined that limits access by guests during the registration process using firewall rules. A guest user profile specifies that when the access point receives the **guest** RADIUS attribute from A3 it will connect the client to the internet, but not to any internal networks.

### A3 Configuration

Four elements are required for this guest access scenario:

1. **Roles.** The names of roles that clients will assume, in this case the **A3GuestRole**.
2. **Authentication sources.** The authentication sources used in this example are null, sms, and email. Each source has a set of authentication rules that indicate the conditions under which the authentication succeeds and what actions to perform when it does.

In this example, the client satisfies authentication through the captive web portal; no conditions are set in the authentication source. All sources have the same action: to assign the **A3GuestRole** to the client. The role is used in the **Devices** element.

3. **Devices.** The device configuration ties the roles to the returned RADIUS attribute returned. The IP address of the AP indicates which AP is to be contacted with the role assignment. To map the **A3GuestRole** to the guest RADIUS attribute, select Role by Device Role.
4. **Connection Profile.** The connection profile creates a correspondence between the AP connection profile and the authentication sources that can be used within that profile.

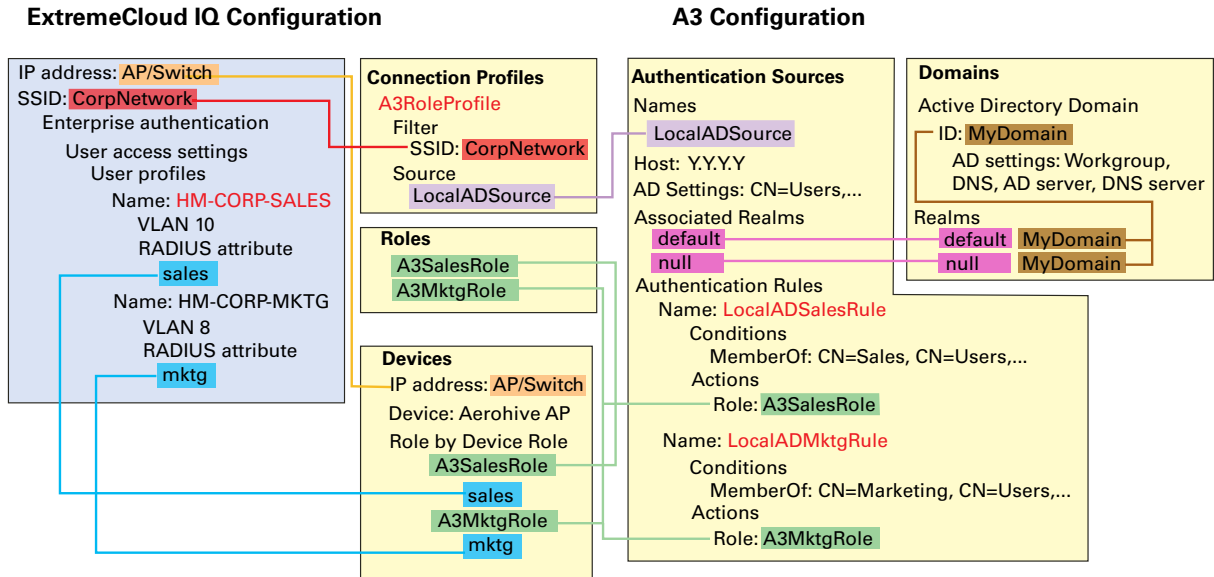
---

## 802.1X Configuration Example

---

This role-based access example uses an AP connected to an A3 server which is in turn connected to an AD server. User credentials are matched against AD entries. Clients whose users are in the **Sales** group are attached to VLAN 10 in the internal network and

those in the **Marketing** group are attached to VLAN 8. The configured elements are pictured below.



The colors in this illustration correlate configured items. Text on a colored background designates configured items that are used in multiple elements. Black text indicates a setting name, and red text indicates an element name that is not used elsewhere.

## ExtremeCloud IQ Configuration

Configure the following AP-related items for this example:

1. **Enterprise Authentication.** Clients are authorized utilizing 802.1X with EAP. Certificates and shared secrets have been omitted from this example.
2. **User Access Settings.** These settings specify that when the AP receives the **sales** RADIUS attribute from A3, it connects the client to VLAN 10. Similarly, the **mktg** attribute is mapped to VLAN 8.

## A3 Configuration

Configure the following five elements for this user access example:

1. **Roles.** Define the role names that clients will assume, in this case **A3SalesRole** and **A3MktgRole**.
2. **Domain.** Define an AD domain named **MyDomain**. Map two realms (**null** and **default**) to this domain.
3. **Authentication Source.** Configure a single, local AD source named **LocalADSource**. This source is associated with the Local AD server through associated realms. Configure two authentication rules to locate the client's credentials in the **CN=Sales** or **CN=Marketing** section of the **CN=Users** tree in AD. In both cases, the action associated with the authentication rules assigns the **A3SalesRole** and **A3MktgRole**, respectively.

4. **Devices.** Configure devices to tie the roles to the RADIUS attribute returned to each device, based on the IP address of each device. Select **Role by Device Role** to map the **A3SalesRole** to the **sales** RADIUS attribute and the **A3MktgRole** to the **mktg** attribute.
5. **Connection Profile.** Configure a connection profile to create a correspondence between the AP SSID and connection profile and the authentication sources that can be used within that profile.



# Certificates and PKI

## Overview

---

Certificates are blocks of data used as part of a network communications technique that ensures authentication and encryption of data. Certificates are issued and signed by CAs (certificate authorities). A list of well-known and trusted CAs is often included in operating system releases. The list below, for example, is from a Windows 10 system:

- |  |  |
|--|--|
|  AddTrust External CA Root                      |  Hotspot 2.0 Trust Root CA - 03                                 |
|  Baltimore CyberTrust Root                      |  Microsoft Authenticode(tm) Root Authority                      |
|  Certification Authority of WoSign              |  Microsoft ECC Product Root Certificate Authority 2018          |
|  Certum CA                                      |  Microsoft Intune Root Certification Authority                  |
|  Certum Trusted Network CA                      |  Microsoft Root Authority                                       |
|  Class 3 Public Primary Certification Authority |  Microsoft Root Certificate Authority                           |
|  COMODO RSA Certification Authority             |  Microsoft Root Certificate Authority 2010                      |
|  Copyright (c) 1997 Microsoft Corp.             |  Microsoft Root Certificate Authority 2011                      |
|  DigiCert Assured ID Root CA                   |  NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.                   |
|  DigiCert Global Root CA                      |  QuoVadis Root CA 2   |
|  DigiCert Global Root G2                      |  QuoVadis Root Certification Authority                        |
|  DigiCert Global Root G3                      |  SecureTrust CA   |
|  DigiCert High Assurance EV Root CA           |  Starfield Class 2 Certification Authority                    |
|  DST Root CA X3                               |  Starfield Root Certificate Authority - G2                    |
|  Entrust Root Certification Authority         |  Starfield Services Root Certificate Authority                |
|  Entrust Root Certification Authority - G2    |  Symantec Enterprise Mobile Root for Microsoft                |
|  Entrust.net Certification Authority (2048)   |  Thawte Premium Server CA                                     |
|  Equifax Secure Certificate Authority         |  thawte Primary Root CA                                       |
|  GeoTrust Global CA                           |  Thawte Timestamping CA                                       |
|  GlobalSign                                   |  USERTrust RSA Certification Authority                        |
|  GlobalSign                                   |  UTN-USERFirst-Object   |
|  GlobalSign Root CA                           |  VeriSign Class 3 Public Primary Certification Authority - G5 |
|  Go Daddy Class 2 Certification Authority     |  VeriSign Commercial Software Publishers CA                   |
|  Go Daddy Root Certificate Authority - G2     |  VeriSign Universal Root Certification Authority              |

Other CAs can be created that are trusted by these CAs, or other CAs. A chain of trust can be established as CAs trust other CAs, called a certificate chain. On the other end of the scale, a self-signed CA can be created. A3's initial configuration generates a self-signed certificate for use with encrypted web traffic.

SSL (secure socket layer) is a technique that authenticates and encrypts HTTPS traffic between clients and web servers, including A3's administrative interface. The server sends its certificate to clients as part of the initial connection. As noted earlier, most modern browsers object to A3's use of a self-signed certificate. This can be overridden by the client, but best practice calls for installation of a certificate from a well-known CA.

## Public and Private Keys

Public and private keys are associated with certificates. Keys are blocks of data, usually 2048 bits or longer in length. They can be generated by CAs, and are always generated in pairs. The intent is that private keys are kept on the client machine in a secure repository, while public keys are attached to certificates.

The public and private keys are interrelated such that data encrypted with a public key can only be unencrypted with the corresponding private key, and vice versa. Using certificates and public/private keys, two parties can establish encrypted communication and authenticate the identity of the party that they are talking to.

Only the server is authenticated in most HTTPS communications although mutual authentication is possible.

Public/private key encryption is a compute-intensive operation and is normally not used for bulk encryption of data. Instead, the initial connection between parties is used to establish a single symmetric key used by both parties for bulk encryption. The symmetric key is changed frequently during a session.

## Public Key Infrastructure

Certificates need to be:

- Issued
- Re-issued upon expiration
- Revoked upon request
- Validated

The facilities that perform these functions are called the PKI (public key infrastructure).

PKI providers offer facilities for:

- **Issuing certificates.** Clients format their own certificates and submit request to PKI providers to sign the certificates. Signing is the process by which the provider encrypts a digest of the certificate with their private key. Their signature can be validated against the public key included in their own certificate. Signed certificates are returned to their clients via download. Certificates are installed by operating system specific software.
- **Re-issuing certificates.** Every certificate has an expiration date. Providers often monitor these expirations, sending out warnings to their owners when the expiration time is near. Providers generate new certificates with new expiration dates for installation on systems.
- **Revoking certificates.** An organization can revoke the certificates of its members, if necessary. The revocation is usually accomplished by adding the certificate to a revocation list that can be distributed or requested. Timely distribution can be problematic for large CA trust chains.
- **Validated.** An alternative to distribution of revocation lists is the use of on-demand validation of certificates. Clients wishing to check the validity of a certificate can request an immediate validation from the certificate issuer. This too can be problematic in heavy usage scenarios.

A3 provides the means of designating one or more PKI providers.

# A3 Certificate Usage

*It is a very good idea to do this before creating a cluster. A restart is required after certificates are installed in order to make them effective.*

A3 uses two types of certificates:

- **SSL/HTTPS certificate.** This type of certificate is issued for the A3 host and offered to clients connecting to its web services: A3 administration, client registration, and A3 sponsor approval.
- **RADIUS certificate.** This certificate is used for communications between clients, access points, and A3s that use the RADIUS protocol. Certificates are used by the PEAP and EAP-TLS authentication protocols. A server certificate is always present on the A3 server; client certificates may be placed on individual hosts to facilitate authentication.

## SSL Certificate

A3 provides two facilities for signing and installation of a certificate for SSL communications:

- **Let's Encrypt.** Let's Encrypt is a cost-free facility for certificate signing. A3's UI automatically requests the signing and installs the certificate. This form of certificate installation is demonstrated below.
- **Certificate Authority** - an organization can host its own certificate server or use one of a number of commercial certificate authorities. A multi-step procedure is used to obtain and install a certificate:
  - a. Use the A3 interface to Generate a Signing Request. This involves filling out a form with identifying information. The result is a block of text that is a request for a signed certificate.
  - b. Copy the block to the clipboard and then paste it into the appropriate place on the certificate authority's web site to request the certificate.
  - c. The certificate authority will send the requested certificate that is download to the client machine.
  - d. The A3 UI is used to install the certificates. Although a new certificate may be installed, the UI may not reflect the new certificate until the next A3 reboot.

This form of certificate installation is not illustrated in this guide.

### Let's Encrypt

There are several prerequisites for the use of Let's Encrypt:

- The value of A3's common name (e.g. a3.company.com) must resolve to a publicly accessible address that is mapped to the VIP address of the cluster (B).
- The A3 server must be publicly accessible at that host name.
- The HTTP protocol (port 80) must be enabled to the A3 server via firewall rules.<sup>1</sup>

Note that this configuration leaves the A3 server accessible from the internet. Controlling or limiting such access may enhance the security of the A3 system.

The certificates issued by Let's Encrypt have an expiration of 60 days. A warning will be issued 30 days before expiration as long as the prerequisites listed above remain in effect.

1. During sponsored authentication, the FQDN of the A3 server is sent to the sponsor for use in authorizing a client. Port 443 is used for this connection and must be accessible internally and/or externally as well. This might be a good time to enable that access.

Use the following steps to obtain a Let's Encrypt certificate:

1. Navigate to Configuration > System Configuration > SSL Certificates.
2. Select .
3. Select the **HTTPS** tab.
4. Ensure that **Use Let's Encrypt** is enabled.
5. Enter the externally accessible FQDN of the A3 VIP (A3-Main(c).example.com(d)) in the Common Name field. Remember, (c) and (d) are just references back to the [Table of Addresses and VLANs](#); they are not entered into the form.
6. Click . If the prerequisites have not been properly implemented a **Request failed with status code 422** message will be displayed.; the 422 code is used for all problems. Troubleshooting for this problem involves testing for port 80 access to A3 on port 80 via its FQDN address mapped to its VIP address (B).
7. If the test succeeded, a **Success validating domain** message will be displayed.

<sup>(1)</sup> *Services must be individually restarted on each member of a cluster. Restarting services will disable authentication for a period of time.*

8. Select the  button. A3 takes care of all additional steps: a signing request is submitted, Let's Encrypt signs the certificate, the certificate is downloaded, and installed on A3.
9. Restart the **radiusd** service on the **Status > Services** page.

## RADIUS Certificate

RADIUS certificates are most often handled internally within an organization due to the possibility of a man-in-the-middle attack. A3 will operate with any CA that supports SCEP (simple certificate enrollment protocol).

The MS AD CS (Microsoft Active Directory Certificate Service) supports SCEP through an NDES (Network Device Enrollment Service) add-on module. This section of the guide outlines the elements needed to integrate MS AD Certificate Service with A3.

The MS CS requires:

- A Microsoft Windows 2008 R2 Enterprise server or later on which the certificate service is installed as an Enterprise Certificate Authority.
- A local DNS service that provides an A-record for the MS AD CS server.
- An AD CS Role with the following add-on role services:
  - Certificate Authority as an Enterprise CA

- Certificate Authority Web Enrollment with all required features.
- Online Responder with all required features
- Network Device Enrollment Service

The following steps can be used to setup A3 for use with an MS AD CS for EAP-TLS authentication.

1. Navigate to System Configuration > SSL Certificates > RADIUS.
2. Select **Generate Signing Request (CSR)**.
3. Enter appropriate values for your organization:

Field	Usage	Example
2-Letter Country Code	A two letter country code for your location. Country codes are defined <a href="#">here</a> .	US
State	State for US and Canadian entities. Do not use abbreviations	California
Locality	The city in which the organization is located. Do not use abbreviations. International entities must enter either a City/Locality or a State/Province field.	Anywhere
Organization Name	The Organization's name, as registered with a government agency. Do not abbreviate or use any of these symbols: ! @ # \$ % ^ * ( ) ~ ? > < / \.	Widgets Plus, Inc.
Common Name	The FQDN used for DNS lookups for your server. This may a network-local name for use internally.	A3-Main.example.com

Generate Signing Request for RADIUS certificate ✕

---

2-Letter Country Code

State

Locality

Organization Name

Common Name

---

4. Select **Generate**. The text of the signing request is displayed.
5. Select **copy to clipboard** to copy the signing request.
6. The certificate is generated by direct interaction with the CA.
  - a. In a web browser, enter the address of your CA. For example: [http://10.150.1.5\(G\)/CertSrv](http://10.150.1.5(G)/CertSrv).

- b. Log in with your administrator credentials for the certificate server.

Sign in  
 http://10.150.1.5  
 Your connection to this site is not private

Username

Password

- c. Select [Request a certificate](#).

#### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

#### Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

- d. Select [advanced certificate request](#).

#### Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

- e. Paste the previously copied CSR from the clipboard, select Web Server from the list of Certificate Templates, and press **Submit>**.

#### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

#### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
acRE+9QAUWu1pkfMWAxucYbvk9rirIKmCV3/QC
1rs0q015cP8HOE3yf+/LcEZeBsIc1Ut0hAG3Hx
V85/0vrIiv9kcHLaw2WghPtxZY3zLXrZ5vxNtq
eAMBSQ==
-----END CERTIFICATE REQUEST-----
```

#### Certificate Template:

#### Additional Attributes:

Attributes:

- f. Choose Base 64 encoded and select [Download certificate](#).

**Certificate Issued**

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

[Download certificate](#)  
[Download certificate chain](#)

- h. Find the downloaded file in your operating system and rename it to **a3-cert.pem**.
7. The MS CA is also used to install the certificate for the CA itself. Continuing from the previous step:

- a. Select **Home** from the upper-right of the screen and then [Download a CA certificate](#).

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

[Request a certificate](#)  
[View the status of a pending certificate request](#)  
[Download a CA certificate, certificate chain, or CRL](#)

- b. Choose Base 64 encoding method and select [Download CA certificate](#).

**Download a CA Certificate, Certificate Chain, or CRL**

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [Install CA Certificate](#)

Encoding method:

DER  
 Base 64

[Install CA certificate](#)  
[Download CA certificate](#)  
[Download CA certificate chain](#)  
[Download latest base CRL](#)  
[Download latest delta CRL](#)

- c. Find the downloaded file in your operating system and rename it to **ca-cert.pem**.


8. These two certificates (a3-cert.pem and ca-cert.pem) are both needed for EAP-TLS.
9. Navigate to Configuration > System Configuration > SSL Certificates > RADIUS.
10. Select **Edit**.
11. Select **Choose Certificate** and select **a3-cert.pem** from the list of downloaded files.
12. Select **Choose Certificate Authority** and select ca-cert.pem from the list of downloaded files.

**(i)** *Services must be individually restarted on each member of a cluster. Restarting services will disable authentication for a period of time.*

13. Select .
14. Restart all A3 services by navigating to Status > Services and selecting .

## PKI Provider

A PKI provider must be defined to interface with the MS AD CA.

1. Navigate to Configuration > Advanced Access Configuration > PKI Providers.
2. Select  > SCEP PKI.
3. Fill in the form as suggested below.


Field	Usage	Example
PKI Provider Name	A name for the provider	MSPKI
URL	The URL for the SCEP service for the PKI Provider. The URL must end in a forward slash.	http://10.150.1.5(G)/CertSrv/mscep/
CA Certificate	The path to the CA certificate to be used to generate client certificate and key combinations.	/usr/local/A3/radddb/certs/01.pen
Server Certificate	The path to the RADIUS server authentication certificate.	/usr/local/A3/radddb/certs/01.pen

4. Select .

## Provisioner

Provisioning plays an important part in the proper configuration of clients. Provisioners are executed as part of the Connection Profiles operation as a result of a successful authentication. Provisioners deliver configuration information to clients or verify a device's management status with third-party MDM solutions. On-device agents deliver wireless network settings to client devices. For iOS-based Apple devices, the required functions are built-in. A3 includes agents for Android- and Windows-based devices.

The following steps define a provisioner for Windows clients connected through the A3-Guest and A3-Corp (a) SSIDs.

1. Navigate to Configuration > Advanced Access Configuration > Provisioners.
2. Select  and then Windows.
3. Fill in the form as suggested below.

Field	Usage	Example
Provisioning ID	An ID for the provisioner	EAP-TLS
Description	An description of the provisioner's scope.	Provisioner for EAP-TLS on Windows systems
Roles	The list of roles that the provisioner will apply to.	Sales, Marketing
SSID	The SSID that will invoke the usage of the provisioner.	A3-Corp (a)
Security Type	The type of security to be used for the SSID.	WPA2



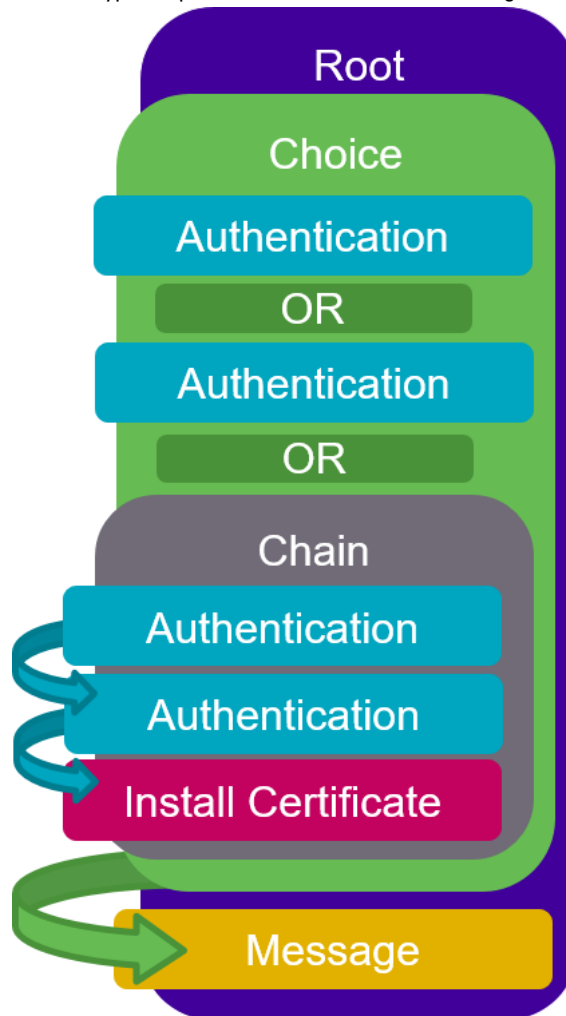
Field	Usage	Example
EAP Type	The EAP type to be used with the SSID. This should be left blank for no EAP. Note that this field will not appear until Security Type is set to WPA2.	EAP-TLS
PKI Provider	The name of the PKI provider to be used by the provisioner.	MSPKI

4. Select [Create](#).

# Portal Modules

A3's CWP (captive web portal) is used to authenticate users and their devices to the network through a set of web pages. The captive web portal may be customized for each Connection Profile.

There are two principal locations where the captive web portal is specified: in Configuration > Policies and Access Control > Connection Profiles and in Configuration > Advanced Access Configuration > Portal Modules. The relationships between the different types of portal modules are shown in the figure below:



## Connection Profile Settings

Two particular settings are significant:

- **Root Portal Module:** the name of a root module in the Portal Module configuration. This refers to the top of the tree for the Connection Profiles.
- **Logo:** the name of the file in the file system where the organization's logo is found. The logo file is displayed at the top of most authentication pages. The file containing the logo is defined in Configuration > Policies and Access Control > Connection Profile > profile name. In the Captive Portal tab, the first entry (Logo) defines where the file is downloaded from. There are two choices for specification of this file:
  - Use an external web server. For example, if example.com has a web server, then [https://www.example.com/my\\_image.jpg](https://www.example.com/my_image.jpg) could be used to host the image. The URL must be available on the internal network. If it is hosted external to the site the domain (example.com in this example) must be included in Passthrough and Isolation Passthrough Domains in Configuration > Network Configuration > Fencing.
  - Upload the files to the A3 servers. This operation requires root access to each of the A3 servers. Contact Extreme Networks support to perform this operation. The file must be uploaded to each server in an A3 cluster.

## Type of Portal Modules

Several type of portal modules can be used to build a portal. Each module can have one or more actions that set client roles, access duration, and bandwidth limits.

- **Root.** Defines the basic portal sequence. The modules listed in this type of module operate in a chained manner - each in the order defined. For example, the default root module shipped with A3 includes three other portal modules, executed in a chain:

Portal Module default\_policy **Root**

Name: default\_policy

Description: Default portal policy  
The description shown to users.

Modules	1	2	3
	default_registration_policy	default_show_local_account	default_provisioning_policy

Save Reset Clone

- **default\_registration\_policy** - a list of possible authentication mechanisms, which will be covered in **Choice**, below.
- **default\_show\_local\_account** - a module intended to display a local account if one was specified in an authentication source used for registration. The operation(s) performed are defined in Actions associated with the module. In the default case, there are no Actions defined, so this is just a place holder.

- **default\_provisioning\_policy** - a module intended to provide provisioning actions for clients. The operation(s) performed are defined in Actions associated with the module. In the default case, there are no Actions defined, so this is just a place holder.
- **Choice.** Allows clients to choose between selected chained, authentication, and provisioning modules. The order of modules in the list dictates the order of the modules as presented to clients. For example, the default registration policy shipped with A3 includes authentication modules for most types of authentication available in A3. Each choice is only offered if there is an applicable Source defined in the Connection Profile, or the module specifies Authentication Sources.
- **Chained.** Specifies a list of modules, all of which must be executed in the order specified to complete authentication.
- **Authentication.** Several authentication types are available. New modules may be defined to override required fields, sources, templates, or other modules. The available types include those listed above in addition to those described in [Source by Options](#).

All authentication modules have a **Mandatory Fields** and **Fields to Save** option. The values entered by clients during registration are available to the [Templates](#) used in information display.

- **Choice:** a set of authentication sources. This type has the same name as Choice listed above, but is different in content. It is referred to as Authentication::Choice in the following discussions.
- **External:** email, null, SMS, sponsor, and OAuth2 sources.
- **Internal:** Login, which covers user name/password-based authentication from multiple internal sources, including Active Directory and LDAP.
- **Password:** requires a user password.
- **Billing:** one or more billing sources.
- **Blackhole:** causes authentication to fail.
- **SAML:** performs SAML-based authentication.
- **Provisioning.** Triggers provisioning to occur as specified in the Connection Profile.
- **Message.** Displays a message to the client being registered.
- **URL.** This module redirects a client to a local or external URL. This feature is currently not supported in A3.
- **Fixed Role.** Performs one or more actions for a filtered set of roles.
- **Select Role.** Used to define a module that overrides the role matched when a device is registered. For example, an administrator can directly set a device's role, bypassing authentication rules.

## Source by Options

<sup>(1)</sup> *When using any of the Source by options, the order and number of options should match those in the Connection Profile's Authentication Sources section.*



Finer control over authentication sources is available by using the **Source by** options in the Authentication::Choice module.


- **Source by Class.** One or more specifications of the form pf::Authentication::Source::<name> can be used in a Choice module. The <name> component may be any of the authentication sources defined in Configuration > Policies and Access Control > Authentication Sources or one of the predefined classes. In some cases a class may only contain one authentication type:

- **Internal sources:** ADSource, EAPTLSSource, HtpasswordSource, HTTPSource, LDAPSource, PotdSource, RADIUSSource, and SAMLSource
- **External sources:** EmailSource, NullSource, SMSSource, and SponsorEmailSource
- **Social login sources:** OAuthSource (all of the following), FacebookSource, GithubSource, GoogleSource, InstagramSource, KerberosSource, KickboxSource, LinkedInSource, OpenIDSource, PinterestSource, TwilioSource, TwitterSource, WindowsLiveSource
- **Authorization sources:** AuthorizationSource
- **Billing sources:** BillingSource (all of the following), AuthorizeNet, ClickatellSource, AuthorizeNetSource, MirapaySource, PaypalSource, and StripeSource
- **Exclusive sources:** AdminProxySource, BlackholeSource, and EduroamSource
- **Source by Type.** One or more type names, indicating individual authentication methods:
  - **Internal sources:** AD, EAPTLS, Htpassword, HTTP, LDAP, Potd, RADIUS, and SAML
  - **External sources:** Email, Null, SMS, and SponsorEmail
  - **Social login sources:** OAuth (all of the following), Facebook, Github, Google, Instagram, Kerberos, Kickbox, LinkedIn, OpenID, Pinterest, Twilio, Twitter, WindowsLive
  - **Authorization sources:** Authorization
  - **Billing sources:** Billing (all of the following): AuthorizeNet, Clickatell, AuthorizeNet, Mirapay, Paypal, and Stripe
  - **Exclusive sources:** AdminProxy, Blackhole, and Eduroam
- **Source by Authentication Class.** One or more class names, as used in Configuration > Policies and Access Control > Authentication Sources:
  - **internal**
  - **external**
  - **billing**
  - **exclusive**

## Templates

Templates are HTML files that used throughout the portal modules to display static and dynamic information. In general, the supplied templates are used as shown in the default portal modules. Templates, however, may be previewed and edited in the Files tab of Configuration > Policies and Access Control > Connection Profile.

The  button will show the template contents, without any dynamic data such as authentication choices. The  button at the top of the page shows a preview for the Root Portal Module and Authentication Sources associated with the Connection Profile.

Any template can be edited by selecting its name in the Files directory. Modifications create separate copies of the files that are used only for that Connection Profiles. Be very careful editing these files; they are often used in multiple contexts. Variables entered and saved as part of an Authentication portal module may be used via the  button. Place the cursor where the variable reference should go and then press the insert variable button to select the variable.

*Any file modifications will be lost during an A3 upgrade.*

As a side note, the authentication type shown to a registering client is dictated by the **Description** field for the portal module. For example, the Description field for the **null** portal module is initially configured as **Null Source**. A more user friendly setting might be **Free Wi-Fi**.

## Example 1: Reorder Choices

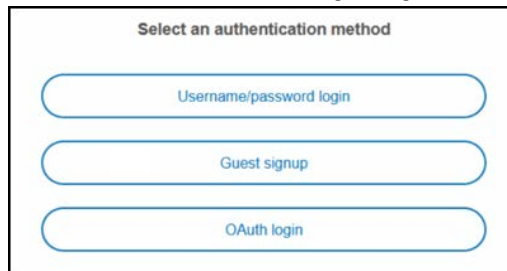
The default portal modules display authentication choices in the following order:

- Login - user name and password logins
- Guest - email, SMS, sponsored email, null
- OAuth - all social logins
- Billing
- SAML
- Blackhole

For example, a particular connection profile may use:

- Guest: null and email
- OAuth: Google
- User name and password

In that case, a client authenticating through A3 is offered choices in the following order.



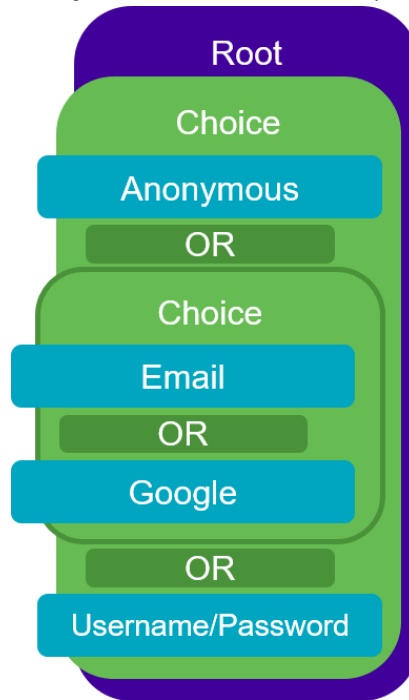
The screenshot shows a box titled "Select an authentication method" containing three buttons stacked vertically: "Username/password login", "Guest signup", and "OAuth login".

This ordering is somewhat unintuitive. A more useful ordering is shown below.



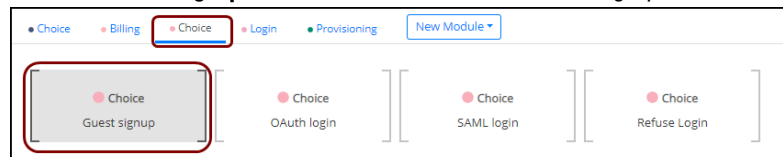
The screenshot shows a box titled "Select an authentication method" containing three buttons stacked vertically: "Anonymous Login", "Register", and "Already Have A Password?".

The organization of modules to accomplish this can be envisioned as below.

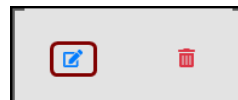


Use the following steps to accomplish the desired layout.

1. Defining portal modules from the bottom up, first define a new **Anonymous** authentication choice module by cloning the **default\_guest\_policy**:
  - a. Select Configuration > Advanced Access Configuration > Portal Modules.
  - b. Select the **Guest signup** module from the (second) **Choice** category.



- c. When selected, the module changes to a graphic that offers the ability to edit or delete the entry. Select the edit icon as shown below.



- d. The definition of the **default\_guest\_policy** is shown. Select **Clone** to copy the entry.
- e. Make the following changes to the definition:

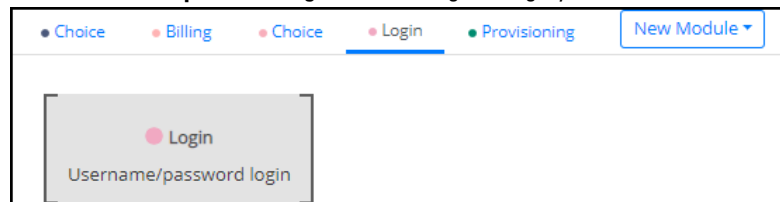
*The authentication type shown to a registering client is dictated by the Description field for the portal module.*

Field	Usage	Setting
Name	Name of the module	Anonymous
Description	Further description	Anonymous Registration
Sources by Class	A list of possible sources, by class. See <a href="#">Source by Options</a> for a list.	pf::Authenticat- ion::Source::NullSource

- f. Select [Create](#).
- 2. Create a **Register** module by cloning the **Anonymous** module, with the following changes:

Field	Usage	Setting
Name	Name of the module	Register
Description	Further description	Register for Access
Sources by Class	A list of possible sources, by class, used in the order specified. See <a href="#">Source by Options</a> for a list.	pf::Authentication::Source::EmailSource pf::Authentication::Source::OAuthSource pf::Authentication::Source::SponsorEmailSource

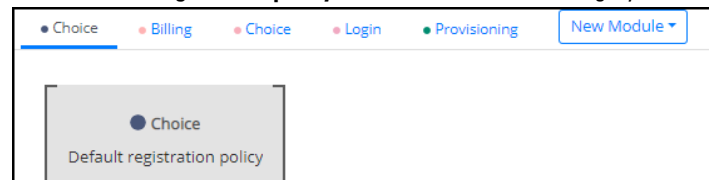
- 3. Create new login portal module by cloning the **default\_login\_policy**.
  - a. Select **Username/password login** from the Login category.



- b. Select the edit icon and then clone the entry.
- c. Make the following changes to the entry:

Field	Usage	Setting
Name	Name of the module	HaveAccount
Description	Further description	Already have a password?
Authentication Sources	Any of the defined authentication sources in A3.	local (As defined in <a href="#">Use Case 3: Local User Authentication</a> )

- d. Select [Create](#).
- 4. Create a new top Choice module by cloning the **default\_registration\_policy**.
  - a. Select **Default registration policy** from the (first) Choice category.



- b. Select the edit icon and then clone the entry.
- c. Make the following changes to the entry:

Field	Usage	Setting
Name	Name of the module	GuestRegistration
Description	Further description	Guest Registration Policy
Template	The template used to display the options.	content-with-choice.html
Modules	The modules to use, in order. This order dictates the order shown in the CWP.	Anonymous Register HaveAccount



- d. Select [Create](#).
- 5. Create a new Root module to tie to the Connection Profile.
  - a. Select [New Root Module](#).
  - b. Fill in the page with the following contents:

Field	Usage	Setting
Name	Name of the module	GuestRoot
Description	Further description	Guest Root
Modules	The modules to use, in order.	GuestRegistration

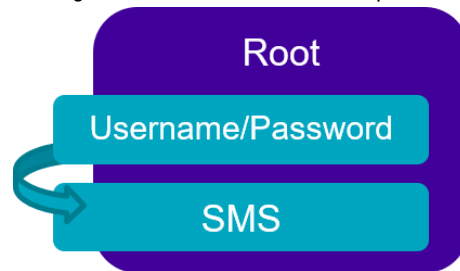
- c. Select [Create](#).
- 6. Navigate to Configuration > Policies and Access Control > Connection Profiles.
- 7. Select the **Guest\_Profile** profile from the list.
- 8. Modify the **Root Portal** Module setting to **Guest Root**.
- 9. Select [Preview](#) to preview the CWP display. Verify the desired ordering as discussed at the beginning of this example.

## Example 2: Two Factor Authentication

Authenticating by a sequence of two methods is a common means for ensuring security in an organization. In this example, the two methods are:

- User name and password
- SMS text message

The organization of modules to accomplish this can be envisioned as:



Use the following steps to accomplish the desired layout.

- 1. Navigate to Configuration > Advanced Access Configuration > Portal Modules.
- 2. Create a new SMS Portal Module by selecting [New Module](#) and then **SMS** from the list.
  - a. Fill in the module’s definition as below:

Field	Usage	Setting
Name	Name of the module	SMS_Module
Description	Further description	SMS Module
Require AUP	Indicates whether the Acceptable Use Policy will be displayed.	Off

- b. Select [Create](#).

## 3. Create a new Root module to tie to the Connection Profile.

- a. Select [New Root Module](#).
- b. Fill in the page with the following contents:

Field	Usage	Setting
Name	Name of the module	Custom_Root
Description	Further description	Custom Root Module
Modules	The modules to use, in order.	default_login_policy SMS_Module

- c. Select [Create](#).

**1** *The default login policy checks all configured databases (local/LDAP).*

4. Navigate to Configuration > Policies and Access Control > Connection Profiles.
5. Select the **Guest\_Profile** module from the list.
6. Modify the **Root Portal** module setting to **Custom Root Module**.
7. Test as in [Use Case 1: Guest Access with Captive Web Portal](#) to verify a two stage verification.

# Security Events and Scan Engines

<sup>(1)</sup> *In pre-V3.0 versions of A3 security events were known as violations.*

Security events are configured by accessing Configuration > Compliance > Security Events. Security events can detect and handle a wide variety of normal and abnormal conditions. For example:

- Condition detected by a scanning engine, such as Nessus or OpenVAS
- Access by particular types of devices or applications, based on:
  - MAC vendor
  - OS versions
  - Browser type
  - Peer-to-peer connections
- Exceeded limits:
  - Bandwidth
  - Connection time
- Unusual device operations:
  - Rogue DHCP message
  - Change of host name
  - Change of transport method
- Need for provisioning

Security events can be handled using a variety of actions, including:

- Automatic client registration with role
- Isolate client
- Email administrator and/or client's owner

Isolated clients can receive event-specific messages explaining the event and suggesting remediation.

## Fingerbank

---

Fingerbank performs device profiling or fingerprinting using the Fingerbank system. It accurately identifies endpoints on your network including type, operating system, and class. Fingerbank updates are downloaded automatically. Local device definitions are also supported. Fingerbank tables are found at Configuration > Compliance.

A3's integration with Fingerbank offers the following features and databases that are used to identify clients or their improper behavior:

- **Devices** - a tree of known device types organized by type
- **DHCP Fingerprints** - known combinations of DHCP options used by clients

- **DHCP Vendors** - DHCP software vendors and versions
- **DHCPv6 Fingerprints** - known combinations of DHCPv6 options used by clients
- **DHCPv6 Enterprises** - known DHCPv6 enterprises (like DHCP vendors)
- **MAC Vendors** - known MAC vendors, by OUI (organizationally unique identifier)
- **User Agents** - user agent strings sent from the browser used by the client
- **Combinations** - user defined combinations of Fingerprint specifications
- **Client Change Detection** - specifies when a device class change alert should be triggered

## Scan Engines

A3 scan engines entries define the interface to freeware and commercial software packages that find and flag conditions present on a client. For example:

- Outdated OS versions
- Non-existent, unapproved, or out-of-date anti-virus or other security software
- Open TCP/IP ports

Scan engines must be defined in A3 in order for security events that use their violations to have effect. Scan engines are defined in Configuration > Compliance > Scan Engines. The definition of scan engines is covered by A3's online help.

A3 supports several scan engine products:

- [Nessus](#)
- [OpenVAS](#)
- [Rapid7](#)
- [Microsoft WMI \(Windows Management Instrumentation\)](#)

## Nessus

*ⓘ The Nessus server should be installed on a separate server from the A3 server.*

Nessus can be downloaded from <http://www.nessus.org/download>. Download and install the package for your operating systems. You will also need to register for the HomeFeed (or the ProfessionalFeed) to get plug-ins.

After installing Nessus, follow the Nessus documentation for the configuration of the Nessus Server, and to create a user for A3. A3 imposes the following requirements:

1. A3 must be able to communicate with the Nessus server on the port specified in the installation.
2. The Nessus server must be able to access the client systems. Local network access is required if scan on registration is enabled.

## OpenVAS

*ⓘ The OpenVAS server should be installed on a separate server from the A3 server.*

Please visit [http://www.openvas.org/install-packages.html#openvas4\\_centos\\_atomic](http://www.openvas.org/install-packages.html#openvas4_centos_atomic) to configure the correct repository to be able to install the latest OpenVAS scanning engine.

Once installed, follow the instructions to correctly configure the scanning engine and create a scan configuration that will fit your needs. You'll also need to create a user for A3 to be able to communicate with the server.

It is important to get the correct scan config ID and NBE report format ID to populate the parameters in the A3 configuration file. The easiest way to get these IDs is by downloading both of the scan configuration and report format from the OpenVAS web UI and retrieve the IDs in the filenames.

For example report-format-f5c2a364-47d2-4700-b21d-0a7693daddab.xml gives report format ID f5c2a364-47d2-4700-b21d-0a7693daddab.

A3 imposes the following requirements:

1. A3 must be able to communicate with the OpenVAS server on the port specified in the installation and in the OpenVAS scan engine definition.
2. The OpenVAS server must be able to access the client systems. Local network access is required if scan on registration is enabled.
3. The OpenVAS server must be able to reach A3's administrative interface on port 1443 using its DNS entry.
4. A valid SSL certificate must be installed on the A3 server.

## Rapid7

Rapid7 can be integrated with A3 to automatically start a scan with a client connects to the network. Alert generation via syslog integration is currently not available.

## Rapid7 Installation

1. Install the InsightVM application from <https://insightvm.help.rapid7.com/docs/installing-in-linux-environments#section-installing-in-red-hat>.
2. Run the application. Refer to <https://insightvm.help.rapid7.com/docs/running-the-application#section-managing-the-application-in-linux>.
3. Log into the Rapid7 server: `https://<Rapid7ServerIP>:3780`, where <Rapid7ServerIP> is the IP address of the Rapid7 server.
4. Create a site for the devices you want to manage in Rapid7, you will need to reference it in the A3 configuration.

## Rapid7 A3 User

1. Navigate to Administration > Users.
2. Click Create.
3. Configure an appropriate name and password for a Rapid7 account that will be used by A3 to perform API calls on Rapid7.
4. In the roles for that user, select the Custom role and assign the following privileges:
  - Manage Sites
  - Manage Scan Engines
  - View Site Asset Data
  - Specify Scan Targets
  - View Group Data
5. In SITE PERMISSIONS, grant access to all sites.
6. In ASSET GROUP PERMISSIONS, grant access to all asset groups.
7. Click SAVE.

## A3 Configuration

### Scan Engine Definition

Configure a new scan engine for Rapid7:

1. Navigate to Configuration > Compliance > Scan Engines.
2. Click [New Scan Engine](#) and select Rapid7.
3. Fill in the following fields:

Field	Value
Name	Rapid7
Host Name or IP Address	Rapid7ServerIP
User Name	User name defined in <a href="#">Rapid7 A3 User</a> .
Password	Password defined in <a href="#">Rapid7 A3 User</a> .
Verify Host Name	Off unless a valid certificate has been generated and installed for Rapid7ServerIP.
Roles	Employees (or a role defined for all applicable users)
OS	The operating systems that the scan engine will be applied to.
Scan Before Registration	On. Leave this and the two following off if scanning will only be performed manually.
Scan on Registration	Off
Scan After Registration	Off

4. The scan template, site, and scan engine will be configured after the scan engine is defined.
5. Click [Create](#).
6. Select the **Rapid7** scan engine from the list of defined scan engines to edit the settings.
7. Select the Scan Engine, Scan template, and Site from the drop down lists populated from Rapid7.

### Connection Profile

For each connection profile associated with users who need to be scanned, select the **Rapid7** scanner from the **Scanners** setting in the connection profile.

### Viewing Rapid7 Results

The results of Rapid7 can be viewed in the entry for a client in the Clients table. A separate Rapid7 tab is shown, with sub-tabs for Summary, Device Profiling, Top Vulnerabilities, and Last Scan.

## Microsoft WMI (Windows Management Instrumentation)

WMI can be used on Windows-based PCs that have been joined to the domain to scan for violations and suspect conditions. A3's interface connects any violations found to security events. WMI must be enabled on each windows device with a GPO (global policy object) in Active Directory.

Multiple steps are required to use WMI A3 for each security event. For example, OS version out of date, no anti-virus software, or anti-virus software is out of date.

1. In Configuration > Compliance > Security Events set up a new security event. Set up a desired enforcement action for the violation.

Field	Value
Enable Security Event	On
Identifier	xxxx (used suggested number)
Trigger	Client, Client Profiling, Data Usage - all default Event: Internal xxxx
Event Actions	Isolate, Email Administrator

2. In Configuration > Compliance > WMI Rules, Rules Actions component add in a snippet for the violation. For example, the following snippet detects if Google is running. The tid value corresponds to the security event ID found in Configuration > Compliance > Security Events. A list of the example security events for WMI is found at [Miscellaneous](#).
3. The items in bold will trigger the violation established in step 1 above.

```
[Google]
attribute = Caption
operator = match
value = Google

[1:Google]
action=trigger_violation
action_param = mac = $mac, tid = xxxx, type = INTERNAL
```

4. Set up the WMI scanner on the Windows PC.
5. Associate the WMI scanner with a Connection Profile.

# Security Events

The key components of a security event are:

- [Event Triggers](#) - controls when a security event is invoked
- [Event Actions](#) - what to do when the event is triggered

## Event Triggers

A security event can use multiple individual triggers, any of which can occur. Each trigger has four components: client, client profiling, data usage, and event. For example,

Event Triggers	Client	Client Profiling	Data Usage	Event
1	No condition	AND All device types	AND Any data usage	AND Detect: 1100005
	OR			
2	No condition	AND All device types	AND Any data usage	AND Detect: 1100006
	OR			
3	No condition	AND All device types	AND Any data usage	AND Detect: 1100007
	OR			
4	No condition	AND Device: Router, Access Point or Femtocell	AND Any data usage	AND Any event

specifies four possible conditions, any of which can invoke the event. Each trigger is based on four clauses:

- **Client** - based on role, MAC address, IP address, or connecting device (accessing point).
- **Client Profiling** - client profiling uses information gathered from Fingerprint identification. Client profiling clauses are based on the device classification, DHCP fingerprint, DHCP vendor, or MAC vendor.
- **Data Usage** - based on upstream and/or downstream data consumption over a period of time.
- **Event** - based on other security events, events from scan engines, or internally triggered events. Internal events include host name change, new DHCP information, device parking, change of connection type, or client discovery.

## Event Actions

Any combination of the following actions may be executed when the event is triggered:

- **Unregister** - removes a devices registration status
- **Register** - register client in a role for a period of time
- **Isolate** - move client into a specific role (such as isolation). The client can receive a browser message indicating the nature of the problem and offering the ability to retry access.



(((1))) *Execute Scripts must be downloaded to each cluster member using root access. Contact support for assistance.*

- **Email administrator** - the administrator is apprised of the violation
- **Email Client Owner** - the client receives a copy of the administrator’s email with additional text
- **Execute Script** - a user downloaded script is executed
- **Close Another Security Event** - stops other events from triggering an action

## Built-in and Sample Events

A3 includes a number of predefined security events, some of which are ready-to-go and some of which must be enabled or require triggers or other parameters to be useful. The pre-defined events are described in the tables below

### Scan Engine Related

#### Internal

Description	Trigger	Action	Required to be Useful
Pre Reg System Scan	Just prior to registration.	Client is placed into the Isolation network.	Define script to be executed.
Post Reg System Scan	Just after registration.	Client is placed into the Isolation network.	Define script to be executed.

#### Nessus

Description	Trigger	Action	Required to be Useful
Nessus Scan	Any of a number of Nessus violations.	Client is placed back into the Registration network and an email is sent to the administrator.	Nessus scan engine definition.

#### Suricata

Description	Trigger	Action	Required to be Useful
P2P Isolation	An ET P2P event.	Client is placed into the Isolation network and an email is sent to the administrator.	Suricata scan engine definition.
Malware	An ET MALWARE condition.	Client is placed into the Isolation network and an email is sent to the administrator.	Suricata scan engine definition.
IRC Trojan	An ET TROJAN condition.	Client is placed into the Isolation network and an email is sent to the administrator.	Suricata scan engine definition.

## OpenVAS

Description	Trigger	Action	Required to be Useful
OpenVAS Scan	Any of a number of OpenVAS violations.	Client is placed back into the Registration network and an email is sent to the administrator.	OpenVAS scan engine definition.

## WMI Related

Description	Trigger	Action	Required to be Useful
Telnet Scan	WMI event	Client is placed into the Isolation network and an email is sent to the administrator.	Define WMI Rules.
Remote Desktop Scan	WMI event	Client is placed into the Isolation network and an email is sent to the administrator.	Define WMI Rules.

## Device Isolation

### Policy

Description	Trigger	Action	Required to be Useful
MAC Vendor isolation example	Any device with MAC OID of 29. Refer to Configuration > Compliance > Devices for a description.	Client is placed into the Isolation network and an email is sent to the administrator.	Change/add device specifications.
Ancient OS isolation example	Three old versions of Windows, plus two device numbers.	Client is placed into the Isolation network and an email is sent to the administrator.	Change/add device specifications.
MAC isolation example	Devices that have a MAC address starting with 01:23:45	Client is placed into the Isolation network and an email is sent to the administrator.	Change/add MAC address specifications.
Bandwidth Limit example	More than 20GB within a month.	Client is placed into the Isolation network and an email is sent to the administrator.	Change limit.
Device based Bandwidth Limit Example	Any Android device exceeding 1 GB in a month.	Client is placed into the Isolation network and an email is sent to the administrator.	Change/add device types and limits.
Time Expiration	None	Client is placed back into the Registration network, so that re-registration is required.	Set time limit in Data Usage column. Enabled by default.
Bandwidth Limit	None	Client is placed back into the Registration network, so that re-registration is required.	Set bandwidth limit in Data Usage column. Enabled by default.
Lost or Stolen	None	Client is placed into the Isolation network and an email is sent to the administrator and client owner. The client is not given a remediation button.	Add triggers to specify individual devices by MAC address.
Generic	None	Client is placed into the Isolation network and an email is sent to the administrator.	Assign triggers.
Block all mobile devices	Any phone, tablet, or wearable.	Client is placed into the Isolation network and an email is sent to the administrator.	None, disabled by default.
Block Apple iPod, iPhone or iPad	Any Apple mobile device.	Client is placed into the Isolation network and an email is sent to the administrator.	None, disabled by default.
Block BlackBerries	Any RIM Blackberry device.	Client is placed into the Isolation network and an email is sent to the administrator.	None, disabled by default.
Block PS3 and PSP	Any Sony Gaming Console.	Client is placed into the Isolation network and an email is sent to the administrator.	None, disabled by default.
Block Slingbox	Any Slingbox device.	Client is placed into the Isolation network and an email is sent to the administrator.	None, disabled by default.

## Suspicious Behavior or Conditions

Description	Trigger	Action	Required to be Useful
Rogue DHCP	Rogue DHCP request.	Client is placed into the Isolation network and an email is sent to the administrator.	None, enabled by default.
Connection transport change	Client changed their connection type. E.g. wired to wireless.	Client is placed into the Isolation network and an email is sent to the administrator.	None, enabled by default.
Fingerbank device class change	A change in Fingerbank device classification.	Client is placed into the Isolation network and an email is sent to the administrator.	None, enabled by default
LSASS Exploit	An attempt to circumvent Microsoft LSASS security enforcement.	Client is placed into the Isolation network and an email is sent to the administrator. Further stinger.exe is invoked to remove specific viruses.	None, disabled by default.
NetBIOS Scan	One of several NetBIOS conditions detected.	Client is placed into the Isolation network and an email is sent to the administrator.	None, disabled by default.
Zotob (W.32.Zotob and variants)	Detects Zotob virus	Client is placed into the Isolation network and an email is sent to the administrator.	None, disabled by default.

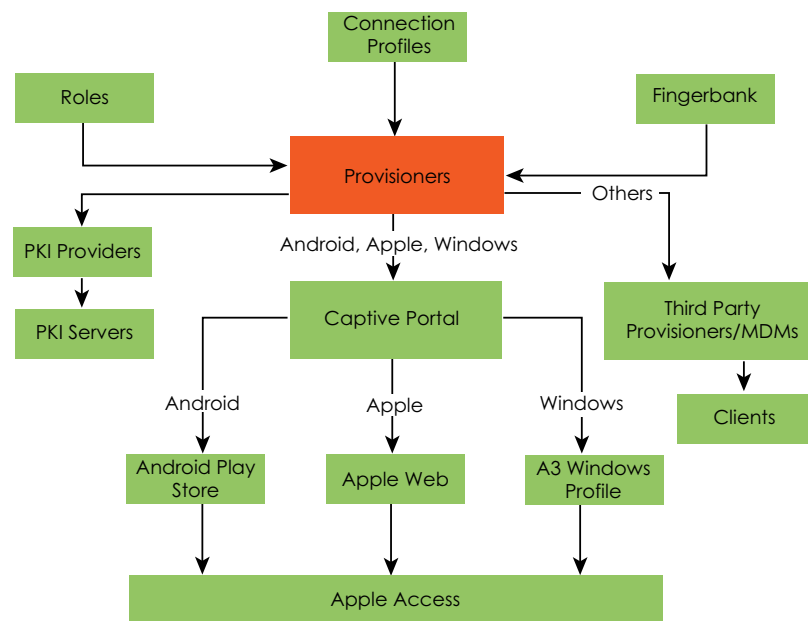
## Miscellaneous

Description	Trigger	Action	Required to be Useful
Provisioning Enforcement	Internal. If registration occurs outside of a CWP, the trigger occurs two minutes after registration.	Perform provisioning actions specified in the Connection Profile.	Specify provisioning actions in Connection Profile.
Generic	None	Client is placed into the Isolation network and an email is sent to the administrator.	Assign triggers.
defaults	None.	Client is placed into the Isolation network and an email is sent to the administrator.	Default values used for a new event definition.

# Provisioning

Provisioning plays an important part in proper client configuration. Provisioners are executed as part of Connection Profile operation as part of the authentication process. Provisioners deliver configuration information to clients or verify a device's management status with third-party MDM (mobile device management) solutions. On-device agents deliver wireless network settings to client devices. The required functions are built into iOS-based Apple devices. The required agents to Android- and Windows-based devices must be downloaded.

The figure below shows an overview of the components involved in provisioning.



The key elements are:

- **Connection Profiles:** multiple provisioners can be invoked in the final step of authentication, tying together all other configuration elements. Provisioners are performed in the order they are defined until one that satisfies operating system and role constraints is executed.
- **Provisioners:** provisioners provide configuration for possible clients, filtering based on operating system, roles, and other conditions. Several provisioners are built into A3 to perform common tasks:
  - **Android** - configures a wireless profile for Wi-Fi connection
  - **Apple** - configures a wireless profile for Wi-Fi connection
  - **Windows** - configures a wireless profile for Wi-Fi connection

- **Accept:** accepts client (filtering on role and OS) without any further provisioning
- **Deny:** denies clients based on role and OS
- **Interfaces:** connect to third party provisioners and MDMs
- **Roles:** the list of all possible roles. Each provisioner has an optional set of roles to use as a filter. Client roles are set as part of authentication as described in Configuration > Policies and Access Control > Authentication Sources. A client's role must match one of the settings in the provisioner role list unless the list is empty.
- **Fingerbank:** provides operating system identities used by provisioners to filter inapplicable clients.
- **PKI Providers:** provide an interface to PKI servers that generate certificates used to sign other certificates and trust third parties.
- **Captive Portal:** the captive web portal is used by Android, Apple, and Windows provisioners to configure clients with these operating systems. Android clients are redirected to obtain their agents through the Android Play Store. Apple clients incorporate agent functionality. Windows agents are contained within A3 and are automatically downloaded. Each of these provisioners may specify a new wireless connection from the access point including SSID, EAP, and security type.
- **Access point:** Android, Apple, and Windows provisioners may specify a new connection from the access point, including SSID, EAP, and security type during their execution.
- **Third party provisioners and MDMs:** A3 provisioners are interfaces to online systems associated with an MDMs. A3 uses these interfaces to query the MDM to determine if the client is included in their databases. If not, the client is transitioned to a isolation status. If the client is in the MDMs database, then it is assumed that the client has been previously configured by the MDM. The compatible MDMs are described in the following sections.

## Mobile Device Managers

---

The following MDMs are compatible with A3. Configuration of each takes place in **Configuration > Advanced Access Configuration > Provisioners**.

### Cisco DPSK

The Cisco DPSK (dynamic pre-shared keys) provisioner causes A3 keys to be dynamically generated.

### Jamf

The A3 interface to Jamf requires the use of a cloud account. The cloud account provides the necessary keys and other information for a connection.

### Microsoft Intune

Microsoft Intune using the Azure portal.

1. Log into the Azure portal and ensure that you have Intune licenses.
2. From the Azure portal , you'll need to create an application to enable access to the Graph API:
  - a. Select Azure Active Directory.

- b. Select App registrations.
- c. Select New registration.
3. On the Register an application form, enter:
  - a. A3, or some other name, in the Name field.
  - b. Select Accounts in this organizational directory only (company name).
  - c. Select Done.
4. On the following form entitled with the Name from above:
  - a. Copy the following that will be used to configure A3: Application (client) ID, Directory (tenant) ID, and Object ID.
  - b. Select Certificates & secrets.
  - c. Select New client secret.
  - d. This will present a password for use for the application. Copy it now; there will not be an opportunity later.
  - e. Add permissions to the API:
    - i. Select API permissions.
    - ii. Select Microsoft Graph.
    - iii. In the right pane select Application permissions and add two lines: Device.ReadWrite.All and DeviceManagementManagedDevices.Read.All.
  - f. Select Grant admin consent.

## MobileIron

MobileIron supports provisioning of Android, Apple, and Windows devices. Use the following steps to prepare for MobileIron for use with A3:

1. Log in to your MobileIron account and select **SETTINGS**.
  - a. Create an MDM certificate for use with Apple devices by clicking **Install MDM Certificate**.
2. Create a user with rights to access MobileIron's API:
  - a. Select **USERS & DEVICES**, then **Users**, and then click **Add local user**.
  - b. Enter information for a user (e.g. **a3user**), noting the user name and password.
  - c. Click **SAVE**.
  - d. Select the **ADMIN** tab, check the box for the just-entered user, then click **Actions** and choose **Assign to Space**.
  - e. Select **Global space** at the top and **check API** at the bottom.
3. Obtain the name of the boarding host by adding a fake device to MobileIron. At the end of the process the registration instructions will be displayed. The boarding host is labeled as the **Server Address** on that page.

## OPSWAT

OPSWAT Metadefender Endpoint provides information about device compliance before and during network access. The following discussion assumes that OPSWAT server components have been installed on a separate host from the A3 host and are referred to via an IP address of **10.150.1.55** or name of **localhost**. The following steps are used to configure an OPSWAT account:

1. Create an OPSWAT Metadefender Endpoint account at <https://www.opswat.com/products/metadefender/endpoint/management/>.
2. Create a developer account at <https://gears.opswat.com/developers>.
  - a. Register a new application with a callback URL of **http://10.150.1.55/opswat**.

- b. Note the client key and client secret.
  - c. Obtain an install URL by clicking **+Devices**, then **Enable Metadefender Endpoint client on another device**, then **Download or send link for guest Metadefender Endpoint clients**.
  - d. Note the URL at the bottom of the screen.
3. Generate an OAuth2 access and refresh token:
- a. Access the web page at **https://gears.opswat.com/o/oauth/authorize?client\_id=<clientid>&response\_type=code&redirect\_uri=http://10.150.1.55/opswat**, where <clientid> is your client key obtained in step 2b.
  - b. When the application is authorized, the browser will be redirected to a non-existent web page: `http://10.150.1.55/opswat?code=<code>`.
  - c. Generate the access and refresh tokens using: **https://gears.opswat.com/o/oauth/token?client\_id=<clientid>&client\_secret=<clientsecret>&grant\_type=authorization\_code&redirect\_uri=http://10.150.1.55/opswat&code=<code>**. <clientid> and <clientsecret> were obtained in step 2b, while <code> is from step 3b.

The access token and refresh token will be embedded in a message of the form:

```
{"access_token":"ab3aec71-fa6a-4752-8804-00c37f934059","token_type":"bearer","refresh_token":"f9e7c698-4d88-42cb-b9ae-c067557e8385","expires_in":43199,"scope":"read","client_id":"1234567890"}
```

## SentinelOne

SentinelOne performs provisioning for Windows and Mac OSX clients. SentinelOne requires root access to the A3 server, which is not currently supported.

## SEPM (Symantec Endpoint Protection Manager)

SEPM is used for provisioning Windows 32- and 64-bit clients. SentinelOne requires root access to the A3 server, which is not currently supported.



# Firewall Integration

A3's firewall integration informs firewalls which client is using a particular IP address. This information can be used by the firewall to apply per-user or per-role policies, effectively establishing single-signon. The firewalls supported by A3 include:

- [Barracuda](#)
- [Checkpoint](#)
- FamilyZone
- [FortiGate](#)
- Iboss
- [JSON-RPC](#)
- JuniperSRX
- LightSpeed Rocket
- [Palo Alto](#)
- SmoothWall
- WatchGuard

## Barracuda

---

### A3 Configuration

Assuming that the host name for the firewall is **barracudaNG**, create a Firewall SSO:

1. Navigate to Configuration > Integration > Firewall SSO.
2. Click [New Firewall](#) and select BarracudaNG.
3. Fill in the following fields:

Field	Value
Host Name or IP address	<b>barracudaNG</b>
User Name	Administrator login name on the firewall
Secret or Key	Password or secret key defined on the firewall
Roles	Employees (or a role defined for all applicable users)
SSO-Enabled Networks	The subnets on which SSO will apply
Default Realm	<b>default</b>

4. Click [Create](#).

## Verification

SSH to the Barracuda NG system and type the command:

```
acpfctrl auth show
```

The response should be similar to:

```
[root@baracudafw:~]# acpfctrl auth show
1 entries
172.20.20.152/0
origin=A3
service=A3
user=Jdoe
```

## Checkpoint

### Setting up the Checkpoint Firewall

#### Enable Identity Awareness

To enable Identity Awareness on the Checkpoint Security Gateway:

1. Navigate to the SmartDashboard.
2. From the Network Objects tree, expand the Check Point branch.
3. Double-click the Security Gateway on which to enable Identity Awareness.
4. In the Software Blades section, select Identity Awareness on the Network Security tab. The Identity Awareness Configuration wizard opens.
5. Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.
6. Select AD Query to allow the Security Gateway seamlessly identify Active Directory users and computers and click Next. The Integration With Active Directory window opens.
7. Select the Active Directory to configure from the list that shows configured LDAP account units or create a new domain. If you have not set up Active Directory, you need to enter a domain name, username, password and domain controller credentials.
8. Enter the Active Directory credentials and click Connect to verify the credentials. Important - For AD Query you must enter domain administrator credentials.
9. Click Finish.

#### Enable RADIUS Accounting

To enable RADIUS Accounting for a Security Gateway:

1. In the SmartDashboard Network Objects tree, open the Security Gateway.
2. On the General Properties page, make sure that the Identity Awareness Blade is enabled.
3. On the Identity Awareness page, select RADIUS Accounting.

## Configure RADIUS Accounting

1. In the Check Point Gateway Window > Identity Awareness panel, click Settings to the right of the RADIUS Accounting option.
2. In the RADIUS Accounting Settings window, configure the Message Attribute Indices:
  - Device Name: Calling-Station-Id (31) (MAC Address of the AP)
  - User Name: User-Name (1) (Username on the A3 Portal)
  - Device Name: Framed-IP-Address (8) (IP Address of the device in the production network)

## RADIUS Client Access Permissions

Gateway interfaces must be authorized to accept connections from A3 RADIUS Accounting. To select gateway interfaces:

1. In the RADIUS Client Access Permissions section, click Edit.
2. Select All Interfaces - All Security Gateway interfaces can accept connections from RADIUS Accounting clients.
3. Leave the default port to 1813.
4. Click OK on both windows to submit the configuration.
5. Select Policy > Install from the SmartDashboard menu.

## A3 Configuration

Assuming that the host name of the Checkpoint firewall is **cpfw**, and the name of the default realm is **default**, configure the A3 SSO definition as per the following instructions:

1. Navigate to Configuration > Integration > Firewall SSO.
2. Click  and select Checkpoint.
3. Fill in the following fields:

Field	Value
Host Name or IP address	<b>cpfw</b>
Secret or Key	The RADIUS shared secret from the Checkpoint configuration.
Roles	Employees (or a role defined for all applicable users)
SSO-Enabled Networks	The subnets on which SSO will apply.
Default Realm	<b>default</b>

4. Click .

## FortiGate

### Setting up FortiGate Firewall

#### Configuration of RSSO Agent

1. Navigate to the FortiGate administration web page in User & Device > User > User Groups > Create New.

- Fill in the form as per the following:

Field	Value
Name	RSSO_group
Type	RADIUS Single Sing-On (RSSO)
RADIUS Attribute Value	Employee (to match the A3 Role)

- Click OK.

### Configure the Endpoint Attribute

Change the endpoint attribute to User-Name via CLI:

```
config user radius
edit RSSO_agent
set rso-endpoint-attribute User-Name
end
```

### Activate Account Listening

- Navigate to System > Network > Interfaces.
- Select the interface that will communicate with A3.
- Check Listen for RADIUS Accounting Messages.

## A3 Configuration

Assuming that the host name of the Checkpoint firewall is **fgfw**, and the name of the default realm is **default**, configure the A3 FortiGate definition as per the following instructions:

- Navigate to Configuration > Integration > Firewall SSO.
- Click [New Firewall](#) and select FortiGate.
- Fill in the following fields:

Field	Value
Host Name or IP address	<b>fgfw</b>
Secret or Key	The RADIUS shared secret from the FortiGate configuration.
Roles	Employees (or a role defined for all applicable users)
SSO-Enabled Networks	The subnets on which SSO will apply.
Default Realm	<b>default</b>

- Click [Create](#).

## JSON-RPC

The JSONRPC module shipped with A3 is a generic firewall SSO module for use with Linux or BSD firewalls that do not ship by default with a vendor-specific SSO interface.

A simple JSON-RPC server written in Python that is compatible with this specification and creates ipsets based on the SSO information provided by A3 can be found at <https://github.com/tribut/ipset-rpcd>.

A compatible server must implement the **Start** and **Stop** methods, both with the identical set of parameters provided below:

Field	Value
Protocol	JSON-RPC 2.0 over HTTPS
Authentication	HTTP Basic authentication
Methods	Start, Stop
Parameters	
user (string)	Username that registered the device
mac (string)	MAC address of the device
ip (string)	IP address of the device
role (string)	A3 role assigned to the device
timeout (int)	Registration expiration in seconds
Response	Success must be indicated by " <b>result</b> ": [" <b>OK</b> "]. Anything other than <b>OK</b> is considered an error message.

## A3 Configuration

Assuming that the host name of the firewall is **json**, and the name of the default realm is **default**, configure the A3 SSO definition as per the following instructions:

1. Navigate to Configuration > Integration > Firewall SSO.
2. Click [New Firewall](#) and select JSONRPC.
3. Fill in the following fields:

Field	Value
Host Name or IP address	<b>json</b>
Username	HTTP Basic credentials
Password	HTTP Basic credentials
Roles	Employees (or a role defined for all applicable users)
SSO-Enabled Networks	The subnets on which SSO will apply.
Default Realm	<b>default</b>

4. Click [Create](#).

# Palo Alto

**(i)** *The integration between A3 and a Palo Alto Networks firewalls requires the use of PANOS 6.0 or higher on the Palo Alto firewall.*

This section describes how to set up A3 to communicate the identity of authenticated clients with a Palo Alto Networks firewall. This allows the Palo Alto Networks firewall to create identity-based security rules instead of subnet/VLAN/host-based rules. The network is then able to assign and enforce security policy based on the identity of the user, no matter what device they use.

## Setting up the Palo Alto Networks Firewall

In order to create user-based firewall policies, the firewall must be enabled to connect to the domain using LDAP, and set up WMI authentication. The firewall can be set up according to the documentation at <https://www.paloaltonetworks.com/documentation/81/pan-os/pan-os/user-id/enable-user-id>.

### Create PA API XML Role

A security best practice is to not use the default **admin** account to generate the token, but rather to create a separate local account on the firewall. First define a role to assign to the new local account.

1. Log on to the management interface of the Palo Alto Firewall.
2. Select Device > Admin Roles > Add.
3. Set the name to **SSO\_Role** or something similar.
4. Disable all rights in the Web UI tab.
5. Enable all features in the XML API tab.
6. Select OK.
7. Save and Commit the configuration.

### Create PA XML API User Account

1. Log on to the management interface of the Palo Alto Firewall.
2. Select Device > Administrator > Add.
3. Fill in the following fields:

Field	Value
Name	xmluser
Password	*****
Confirm Password	*****
Administrator Type	Role Based
Profile	SSO_Role

4. Select OK.
5. Save and Commit the configuration.

## A3 Configuration

Assuming that the host name of the Palo Alto firewall is **pafw**, and the name of the default realm is **default**, configure the A3 SSO definition as per the following instructions:

1. Generate the token (secret or key) using the following URL: [https://pafw/api/?type=keygen&user=\[xmlapiaccount\]&password=\[password\]](https://pafw/api/?type=keygen&user=[xmlapiaccount]&password=[password]), where [xmlapiaccount] and [password] are as defined in [Create PA XML API User Account](#).
2. Navigate to Configuration > Integration > Firewall SSO.
3. Click  and select PaloAlto.
4. Fill in the following fields:

Field	Value
Host Name or IP address	<b>pafw</b>
Vsys	1 if not used in a virtual environment, or the vsys number otherwise
Secret or Key	As generated in step 1) above.
Roles	Employees (or a role defined for all applicable users)
Networks on which to do SSO	The subnets on which SSO will apply.
Default Realm	<b>default</b>

5. Click .

## Verification

The Palo Alto firewall should now show the identity of users authenticating to A3. Refer to the Monitor tab > traffic in the Source User column.

## Use Case 1: Guest Access with Captive Web Portal

This use case implements guest authentication using most of A3's external authentication sources (see [External Authentication Sources](#)):

- [Null](#) - no identification is required.
- [Email](#) - the client enters their email address, which A3 uses to send a message. The message that the client receives includes a link that will complete the authentication. This form of authentication requires that [Alerting](#) be set up during [Initial A3 Configuration](#).
- [SMS](#) - the client enters their cell phone number, which A3 uses to send an SMS message. The message that the client receives includes a PIN (personal identification number) that is entered into the CWP (captive web portal) page to complete the authentication. This form of authentication requires that [Alerting](#) be set up during [Initial A3 Configuration](#).

The sponsor external authentication types will be demonstrated in [Use Case 4: Sponsored Access](#), for use with Active Directory.

A3 is configured through its administration interface. Access point configuration through ExtremeCloud IQ is covered in [MAC Authentication](#).

A3 configuration requires definition or modification of several A3 settings:

1. [Roles](#) - classifies the type of user. 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.
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. The connection profile also determines the RADIUS type and value attributes that will be sent to network devices upon connection and registration.

When configuration is completed, 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://<\(B\) address>:1443](https://<(B) address>:1443).



## Roles

---

Roles are accessed through the following steps:

1. Select Configuration > Policies and Access Control > Roles.
2. The list of predefined roles is shown. Verify that the **guest** role is visible.

All of the authentication sources in this use case will use the **guest** role.

## Authentication Sources

---

### Null

Inspect the **null** authentication source.

1. Select Authentication Source from the list on the left, below Roles.
2. Select the **null** source in the External Sources drop-down list.
3. Select Authentication Rules > Rule - catchall () at the bottom of the page.
4. 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.
5. Click Authentication Sources from the left-hand menu to return to the main Authentication Sources page.

### Email

Inspect the Email authentication source.

1. Select Authentication Source from the list on the left, below Roles.
2. Select the **email** source in the External Sources drop-down list.
3. Select Authentication Rules > Rule - catchall () at the bottom of the page.
4. 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.
5. Click Authentication Sources from the left-hand menu to return to the main Authentication Sources page.

### SMS

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. Select the **sms** source in the External Sources drop-down list.
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.
4. Click Save to save the authentication source if any changes were made or click Authentication Sources from the left-hand menu to return to the main Authentication Sources page.

## Devices

---

Device configuration is next:

1. Click **Devices** beneath **Network Devices**. The list of predefined entries is displayed.
2. A device for an access point must be defined. Click the **New Device** drop down control and then select **Aerohive\_AP**.
3. In the **New Device** form:
  - a. Enter the IP address of your access point **10.150.1.19 (C)** or an entire subnet using CIDR format in the **IP Address/MAC Address/Range (CIDR)** field.
  - b. Enter a **Description**.
  - c. Ensure that the **Use CoA** box is selected.
4. Select the **Roles** tab, ensure that only **Role by Device Role** is enabled. Enter **registration (e)**, **isolation (f)**, and **guest (g)** 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 ExtremeCloud IQ. Values are case sensitive.
5. Select the **RADIUS** tab. Enter **8AB7tHkP (b)** into the **Secret Passphrase** field. This matches the setting entered in the ExtremeCloud IQ.
6. 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**
2. Select **New Connection Profile**.
3. Fill in **Guest\_Profile** as the profile name and enter a description.
4. Uncheck **802.1X Recompute Role from Portal** since we are not using 802.1x authentication in this example.
5. **Filters**. Move down the page to the **Filters** section.
  - a. Select **Add Filter**
  - b. Select **SSID** from the list, and enter **A3-Guest (a)** beside the SSID. This tells A3 to use this connection profile when anyone connects to the access point using the A3-Guest (a) SSID.
6. **Sources**. Just below is the **Sources** section:
  - a. Select **Add Source**
7. Select **null** as the authentication source. This tells A3 to authenticate users against the sms authentication source.
8. Repeat for **email**.
9. Repeat for **sms**.
10. Click **Create**.

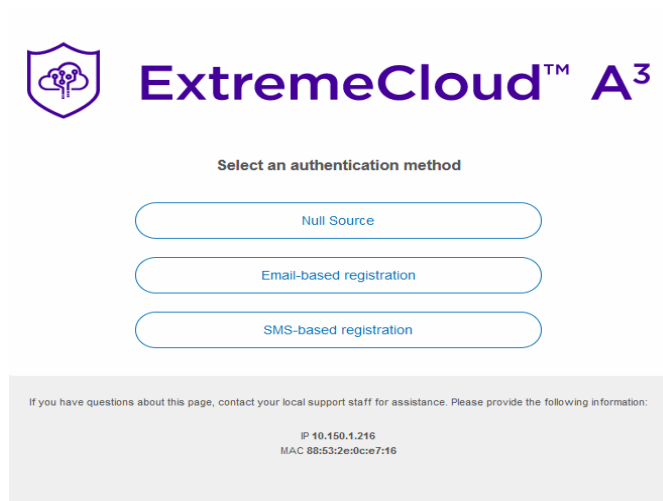
# Testing

If any Apple devices are used in the test, make sure to use a full browser for authentication, as opposed to Apple's Captive Network Assistant (CNA).

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

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

If your browser complains about the site or certificates, please reread the [A3 Server Certificate](#) section of this guide. The browser warnings relate to the use of a default self-signed certificate on A3. With persistent effort<sup>1</sup>, a banner page with a logo, terms of service, and offers for authentication will be shown.



Each of the alternatives can be selected for further testing. If more than one authentication type is used for the same client, the client must be unregistered in the A3 GUI:

<sup>(1)</sup> *Clients must be unregistered between tests as per the instructions to right.*

1. Select **Clients**.
2. Double click on the line corresponding to the client. The client should show a **registered** status.
3. Make the following changes to the entry:
  - a. Owner to **default**.
  - b. Status to **Unregistered**.
  - c. Role to **No Role**.
4. Select **Save**.

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.

## SMS Test

A screen that asks you for your phone number and choice of mobile carrier.

When Continue is selected, A3 sends an email to the mobile number for the carrier. The mobile number will receive an SMS with a PIN. The PIN is then entered into the web page, followed by Continue.

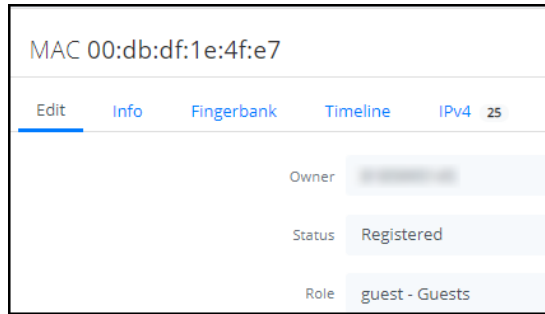
A success page is displayed with a progress bar letting you know that internet access is being enabled.

When the progress bar is finished, internet access will have been enabled. The browser is redirected to the site that is predefined in the captive web portal section of the [Connection Profile](#). You can also test this by selecting [extremenetworks.com](http://extremenetworks.com) or other site in your browser address bar.

In addition to successful authentication and network access, using A3's auditing function to check on the status of the authentication. Select Auditing from the top menu bar. Items are displayed in reverse order.

Created At	ID	Auth Status	MAC Address	IP Address	Is a Phone	Client Status	User Name	Unique ID	NAS IP Address
2019-12-06 01:12:31	2	Disconnect-ACK	00:08:ca:e1:da:21		0	reg	8185995145		10.150.1.19
2019-12-06 01:12:31	3	Accept	00:08:ca:e1:da:21		0	reg	0008cae1da21		10.150.1.19
2019-12-06 01:08:25	1	Accept	00:08:ca:e1:da:21		0	unreg	0008cae1da21		10.150.1.19

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.



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

## Use Case 1 Complete

This completes the External Authentication example.

## Use Case 2: Active Directory Authentication

<sup>(1)</sup> Alerting must be configured for this use case. See [Alerting](#).

This use case describes differentiated authentication based on Active Directory information. Users in marketing and sales security groups in the organization's Active Directory are assigned to user profiles that allow them access to potentially different network resources. Users in neither group will be assigned to a third VLAN associated with all other employees.

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 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. The connection profile also determines the RADIUS type and value attributes that will be sent to network devices upon connection and registration.

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://<\(B\) address>:1443](https://<(B) address>:1443).

### Active Directory Domain Join

---

#### Requirements

The following pieces of information are needed to join A3 to a domain:

- 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** (G) address.
- Domain DNS Server IP Address. This is the **10.150.1.5** (F) 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**.

## Active Directory Domain

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:

Field	Value
Identifier	CorpActive
Workgroup	example
DNS Name of the Domain	example.com
Active Directory Server	10.150.1.5 (G)
DNS Server(s)	10.150.1.5 (F)
Organizational Unit	Computers

4. Select [Create and Join](#).
5. When prompted, enter the administrator account and password that has privileges to join the domain.
6. 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-Main (c)) to your DNS server that refers to the A3 cluster address (B).

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.

## Realms

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 other 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.
  - a. In the Realm DEFAULT titled dialog, under NTLM Auth Configuration, select **CorpActive** from the Domain drop-down.
  - b. Enable Strip in the Captive Portal.
  - c. Enable Strip in the Administrative Interface.
  - d. Enable Strip in RADIUS Authorization.
  - e. Click SAVE.
4. Repeat the previous step for NULL.

It is common practice to use this the DEFAULT and NULL realms in this manner for simple Active Directory configurations.

## 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 SAVE.
4. Repeat the last step for the **Marketing** and **Employee** roles.

## Authentication Sources

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

1. Select Configuration > Policies and Access Control > Authentication Source.
2. Inside the Internal Sources box, click New Internal Source, and choose Active Directory.
3. Fill in the form as shown below, with:

Field	Comment	Value
Name		CorpAD
Description		Corporate Active Directory
Host	The Active Directory server	10.150.1.5 (G)
Base DN	The base AD tree location from which to start a user search	CN=Users,DC=EXAMPLE,DC=COM
Scope	Allows the search to progress to the entire tree beneath the Base DN	Subtree
User Name Attribute	The normal AD entry for the user's name	sAMAccountName
Email Attribute	The normal AD entry for the user's email, used for sponsored access.	mail
Bind DN	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	CN=jstaff,CN=Users,DC=example,DC=com
Password	The Bind DN user's password. At this point the TEST button beside the password can be used to check for a working connection.	*****
Associated Realms		default, null

4. Click Authentication Rules at the bottom of the page.
5. Add a **Sales** rule that matches Sales group membership in Active Directory:

Field	Value
Name	Sales
Description	Sales department members
Conditions	memberOf--equals--CN=Sales,CN=Users,DC=EXAMPLE,DC=COM
Actions	Role--Sales, Access Duration--1day.



- Click the plus sign to the right of **Sales (Sales department members)**. Repeat for the **Marketing** role:

Field	Value
Name	Marketing
Description	Marketing department members
Conditions	memberOf--equals--CN=Marketing,CN=Users,DC=EXAMPLE,DC=COM
Actions	Role--Marketing, Access Duration--1day.

- 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:

Field	Value
Name	catchall
Description	All other employees
Conditions	<none>
Actions	Role--Employee, Access Duration--1day.

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

## Devices

Device configuration is next:

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

Identifier	Description	Group	Type	Mode	
10.150.1.19	QSG AP (C)	Aerohive_AP	Aerohive::AP	production	<a href="#">Delete</a> <a href="#">Clone</a>
192.168.0.1	Test Access Point	Aerohive_AP	Aerohive::AP	production	<a href="#">Delete</a> <a href="#">Clone</a>
192.168.1.0/24	Test Range of Access Points	Aerohive_AP	Aerohive::AP	production	<a href="#">Delete</a> <a href="#">Clone</a>

- A device for our access point must be defined. Select [New Device](#) and then select **Aerohive\_AP**.
- In the New Device form, enter the IP address of your access point **10.150.1.19 (C)** in the IP Address/MAC Address/Range (CIDR) field, enter a Description, and ensure that the Use CoA box is checked.
- Select the Roles tab, ensure that only Role by Device Role is enabled.
  - Next to isolation, enter **isolation (f)**.
  - Next to **Sales**, enter **sales (h)**. Note that the entry is all lower case. This matches what the access point is expecting from A3.
  - Next to **Marketing**, enter **marketing (i)**.
- Select the RADIUS tab. Enter **8AB7tHkP (b)** 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, and then click [New Connection Profile](#).
2. Fill in a Profile Name as **Corp\_Conn** and Profile Description as desired.
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 (a)** next to SSID. This tells A3 to use this connection profile when anyone connects to the access point using the A3-Corp (a) 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.
7. Click [Create](#).

# Testing Active Directory

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 (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

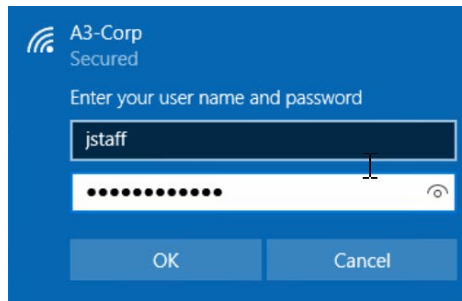
If a client has previously been authenticated, the client must be unregistered in the A3 GUI:

1. Select Clients.
2. Double click on the line corresponding to the client. The client should show a registered status.
3. Make the following changes to the entry:
  - a. Owner to **default**.
  - b. Status to **Unregistered**.
  - c. Role to **No Role**.
4. Select **Save**.

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

*Clients must be unregistered between tests as per the instructions to right.*

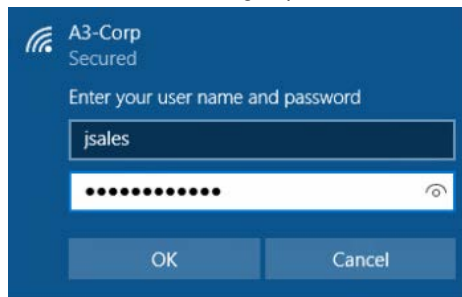
1. Connect to the **A3-Corp (c)** SSID and enter credentials for **jstaff**, who is an employee but not a member of either the **Sales** or **Marketing** AD security groups:



2. 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

3. If you intend to retest with the same client, then you need to ask A3 to forget the device registration as per the instructions above.
4. Connect to the **A3-Corp (c)** SSID and enter credentials for **jsales**, who is a member of either the **Sales** AD group:



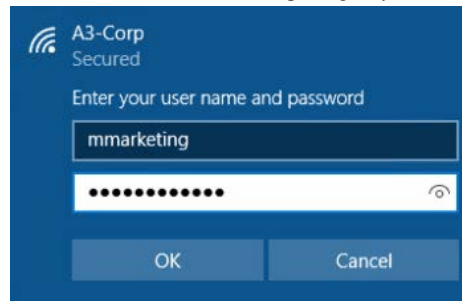
5. After the successful connection, look at the properties for the WiFi connection:

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 3 if you intend to reuse the same client for further testing.

7. Connect to the **A3-Corp (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:



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. 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 + sign next to Accept 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-Proxyed-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"	

## Use Case 2 Example Complete

This completes the Active Directory Authentication example for A3.

# Use Case 3: Local User Authentication

<sup>(1)</sup> Alerting must be configured for this use case. See [Alerting](#).

Another guest access alternative is referred to as local user, in which credentials are pre-defined and stored within A3. This type of authentication can be used for:

- Employees visiting from a remote site
- Contractors
- Visitors
- Temporary access for any reason
- Experimentation

Local user registrations are characterized by a user login, password, email address, usage time window, and network access role. The local user facility, however, cannot be used for 802.1X authentication.

## User Manager

The person creating a local user account must have appropriate A3 administration access rights. This can be done by any member of the User Manager Admin Role or by creation of a custom rule. The administrator login created when A3 was first installed is automatically a User Manager. If there will only ever be a single administrator, then this step can be skipped; proceed to [Create a Local User](#).

The rights associated with the User Managers can be viewed by selecting Configuration > System Configuration > Admin Access and then User Manager. These rights may be modified, or an alternate User Manager type Admin Role can be defined.

Employees are given User Manager access by creating or modifying an authentication source's administrative rule. Administrative rules are like authentication rules, but relate to A3 administration.

For example, all marketing department members may be given User Manager access. This example uses a local Active Directory. The following uses the same setup as in [Use Case 1: Guest Access with Captive Web Portal](#).

1. Navigate to Configuration > Policies and Access Control > Active Directory Domains.
2. If there is no domain definition, create one as in [Active Directory Domain Join](#).
3. Navigate to Configuration > Policies and Access Control > Authentication Sources.
4. If there is no AD type definition, create one as in [Authentication Sources](#).
5. Within the AD type authentication source, scroll down to **Administration Rules**.
6. Select  to add an Administration Rule. These are different and distinct from Authentication rules. Enter the following values.

Field	Value
Name	UserManager
Description	Allow all marketing members to be User Managers

Field	Value
Matches	All
Conditions	memberOf--equals--CN=Marketing,CN=Users,DC=EXAMPLE,DC=COM
Actions	Access level--User Manager

- Click Save.

## Local User Authentication

The final step adds the **local** authentication source to the **Guest** connection profile:

- Navigate to Configuration > Policies and Access Control > Connection Profiles.
- If a **Guest** connection profile does not exist, then create one as described in [Connection Profile](#).
- Select the **Guest** connection profile.
- Scroll down to sources. Add a new source, for **local**.
- Click Save.

## Create a Local User

At this point, the initial administrator can log out of A3 and any member of the company's Marketing group can log into A3's administrative interface with their company's Active Directory login name and password. That person has User Manager privileges, allowing them to create a local user.

The steps to create a local user are:

- Navigate to Users > Create.
- Fill in the form with the following fields:

Field	Value	Comment
User Name (PID)	contractor	A unique name for use on the captive web portal.
Password	secret1234	A password for use on the captive web portal.
Email	bill@contractor.com	An email address used for an invitation.
Registration Window	2019-08-22 --> 2019-08-25	A range of dates during which the user may login.
Actions	Role - Guest Access duration - 1 day	The role for the user and how long they can stay logged in.

- Click Send to send an email message at the address used in the form inviting them to log in to the local network when they arrive on-site.
- Click Save.

# Testing Local User Authentication

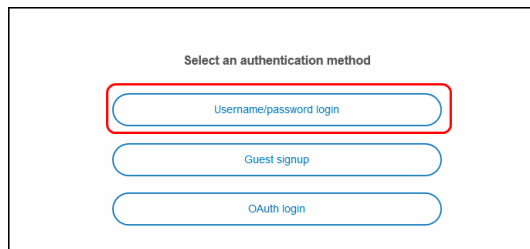
*Clients must be unregistered between tests as per the instructions to right.*

If a client has previously been authenticated, the client must be unregistered in the A3 GUI:

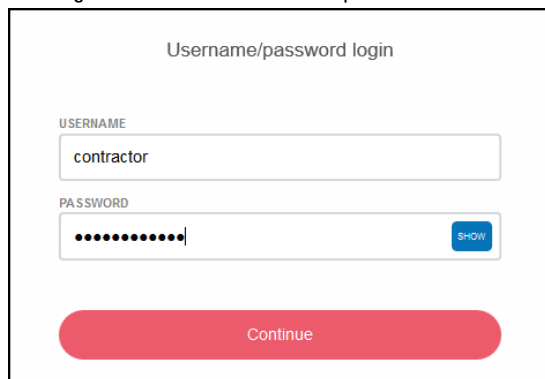
1. Select **Configuration > Clients**.
2. Click on the line corresponding to the client. The client should show a **registered** status.
3. Make the following changes to the entry:
  - a. Owner to **default**.
  - b. Status to **Unregistered**.
  - c. Role to **No Role**.
4. Select **Save**.

To test local user authentication.

1. Create a new user with your email address. The login **contractor** is used in this example.
2. Choose a device to access your network on the guest SSID. Connect to the guest SSID. An additional authentication choice will be displayed.



3. Log in with the user name and password used to define the user.



4. If the user name and password are correct, then guest access will be provided.

## Use Case 3 Example Complete


This completes the Local User Authentication example for A3.



## Use Case 4: Sponsored Access

This use case involves guest access requiring employee approval. The flow in this scenario is:

1. A client connects to the registration network, **A3-Guest** (a), for example.
2. The client accepts a standard acceptable use policy.
3. The client enters:
  - a. Their own email address.
  - b. The email address of the employee/sponsor. A3 will check that the sponsor is approved or not.
4. A3 sends an email to the sponsor. The sponsor must click through the email to activate the connection.

 *Alerting must be configured for this use case. See [Alerting](#).*

Authentication setup requires inspection, definition, or modification of several A3 settings:

1. [Active Directory Domain Join](#) - this was accomplished in a previous use case. Follow the link for details.
2. Roles - the guest role will be used.
3. [Authentication Sources](#) - an administration rule is used to designate authorized sponsors.
4. [Active Directory Source](#) - modifies the **CorpAD** active directory source and verifies the **sponsor** external source.
5. [Devices](#) - defines the network devices that authenticate clients against A3, in this case the access point. The same device is used as in previous use cases; follow the link for details.
6. [Connection Profile](#) - adds the local sponsor to the Guest connection profile from [Use Case 1: Guest Access with Captive Web Portal](#).

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).

## Authentication Sources

---


### Active Directory Source

The next steps modify the **CorpAD** authentication source which was defined in [Use Case 2: Active Directory Authentication](#).

1. Select Configuration > Policies and Access Control > Authentication Source.
2. Inside the Internal Sources box, select **CorpAD**.
3. Under Administration Rules: select  to add a new Administration rule.

4. Add a **Sponsor** rule that matches Sponsor group membership in Active Directory. The members of the Sponsor group must have valid email addresses in their mail attributes.

Field	Value
Name	Sponsor
Description	Employees who can sponsor access
Conditions	memberOf--equals--CN=Sponsors, CN=Users,DC=EXAMPLE,DC=COM
Actions	Mark as Sponsor

5. Click  to save the authentication source.


## Sponsor Source

The next steps verify the settings for the sponsor authentication source.

1. Select Configuration > Policies and Access Control > Authentication Source.
2. Inside the External Sources box, select **sponsor**.
3. Under Authentication Rules verify that a catchall rule exists with an action that sets **Role** to **guest**, and a reasonable **Access Duration**.

## Connection Profile


The connection profile in this use case was built in [Use Case 1: Guest Access with Captive Web Portal](#). The following modifications are made to support sponsored access.

1. Navigate to Configuration > Policies and Access Control > Connection Profiles.
2. Select the **Guest-Connection** profile.
3. In the Sources category, add **sponsor** as an additional source. This adds another choice to the guest CWP.
4. Click  to save the connection profile.

## Testing Sponsored Access

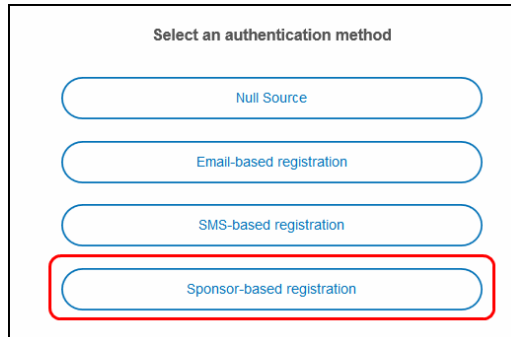
*Clients must be unregistered between tests as per the instructions to right.*

If a client has previously been authenticated, the client must be unregistered in the A3 GUI:

1. Select **Configuration > Clients**.
2. Click on the line corresponding to the client. The client should show a  status.
3. Make the following changes to the entry:
  - a. Owner to **default**.
  - b. Status to **Unregistered**.
  - c. Role to **No Role**.
4. Select **Save**.

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

1. Depending on the configuration of the guest connection profile, the user will be offered an additional choice for registration.



Select an authentication method

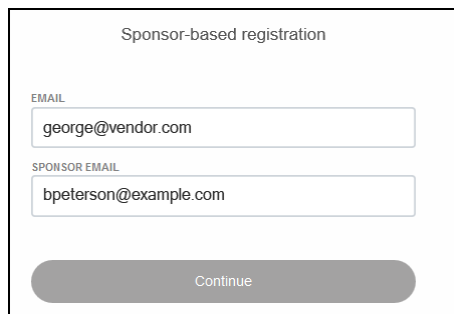
Null Source

Email-based registration

SMS-based registration

Sponsor-based registration

2. After selecting Sponsor-based registration, the client will be asked for their email address as well as that of their sponsor.



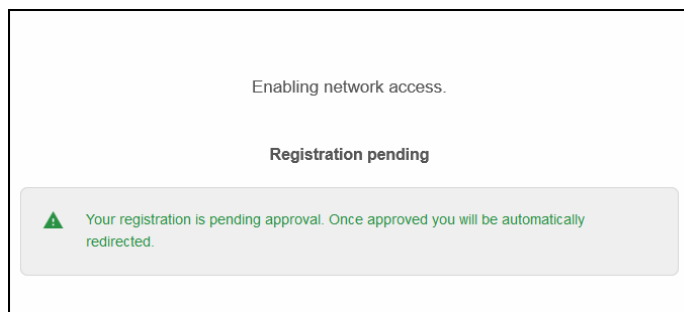
Sponsor-based registration

EMAIL  
george@vendor.com

SPONSOR EMAIL  
bpeterson@example.com

Continue

3. The user will be held while the sponsor is contacted.



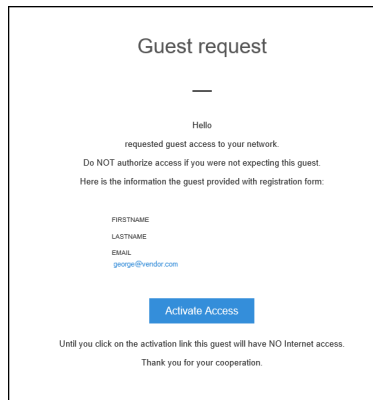
Enabling network access.

Registration pending

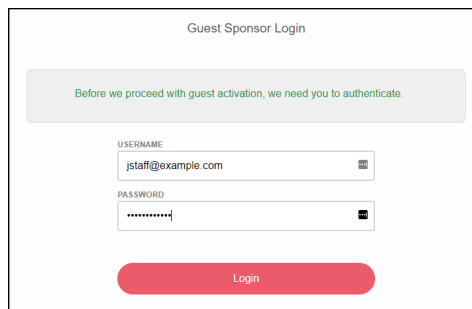
▲ Your registration is pending approval. Once approved you will be automatically redirected.

4. The employee designated in the SPONSOR EMAIL field will receive an email requesting approval for the user.

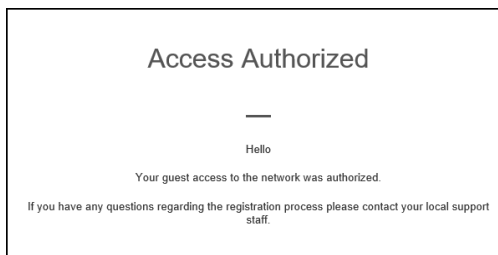
<sup>(1)</sup> A DNS entry for the A3 VIP (B) must be configured for this to work.



5. Clicking the link invokes an administrative login for A3.



6. Upon successful login, the client will be granted access. The client will also receive an email to the same effect.



### 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. 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
2019-09-16 20:22:59	52	Accept	e0:db:df:1e:4f:e7		0	reg	00dbdf1e4fe7		10.150.

### Use Case 4 Example Complete

This completes the Sponsored Authentication example for A3.

# Use Case 5: EAP-TLS Authentication

This case utilizes RADIUS certificates to perform EAP-TLS authentication between Windows clients and A3. The installation of RADIUS certificates on A3 is discussed in [RADIUS Certificate](#). This use case assumes that [PKI Provider](#) and [Provisioner](#) setup has been performed.

## EAP-TLS Authentication Source

A new EAP-TLS authentication source is defined to match all organization members. Authentication and authorization rules will be inherited from the Active Directory authentication source.

1. Navigate to Configuration > Policies and Access Control > Authentication Sources.
2. In the Internal Source category, select  and select EAP-TLS.
3. Fill in the form as per the following:

Field	Usage	Example
Name	Name of the authentication source.	EAPTLS
Description	Further description	EAPTLS used for employees
Associated Realms	The realm to associate with the source. See <a href="#">Use Case 2: Active Directory Authentication</a> for a description of how realms are established.	default
Authentication Rule	New rule to catch all EAP-TLS users	See below.

The authentication rule should include:


Field	Usage
Name	catchall
Description	Match all employees
Matches	All
Conditions	None
Actions	Role -- default, Access duration -- 5 days

## Connection Profile



---

This section assumes that the configuration associated with [Use Case 2: Active Directory Authentication](#) has been performed. The **Corp\_Conn** and **Guest\_Profile** should be modified as per the directions below.

### Corporate Profile

1. Navigate to Configuration > Policies and Access Control > Connection Profile.
2. Select the **Corp\_Conn** profile.
3. Enable 802.1X Recompute Role from Portal. This will cause the client's role to be recomputed from the 802.1X user name instead of re-using the value initially computed from the **Guest\_Profile**.
4. Add the **EAPTLS** authentication source to the Sources.
5. Click .

### Guest Profile


1. Navigate to Configuration > Policies and Access Control > Connection Profile.
2. Select the **Guest\_Profile** profile.
3. Ensure that the **CorpAD** authentication source is included in the Sources.
4. Select  to add the EAP-TLS provisioner defined in [Provisioner](#).
5. Click .


## Testing EAP-TLS

---

This sequence demonstrates the on-boarding and provisioning of a Windows client using the configuration described above, including [PKI Provider](#) and [Provisioner](#) setup. The client first connects to the **A3-Guest** SSID. Upon completion of the provisioning process, the client is directed to connect to the **A3-Corp** SSID. The client is then connected without any further interaction.

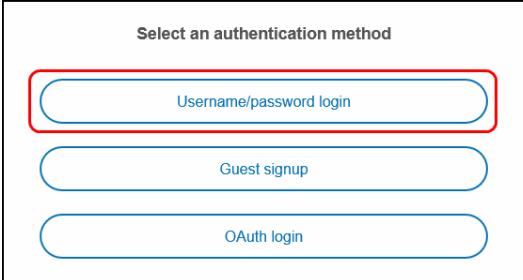
If a client has previously been authenticated, the client must be unregistered in the A3 GUI:

 *Clients must be unregistered between tests as per the instructions to right.*

1. Select **Configuration > Clients**.
2. Double click on the line corresponding to the client. The client should show a  status.
3. Make the following changes to the entry:
  - a. Owner to **default**.
  - b. Status to **Unregistered**.
  - c. Role to **No Role**.
4. Select **Save**.

The client first connects to the **A3-Guest** SSID.

1. After connecting to the guest SSID, the client is offered several choices, depending on the configuration of the **Guest\_Profile** connection profile. User name/password login is selected.



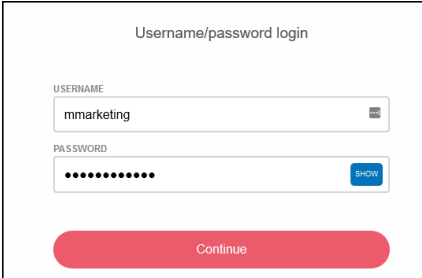
Select an authentication method

Username/password login

Guest signup

OAuth login

2. The client must agree to acceptable usage policy and is then offered a user name/ password form. Domain-specific credentials must be entered.



Username/password login

USERNAME

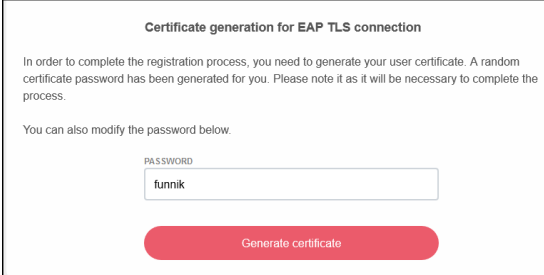
mmarketing

PASSWORD

.....

Continue

3. A3 will generate a certificate for the client, but first asks for a password to be used to protect the certificate. The client accepts the offered password or enters their own.



Certificate generation for EAP TLS connection

In order to complete the registration process, you need to generate your user certificate. A random certificate password has been generated for you. Please note it as it will be necessary to complete the process.

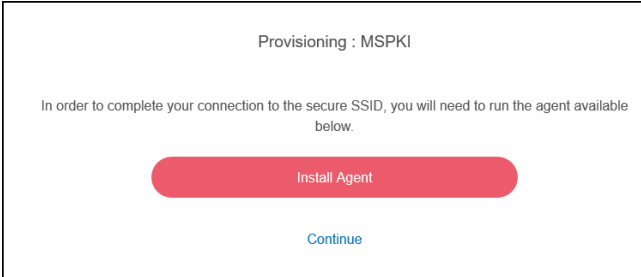
You can also modify the password below.

PASSWORD

funnik

Generate certificate

4. An agent program must next be downloaded and installed. Click on the **Install Agent** button.



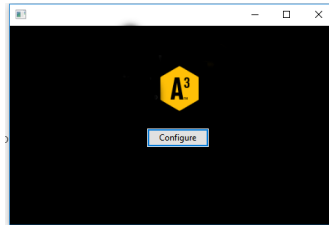
Provisioning : MSPKI

In order to complete your connection to the secure SSID, you will need to run the agent available below.

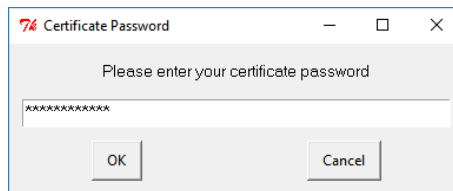
Install Agent

Continue

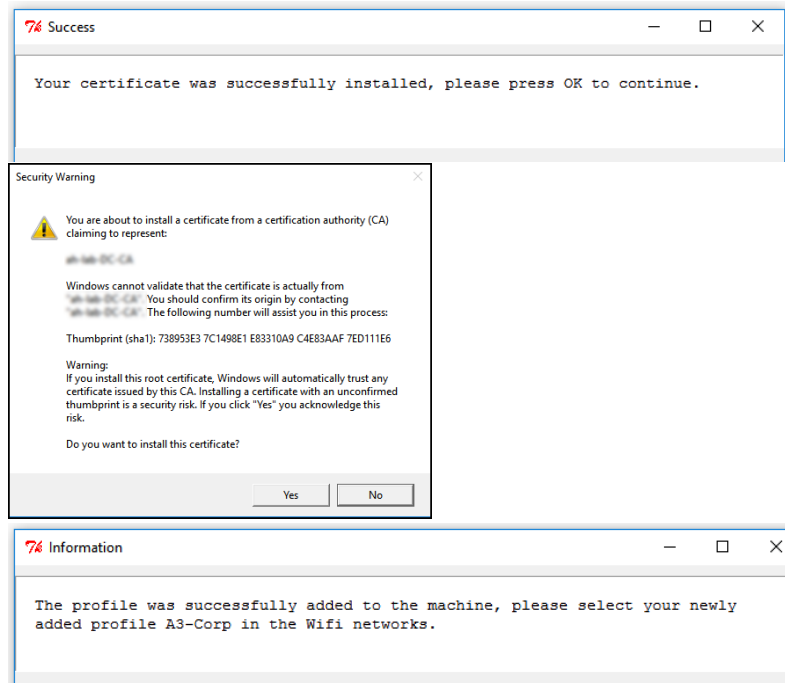
- The **a3-windows-agent.exe** file is downloaded. Locate and execute the file. Since the client is only connected to the registration network, any security scanners that require internet access may complain. This can be avoided through configuration of Passthrough Domains in Configuration > Network Configuration > Fencing. For the purpose of this example, any warning should be overridden. The agent prompts the client to configure the certificate. Select the **Configure** button.



- The client is next prompted for the password entered in step 3 above.



- A sequence of three prompts are displayed. Answer in the affirmative for each.



- At this point, the client can connect to the **A3-Corp** SSID. No login screen is needed since EAP-TLS is configured in A3 and the client's certificate has been installed on the computer.

## Use Case 5 Example Complete

This completes the EAP-TLS Authentication example for A3.



## Use Case 6: Guest Access with External Captive Web Portal

The requirement to extend registration and isolation VLANs out to each edge of a network may be inconvenient for an organization. An alternative authentication technique is available that uses an E-CWP (external captive web portal), which simplifies network configuration. Several restrictions apply:

- Client authentication may use any of the following techniques:
  - Internal sources: Active Directory, EAP-TLS
  - External sources: sms, email, sponsored, and null. OAuth2-based logins, such as Google and Facebook) may be used, but require the applicable servers to be added to the walled garden defined in [Network Policy](#) below.
- Only one access policy is used per SSID in ExtremeCloud IQ configuration.



This use case will use an E-CWP to authenticate guest access using VLAN 2. VLAN 2 is used for the default VLAN in ExtremeCloud IQ and is also returned by A3 as the selected VLAN.

In general, A3 may specify different VLANs based on different authentication mechanisms. The Role tab in the Device’s configuration will use Role by VLAN ID; a VLAN should be specified for each role used in the Connection Profile.

## ExtremeCloud IQ Configuration

It is necessary to configure a network policy for E-CWP that is different to the configurations covered in [ExtremeCloud IQ Setup](#). Use the following steps to configure a network policy named **A3-WA** (web authentication) in ExtremeCloud IQ.

### Network Policy

1. A new network policy is defined by selecting CONFIGURE > NETWORK POLICIES.
2. In the box entitled **Corp-Policy**, select the  icon.
3. Select the Wireless Networks tab.
4. Select the  button, and then the **All other Networks (standard)** choice.
5. Fill in the page with the following settings.

Field	Usage	Setting
Name (SSID)	Name of the SSID to be used for E-CWP	A3-WA
SSID Usage	The type of authentication for the SSID.	Open
Enable Captive Web Portal	Enables the use of the E-CWP	On
Captive Web Portal	The options for the E-CWP.	User Auth on Captive Web Portal (only)
Choose Authentication Type	How to perform authentication.	Redirect to External URL for Authentication
Default Captive Web Portal	Defines where to find the E-CWP web page.	See below.

Field	Usage	Setting
Authentication Settings - Authenticate via RADIUS Server	Defines the RADIUS server connection to A3.	See the RADIUS Server step in <a href="#">Authentication</a> .
User Access Settings	Sets up the Default User Profile with the single VLAN that will be used while the client is registering.	See the Default User Profile step in <a href="#">Authentication</a> . Use the VLAN for your network associated with guests. VLAN 2 is used in this example.

- Do not press SAVE yet.
- Beside Default Captive Web Portal, select the **ADD** button. Fill in the dialog with the following settings:

Field	Usage	Setting
Name	A name to identify the E-CWP server	A3-V3
Password Encryption	The form of encryption used between the access point and the E-CWP server.	UAM Basic
Authentication Method	The form of authentication used between the access point and the E-CWP.	PAP
Client Redirection - Use HTTP 302	Click on Advanced Configuration. Scroll down to Client Redirection. Select Use HTTP 302	Checked.
Walled Garden	Clients will have no network access until they have authenticated. This includes the E-CWP server. To allow necessary access to the A3 server, an entry must be added.	Add a new entry using the <b>+</b> sign. Select All and add the 10.150.1.254 <B> address in the box. Press <b>ADD</b> .

- Press **SAVE CWP** and then **Save** to save the new A3-WA network.

## A3 Configuration

A3 configuration requires definition or modification of several A3 settings:

- Roles - the **guest** role will be used, as defined in [Roles](#). The intention is to identify allow guest access through the E-CWP.
- Authentication Source - multiple alternative guest authentication sources will be used, as defined in [Authentication Sources](#).
- [Devices](#) - the device definition is modified as discussed below.
- [Connection Profile](#) - a new profile is defined to tie together the authentication source with a connection source, in this case an access point's **A3-WA** SSID.

When configuration is completed, authentication will be tested.

## Devices

- Navigate to Network Devices > Devices.
- Select the device to be used in [Devices](#).
- Select the Roles tab at the top.
- Enable **Role by VLAN ID** and disable **Role by Device Role**.
- The settings beneath Role by VLAN ID are used sent to the AP as the VLAN to be used by registered clients. Enter **2** beside the **guest** role.
- Click **Save**.

## 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
2. Select New Connection Profile.
3. Fill in the page as per the table:

Field	Usage	Setting
Profile Name	The name of the connection profile.	AD-WebAuth
Filter	Used to ensure that this connection profile is only used for the A3-WA SSID.	SSID -- A3-WA
Sources	The authentication sources to be used for the authentication.	null, email, sms

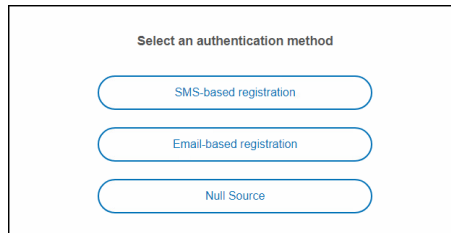
4. Click .

## Testing E-CWP Access

If any Apple devices are used in the test, make sure to use a full browser for authentication, as opposed to Apple's Captive Network Assistant (CNA).

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

Depending on your configuration, your default browser will reference [https://10.150.1.254\(B\)/captive-portal...](https://10.150.1.254(B)/captive-portal...) and open up an authentication challenge window.



Before going through authentication, note two things:

1. The client has been assigned an address in VLAN 2.

Properties	
SSID:	A3-WA
Protocol:	802.11n
Security type:	Open
Network band:	2.4 GHz
Network channel:	1
IPv4 address:	10.150.2.10
IPv4 DNS servers:	10.150.2.1
Manufacturer:	AzureWave Technologies, Inc.
Description:	802.11n Wireless LAN Card
Driver version:	5.0.57.0
Physical address (MAC):	00-08-CA-E1-DA-21

① *Clients must be unregistered between tests as per the instructions to right.*

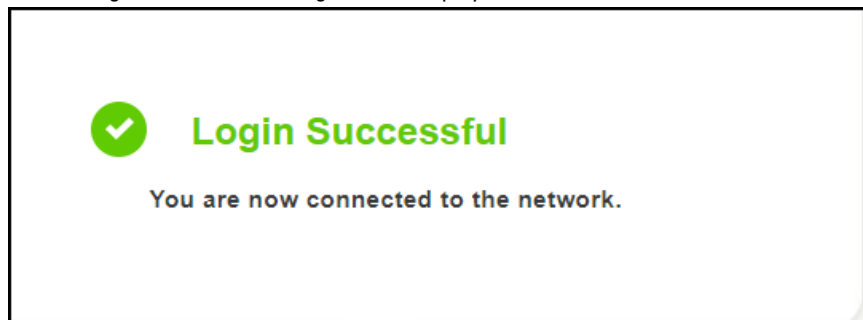
2. If an external web site, such as [extremenetworks.com](http://extremenetworks.com), is referenced in a new browser tab that another authentication challenge is issued. This verifies that the client is completely isolated from the organization's network.

Each of the alternatives can be selected for testing. If more than one authentication type is used for the same client, the client must be unregistered in the A3 GUI:

1. Select **Configuration > Clients**.
2. Double click on the line corresponding to the client. The client should show a **registered** status.
3. Make the following changes to the entry:
  - a. Owner to **default**.
  - b. Status to **Unregistered**.
  - c. Role to **No Role**.
4. Select **Save**.

## Null Authentication Test

1. Select **Null Source** and click **I accept the terms** on the subsequent page.
2. The login successful message should display.



3. Verify that the client's network address has not changed.
4. Verify that internet access is permitted by referencing an external web site, such as [cnn.com](http://cnn.com).

## Use Case 6 Complete

This completes the External Captive Web Portal example.

## Use Case 7: Headless IoT Devices

Devices that do not have any means of performing interactive authentication are often referred to as headless or IoT (internet of things) devices. They must be registered by other means.

Two options exist to manually register headless client devices:

1. **Manual:**
  - a. Login as an administrator.
  - b. Navigate to Clients > Search.
  - c. To define a single device found in the client list.
    - i. The device can be located by its Fingerprint identification and/or MAC address.
    - ii. Register the client device with a role and access duration.
  - d. To define a single device by entering its MAC address.
    - i. Select Create.
    - ii. Enter the MAC address, Role, and access duration (Unregistration time).
  - e. To import a list of devices from a csv (comma-separated values) file.
    - i. Navigate to Import.
    - ii. Click [Open CSV File](#). Select your CSV file.
    - iii. Use the Import Data tab to define the column layout in the file. Details on how to use this tab can be found in the A3 online help.
    - iv. Click on Import XX selected rows.
2. **Automatic:** set up a security event based on Fingerprint ID or other identification that registers the client device with a role and access duration. Security events can also be triggered manually for one or more client devices.

Manual configuration does not scale very well. Automatic registration will be discussed in this chapter.

Extreme Networks suggests the following configuration on ExtremeCloud IQ and A3

Field	Usage	Example
ExtremeCloud IQ > Configure > Add Network	SSID. Set up a separate SSID for IoT devices.	A3-IoT
	Broadcast SSID Using... Many devices require initial discovery over 2.4 GHz networks. <sup>a</sup>	Enable WiFi0 Radio Enable WiFi1 Radio
	MAC Authentication	On
	SSID Authentication	Personal WPA/WPA2/WPA3
	Key Value	IoTDeviceE2358
	User Access Settings: Default User Profile	default profile - Registration (VLAN: 11)
	User Access Settings: Apply a different user profile to various clients and user groups	On

Field	Usage	Example
	User Access Settings: Allow user profiles assignment using RADIUS attributes in addition to three tunnel RADIUS attributes.	On
	User Access Settings: Add User Profile	User Profile Name = iot VLAN 2 (Guest VLAN) Assignment: RADIUS attribute = iot
A3	Role. Any role can be used in conjunction with ExtremeCloud IQ access settings.	IoT
	Device. In the role tab for the device, map the role to something that will be matched in Extreme-Cloud IQ access settings.	IoT -> iot
	Connection Profile.	Filter: SSID = IoT.

- a. Most IoT devices require initial Wi-Fi discovery over 2.4 GHz connections (802.11b/g/n/ax). Check your devices requirements and set up your Wi-Fi network to match them.

## Automatic Registration Security Event

A security event is defined to trigger on the appearance of a headless IoT device:

- Navigate to Configuration > Compliance > Security Events.
- Click [New Security Event](#). Fill in the form as per the table below:

Field	Usage	Example
Enable Security Event	Enabled for use or not	On
Identifier	A unique number that identifies the security event.	3000006
Description	A further descriptive name shown in the Security Events list.	Automatic registration of IoT devices
Event Actions	What to do when the device is detected.	Register
	Role. A role should be specified that maps to connectivity needed for IoT devices.	IoT
	Duration. Any duration will work since A3 will re-evaluate the role at each expiration.	1 day
Event Actions	Email Administrator. This is optional, but will allow the administrator to keep track of new IoT devices.	
Event Triggers	Client Profiling.	Device -- Internet of Things (IoT)

- Click [Create](#).

The devices contained in the Internet of Things (IoT) category is listed in Configuration > Compliance > Devices. Search for **Internet of Things**; expand the list by selecting the plus sign.

The Security Event is now completely configured and will trigger for any device that profiles as an Internet of Things (IoT) device.


## Manual Use of Security Event

---

If a headless IoT device is not currently in the Fingerprint database or was otherwise missed by the security event trigger, the security event can still be used

1. Select Clients
2. Find and select the device in the client list.
3. Select the Security Events tab.
4. Select **Automatic registration of IoT devices** in the drop-down at the bottom of the form.
5. Select  . The security event will appear in the listing.

IoT registration can also be performed in bulk from the Clients view.

1. Select Clients.
2. Place a  beside all IoT devices to be registered.
3. Select the  at the top of the table.
4. Select **Automatic registration of IoT devices** from the Apply Security Event part of the list.

## Use Case 7 Complete

This completes the Headless IoT Devices example.

## Use Case 8: Eduroam

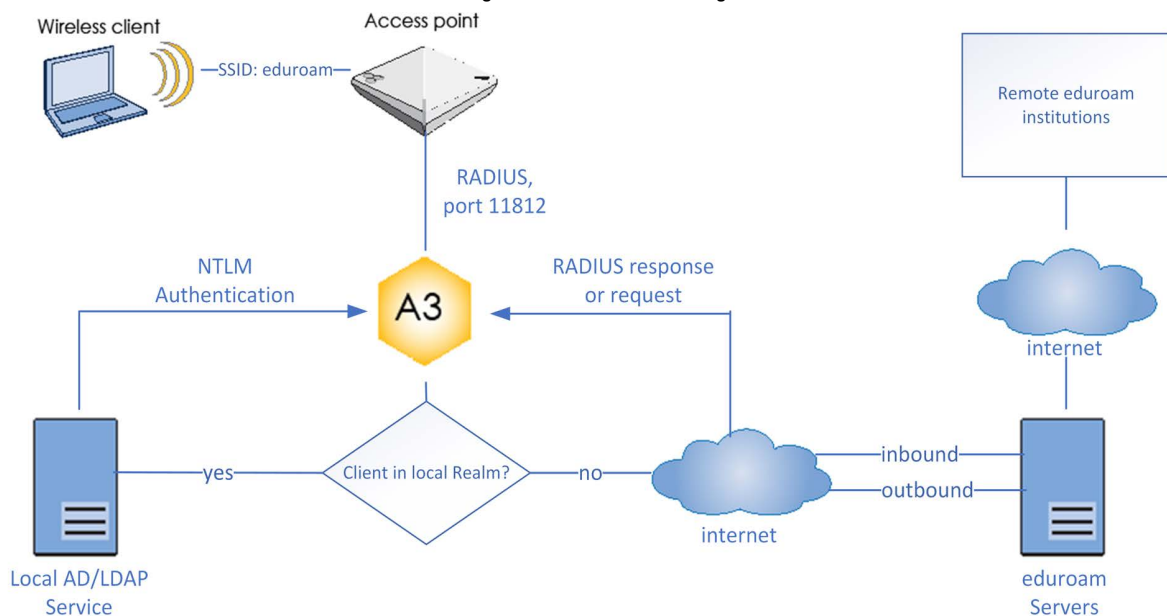
Eduroam (education roaming) is a secure, world-wide federated roaming access service used by the international research and education community. Eduroam allows students, researchers, and staff from participating institutions to obtain internet connectivity across campus and when visiting other participating institutions. Further information on eduroam is available at <http://www.eduroam.org/>.

Eduroam is a global example of realm-based authentication. The technology behind Eduroam is based on the IEEE 802.1X standard and a hierarchy of RADIUS proxy servers. An eligible organization can provide students, researchers, staff and faculty with wireless access at participating institutions through the use of their home institution credentials.

When a user connects with any participating wireless network using the **eduroam** SSID, the home RADIUS server does the authentication, while the host institution does the authorization.

## Overview

A3's eduroam integration is shown in the figure below.





## Local Users

Eduroam users who are associated with the institution local to your A3 can use the **eduroam** SSID for internet access. When they do so, the access point connects to A3 via RADIUS on port 11812 (1812 is the normal RADIUS port). This port lets A3 know that eduroam authentication is to be applied.

Based on configuration of the eduroam-based authentication source, A3 decides whether the user is in the local realm or not. If the user is in the local realm, A3 performs normal NTLM-based authentication using an AD or LDAP service.

## Remote Users

Eduroam users who are associated with some other institution, but connect through your local A3 may also use the **eduroam** SSID for internet access. When they do so, the AP connects the **eduroam** SSID to A3 for internet access via RADIUS on port 11812, as before.

Based on the configuration of the authentication source, A3 decides that the client is **not** part of a local realm. A3 then contacts one of the eduroam servers for authentication. The eduroam server proxies the request to the appropriate institution using RADIUS. The success/failure response is fed back to A3 and thence to the AP for enforcement.

## Local Users at Remote Sites

Eduroam users from your institution can use the **eduroam** SSID at another institution. That institution's authentication mechanism will find that the user is not local to their site, thus sending an authentication request to the eduroam servers. That request will be forwarded to your local site via RADIUS. A3 performs local NTLM authentication and sends the success/failure response back to the eduroam server.

## ExtremeCloud IQ Configuration

---

ExtremeCloud IQ must be configured for an **eduroam** SSID, but using port 11812 for RADIUS communications with A3 instead of the normal 1812. The same shared secret used for normal operation (port 1812) should be used. Other configuration requirements are dictated by the eduroam configuration documents.

## A3 Configuration

---

A3 must be configured for both local and remote eduroam-related authentication. This involves creation or editing of five items:

- [Local Domain and Realm](#) - named **ExampleUAD** and **exampleu.edu**.
- [Local Authentication Source](#) - named **LocalADAuth**.
- [Eduroam Authentication Source](#) - named **eduroamAS**.
- [Local Connection Profile](#) - named **LocalEduroamCP**.
- [Eduroam Connection Profile](#) - named **eduroamCP**.

## Local Domain and Realm

If not already defined, both an Active Directory domain and realm that refers to the domain must be defined. The domain will be named **ExampleUAD** and the realm will be named **exampleu.edu**.

### Active Directory Domain

1. Navigate to Configuration > Policies and Access Control > Active Directory Domains.
2. Select [New Domain](#).
3. Fill in the form with the values below.

Field	Usage	Example
Identifier	A name for the AD.	<b>ExampleUAD</b>
Workgroup	Name of the workgroup.	exampleu
DNS Name of the Domain	DNS name for the institution's DNS	<b>exampleu.edu</b>
Active Directory Server	The IP address of the AD server.	10.150.1.5 (G)
DNS Server(s)	The IP address(es) of the domain's DNS server(s).	10.150.1.5 (F)
Organizational Unit	The computer account name in the AD.	Computers

4. Select [Create and Join](#).
5. When prompted, enter the administrator account and password that has privileges to join the domain.
6. 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-Main (c)) to your DNS server that refers to the A3 cluster address (B).

### Realm

A realm must be created to use the Active Directory that you just defined.

1. Select Configuration > Policies and Access Control > Realms.
2. Select [New Realm](#).
3. Fill in the form with the values below:

Field	Usage	Example
Realm	A name for the realm.	<b>exampleu.edu</b>
Domain	The domain used for authentication in the realm.	ExampleUAD

4. (Optional) If the Eduroam Realm will use a RADIUS proxy, fill in the form with the values below:

Field	Usage	Example
Eduroam Realm Options	Options for FreeRADIUS proxying to a local server.	<b>strip</b>
Eduroam RADIUS Auth	The RADIUS server(s) used to proxy Eduroam authentication. The list is composed of entries from RADIUS Internal Authentication sources.	eduradius

5. Click [Create](#).

## Local Authentication Source

A local AD authentication source must be defined that references the LocalRealm just defined. The authentication source will be named **LocalADAuth**.

1. Select Configuration > Policies and Access Control > Authentication Source.
2. Inside the Internal Sources box, click [New Internal Source](#), and choose Active Directory.
3. Fill in the form as shown below:

Field	Value
Name	<b>LocalADAuth</b>
Description	Local authentication for eduroam users
Host	10.150.1.5 (G)
Base DN	CN=Users,DC=exampleu,DC=edu
Scope	Subtree
User Name Attribute	sAMAccountName
Email Attribute	mail
Bind DN	CN=admin,CN=Users,DC=exampleu,DC=org
Password	*****
Associated Realms	LocalRealm

4. Click Authentication Rules at the bottom of the page.
5. Click [Add Rule](#) to create a **catchall** rule that will place all users into the Guest role:

Field	Value
Name	catchall
Description	All local eduroam users
Conditions	<none>
Actions	Role--Student <sup>a</sup> , Access Duration--1day.

- a. Or other appropriate role for internal eduroam authenticated users.

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

## Eduroam Authentication Source

<sup>(1)</sup> *The iptables service must be restarted after the eduroam authentication source is created.*

An eduroam authentication source must be defined. The authentication source will be named **eduroamAS**.

1. Select Configuration > Policies and Access Control > Authentication Source.
2. Inside the Exclusive Sources box, click [New Exclusive Source](#), and choose Eduroam.

- Fill in the form as shown below:

Field	Value
Name	<b>eduroamAS</b>
Description	Eduroam authentication
Server 1 Address	1.2.3.4
Eduroam Server 1 Port	1812
Server 2 Address	2.3.4.5
User Name Attribute	1812
RADIUS Shared Secret	Value supplied by eduroam.
Local Realms	exampleu.edu

- Click Authentication Rules at the bottom of the page.
- Click [Add Rule](#) to create a **catchall** rule that will place all users into the Guest role:

Field	Value
Name	catchall
Description	All eduroam users
Conditions	<none>
Actions	Role--Guest, Access Duration--1day.

- Click [Create](#) to save the authentication source.
- Restart the iptables service using Status > Services.

## Local Connection Profile

*LocalEduroamCP must appear before eduroamCP in the list of all connection profiles.*

The local connection profile will be named **LocalEduroamCP**.

- Select Configuration > Connection Profiles, and then click [New Connection Profile](#).
- Fill in the form with the following values:

Field	Value
Profile Name	<b>LocalEduroamCP</b>
Profile Description	Connection for local eduroam users
Automatically Register Clients	On
802.1X Recompute Role from Portal	Off
Filters	SSID -- eduroam
Sources	LocalADAuth

- Click [Create](#).

## Eduroam Connection Profile

The eduroam connection profile will be named **eduroamCP**.

- Select Configuration > Connection Profiles, and then click [New Connection Profile](#).
- Fill in the form with the following values:

Field	Value
Profile Name	<b>eduroamCP</b>
Profile Description	Connection for local eduroam users

Field	Value
Automatically Register Clients	On
802.1X Recompute Role from Portal	Off
Filters	Filters all SSID -- eduroam Realm -- eduroam
Sources	eduroamAS

3. Click [Create](#) .

## Use Case 8 Complete

This completes the Eduroam use case.

# Advanced Topics

## Best Deployment Practices

---

A3's database is a distributed database, requiring high performance and low latency to operate correctly. This section discusses best deployment practices to ensure latency and stability.

### Memory and vSwap

VMware vSwap should be turned off for A3. vSwap may cause latency as a cluster member attempts to swap memory. It's also best to set 100% Memory Reservation by entering the amount of RAM required in the VM configuration and selecting **Reserve all guest memory (All locked)**. An additional benefit of this approach is to eliminate physical memory fragmentation - another factor in controlling latency.

### vMotion

vMotion is not supported for A3 VMs.

### Fault Domains

vSphere's affinity model allows a set of VMs to be spread across ESXi hosts in a vSphere cluster. A3 is already a distributed system that handles its own data replication. A3 VM affinity should be configured so that vSphere will not put any two A3 VMs on the same physical host.

### RARP

Switches must be notified to modify the ARP entries for virtual machines as they migrate. This avoids long pauses while forwarding paths are resolved. All switches in the network must support ARP in a VMware-compatible manner. vMotion's notify switches option must also be enabled to send RARP packets.

### Link Capacity

vMotion requires significant bandwidth to transfer gigabytes of VM RAM between hosts. Although it is normally configured to limit its bandwidth to 10Gbps, it can be configured for larger links. If possible, dedicated links should be used for vMotion traffic. Those links should be configured with jumbo packets of 9000 bytes, if possible.

## Paravirtualization

Under certain heavy I/O load from multiple VMs, paravirtualization can cause A3 VMs to slow by a factor of 20%. Beneficially, however, paravirtualization improves stability and performance reliability and linearity.

## Snapshots

VM snapshots affect the performance of running VMs. Copy-on-write snapshots have a further detrimental affect, since two disk accesses are performed for each application write operation. It is desirable, therefore, to disable snapshotting of A3 VMs.

If snapshots are used, only VM disks should be snapshot and not the RAM. Memory snapshots will introduce extended latency in A3 operation.

## Administrative Access

Although a single administrator is defined at A3 installation, lesser administrative access can be given to other A3 administrators. The admin access roles are used in Authentication Sources under Administrative Rules. See the example below; a larger scale example is included in [Use Case 3: Local User Authentication](#).

1. Navigate to **Configuration > System Configuration > Admin Access**.
2. The built-in roles are listed below. These can be used as-is:
  - **ALL**: provides the user with all the admin roles without any exception
  - **ALL\_PF\_ONLY**: provides the user with all the admin roles related to the A3 deployment (excludes switch login rights)
  - **Node Manager**: provides the user the ability to manage the nodes
  - **User Manager**: provides the user the ability to manage other users
  - **Security Event Manager**: provides the user the ability to manage the security events (trigger, open, close) for the nodes
3. Otherwise a new role can be defined, select [New Admin Role](#).
4. Fill in the form as per the following table:

Field	Usage	Example
Name	Name for the type of administrator, not the name of the administrator.	User admin
Description	A further description	Can administer user entries
Actions	Which actions this type of admin can perform.	Select all the actions under <b>Users</b> .

## Creating Dynamic Reports

Using the `/usr/local/pf/conf/report.conf` configuration file, you can define reports that create SQL queries to view tables in the A3 database. These reports will appear under the **Reports > Dynamic Reports** menu of the A3 GUI.

In order to configure a report, you need to edit `/usr/local/pf/conf/report.conf` and add a section that defines your report. Then execute the command:

```
/usr/local/pf/bin/pfcmd configreload hard.
```

The following attributes are available to define your report:

Field	Usage	Example
type	Determines what type of report this is. Setting <b>type=built-in</b> will cause this report to appear under <i>Other</i> reports in the A3 GUI. If this field is left blank the report will appear under Dynamic reports.	
description	(Mandatory) The text that will be displayed under the appropriate heading for the report.	Authentication report
base_table	(Mandatory) The base SQL table that will be used to create the report.	auth_log
columns	(Mandatory) The columns to select from the table(s).	auth_log.*
date_field	(Mandatory) The field to use for date filtering. This will also be used as the default sorting field unless <b>order_fields</b> is defined.	attempted_at
joins	The tables to join in the base table and how to join them. See below for an example.	
group_field	The field to group the entries by. No grouping is performed if this field is empty.	
order_fields	A comma separated field indicating the ordering of the report. The field should be prefixed with a minus sign (-) if the sort should be made in descending order for the field.	-node.regdate, locationlog.start_time, +iplog.start_time
base_conditions	A comma separated field indicating conditions that should be applied to the report. This can be used to filter the report without requiring that the user use the search facility. Conditions should use the following format: <i>field:operator:value</i> .	auth_log.source::=sms, auth_log.status!:=:completed
base_conditions_operator	One of <i>all</i> or <i>any</i> , indicating how the base conditions should be matched.	all
person_fields	The comma separated fields in the report that represent a user in the A3 database. Field values in this field will be clickable, allowing the user to view or modify values for the selected user. The fields must be listed with the name they have in the report header without any quotes.	
node_fields	The comma separated fields in the report that represent a node in the A3 database. Field values in this field will be clickable, allowing the user to view or modify values for the selected node. The fields must be listed with the name they have in the report header without any quotes.	mac
searches	A comma separated list of searches that should be available in the report. Each entry should be in the following format <i>type:Display Name:field</i> . <ul style="list-style-type: none"> <li><b>type</b> defines the type of the search, the only type currently supported is string.</li> <li><b>Display Name</b> is the user friendly name of the field for display.</li> <li><b>field</b> is the SQL name of the field to search.</li> </ul>	string:Username:auth_log.pid



**Notes:**

1. The operators IS and <> should be replaced by = and !=, respectively.
2. You should always prefix the fields with the table name and a dot (e.g. node.mac, locationlog.role) so that they are not ambiguous. Although your query may work with a single table, it will not if you decide to add joins that contain column name(s) that are the same as the base table.

## Examples

### View of the authentication log

In this simple example, you will be able to select the whole content of the auth\_log table and use the date range on the attempted\_at field as well as search on the pid field when viewing the report.

```
[auth_log]
description=Authentication report
# The table to search from
base_table=auth_log
# The columns to select
columns=auth_log.*
# The date field that should be used for date ranges
date_field=attempted_at
# The mac field is a node in the database
node_fields=mac
# Allow searching on the PID displayed as Username
searches=string:Username:auth_log.pid
```

### View of opened security events

In the following example, the security\_event table is left joined to the class, node and locationlog tables. All security events are listed, even on deleted nodes. Base conditions are added to filter out outdated locationlog entries as well as include devices without

locationlog entries. Removing those conditions would lead to duplicate entries being shown since the report would reflect all the historical locationlog entries.

```
[open_security_events]
description=Open security events
# The table to search from
base_table=security_event
# The columns to select
columns=security_event.vid as "Security event ID", security_event.mac as "MAC
Address", class.description as "Security event description", node.computername
as
"Hostname", node.pid as "Username", node.notes as "Notes", locationlog.switch_ip
as "Last switch IP", security_event.start_date as "Opened on"
# Left join node, locationlog on the MAC address and class on the security event
ID
joins=<<EOT
=>{security_event.mac=node.mac} node|node
=>{security_event.mac=locationlog.mac} locationlog|locationlog
=>{security_event.vid=class.vid} class|class
EOT
date_field=start_date
# filter on open locationlog entries or null locationlog entries via the end_date
field
base_conditions_operator=any
base_conditions=locationlog.end_time=:0000-00-00,locationlog.end_time:IS:
# The MAC Address field represents a node
node_fields=MAC Address
# The Username field represents a user
person_fields=Username
```

## Performance Enhancements

### DHCP - IP Helpers

A3 works best when it sees IP DHCP assignment for devices on its networks. For any networks or VLANs where client isolation or IP address lookup is required, IP helpers can be used.

No action is required for the registration or isolation networks or VLANs since A3 performs DHCP functions.

IP helpers are the simplest and best solution for production networks that already use IP helpers. To use this feature on Extreme Networks Access Points, set the secondary DHCP server to A3's management VIP address (B).

To use this feature on other equipment, add A3's management VIP address as the last **ip-helper-address** statement in your network equipment. This will cause A3 to receive a copy of all DHCP requests for that VLAN and will record what IP addresses were distributed to what client.

## DHCP - Remote Sensor

The DHCP remote sensor is a lightweight binary that can be installed on a production DHCP server in order to replicate the DHCP traffic 1:1 to the A3 server. This solution is more reliable than the DHCP relaying since A3 will receive a copy of all DHCP traffic, not just the broadcast DHCP traffic. Supported DHCP servers are Microsoft DHCP server and CentOS 6 and 7.

### Microsoft DHCP Sensor

DHCP-Forwarder is an optimized version of udp-reflector, which installs easily and only copies DHCPREQUESTS and DHCPACK packets to the destination.

Download the installer from [here](#). This will

1. Install **WinPCAP** and **nssm**.
2. Launch a configurator to set interface, IP, and port. Specify A3's VIP address (B) and port 767 as the UDP port.
3. Save the configuration.
4. Install and launch the DHCP-Forwarder service.

### Linux-based Sensor

1. Download the RPM on your non-A3 DHCP server.
  - a. CentOS 6 servers:

```
wget http://inverse.ca/downloads/PackageFence/CentOS6/extra/x86_64/RPMS/udp-reflector-1.0-6.1.x86_64.rpm
```

- b. For CentOS 7:

```
wget http://inverse.ca/downloads/PackageFence/CentOS7/extra/x86_64/RPMS/udp-reflector-1.0-6.1.x86_64.rpm
```

2. Install the sensor:

```
rpm -i udp-reflector-*.rpm
```

3. Configure the sensor. Place the following line in **/etc/rc.local**:

```
/usr/local/bin/udp_reflector -s pcap0:67 -d 10.150.1.254(B):767 -b 25000 &
```

where **pcap0** is the pcap interface that the DHCP server listens on (the interfaces can be listed using the **udp\_reflector -l** command) and 10.150.1.254(B) is the management VIP of your A3 server.

*On some versions of Windows, the **getmac** command will return invalid output when running the installer in a language other than English. In order to workaround the issue, change your Windows language to English, then logout/login and run the installer again.*

## 4. Start the sensor:

```
/usr/local/bin/udp_reflector -s pcap0:67 -d 10.150.1.254(B):767 -b 25000 &
```

DHCP traffic should now be reflected on the A3 server.

## Active Directory Integration

A complete active directory integration requires that A3 be kept aware of deleted, disabled, and locked accounts. This allows A3 to disconnect a user whose account has been deleted, disabled, or locked. How quickly this takes effect is dependent on the frequency of the scheduled job used to run these scripts.

### Deleted Account

1. Create the script **unreg\_node\_deleted\_account.ps1** on the Windows Server with the following content. Make sure to change **@IP\_A3** to the IP address of your A3 server's VIP address (B). The user name and password must match the credentials defined in the A3's administrative interface under **Configuration > Integration > Web Services**.

```
#####
#Powershell script to unregister deleted Active Directory account based on the UserName.#
#####

Get-EventLog -LogName Security -InstanceId 4726 |
  Select ReplacementStrings,"Account name"|
  % {
    $url = "https://@IP_A3:9090/"
    $username = "admin" # Username for web services
    $password = "admin" # Password for web services
    [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
    $command = '{"jsonrpc": "2.0", "method": "unreg_node_for_pid", "params": ["pid",
      "'+$_.ReplacementStrings[0]+'"]}'

    $bytes = [System.Text.Encoding]::ASCII.GetBytes($command)
    $web = [System.Net.WebRequest]::Create($url)
    $web.Method = "POST"
    $web.ContentLength = $bytes.Length
    $web.ContentType = "application/json-rpc"
    $web.Credentials = new-object System.Net.NetworkCredential($username, $password)
    $stream = $web.GetRequestStream()
    $stream.Write($bytes,0,$bytes.Length)
    $stream.close()

    $reader = New-Object System.IO.Streamreader -ArgumentList
      $web.GetResponse().GetResponseStream()

    $reader.ReadToEnd()
    $reader.Close()
  }
}
```

2. Create the scheduled task based on an event ID in **Start > Run > Taskschd.msc, Task Scheduler > Task Scheduler Library > Event Viewer Task > Create Task**. Settings:

Field	Usage
General	Name: A3-Unreg_node-for-deleted-account Check: Run whether user is logged on or not Check: Run with highest privileges
Triggers > New	A further Begin on the task: On an event Log: Security Source: Microsoft Windows security auditing. Event ID: 4726
Actions > New	Which actions this type of admin can Action: Start a program Program/script: powershell.exe Add arguments (optional): C:\scripts\unreg_node_deleted_account.ps1
Settings	Run a new instance in parallel

3. Validate with Ok and designate the account that will run this task. (Usually DOMAIN\Administrator)

## Disabled Account

1. Create the script **unreg\_node\_disabled\_account.ps1** on the Windows Server with the following content. Make sure to change **@IP\_A3** to the IP address of your A3 server. The user name and password must match the credentials defined in the A3 administrative interface under **Configuration > Integration > Web Services**.

```
#####  
#Powershell script to unregister disabled Active Directory account based on the UserName.#  
#####  
  
Get-EventLog -LogName Security -InstanceId 4725 |  
  Select ReplacementStrings,"Account name"|  
  % {  
    $url = "https://@IP_A3:9090/"  
    $username = "admin" # Username for the webservices  
    $password = "admin" # Password for the webservices  
    [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}  
    $command = '{"jsonrpc": "2.0", "method": "unreg_node_for_pid", "params": ["pid",  
      "'+$_.ReplacementStrings[0]+'"]}'  
  
    $bytes = [System.Text.Encoding]::ASCII.GetBytes($command)  
    $web = [System.Net.WebRequest]::Create($url)  
    $web.Method = "POST"  
    $web.ContentLength = $bytes.Length  
    $web.ContentType = "application/json-rpc"  
    $web.Credentials = new-object System.Net.NetworkCredential($username, $password)  
    $stream = $web.GetRequestStream()  
    $stream.Write($bytes,0,$bytes.Length)  
    $stream.close()  
  
    $reader = New-Object System.IO.Streamreader -ArgumentList  
      $web.GetResponse().GetResponseStream()  
    $reader.ReadToEnd()  
    $reader.Close()  
  
  }
```

2. Create the scheduled task based on an event ID in **Start > Run > Taskschd.msc, Task Scheduler > Task Scheduler Library > Event Viewer Task > Create Task**. Settings:

Field	Usage
General	Name: A3-Unreg_node-for-disabled-account Check: Run whether user is logged on or not Check: Run with highest privileges
Triggers > New	Begin on the task: On an event Log: Security Source: Microsoft Windows security auditing. Event ID: 4725
Actions > New	Action: Start a program Program/script: powershell.exe Add arguments (optional): C:\scripts\unreg_node_disabled_account.ps1
Settings	Run a new instance in parallel

3. Validate with Ok and designate the account that will run this task. (Usually DOMAIN\Administrator)

## Locked Account

1. Create the script **unreg\_node\_locked\_account.ps1** on the Windows Server with the following content. Make sure to change **@IP\_A3** to the IP address of your A3 server. The user name and password must match the credentials defined in the A3 administrative interface under **Configuration > Integration > Web Services**.

```
#####  
#Powershell script to unregister locked Active Directory account based on the UserName.#  
#####  
  
Get-EventLog -LogName Security -InstanceId 4740 |  
  Select ReplacementStrings,"Account name"|  
  % {  
    $url = "https://@IP_A3:9090/"  
    $username = "admin" # Username for the webservices  
    $password = "admin" # Password for the webservices  
    [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}  
    $command = '{"jsonrpc": "2.0", "method": "unreg_node_for_pid", "params": ["pid",  
      "'+$_.ReplacementStrings[0]+'"]}'  
  
    $bytes = [System.Text.Encoding]::ASCII.GetBytes($command)  
    $web = [System.Net.WebRequest]::Create($url)  
    $web.Method = "POST"  
    $web.ContentLength = $bytes.Length  
    $web.ContentType = "application/json-rpc"  
    $web.Credentials = new-object System.Net.NetworkCredential($username, $password)  
    $stream = $web.GetRequestStream()  
    $stream.Write($bytes,0,$bytes.Length)  
    $stream.close()  
  
    $reader = New-Object System.IO.Streamreader -ArgumentList  
      $web.GetResponse().GetResponseStream()  
  
    $reader.ReadToEnd()  
    $reader.Close()  
  
  }
```



2. Create the scheduled task based on an event ID in Start > Run > Taskschd.msc. Task Scheduler > Task Scheduler Library > Event Viewer Task > Create Task. Settings:

Field	Usage
General	Name: A3-Unreg_node-for-locked-account Check: Run whether user is logged on or not Check: Run with highest privileges
Triggers > New	Begin on the task: On an event Log: Security Source: Microsoft Windows security auditing. Event ID: 4740
Actions > New	Action: Start a program Program/script: powershell.exe Add arguments (optional): C:\scripts\unreg_node_locked_account.ps1
Settings	Run a new instance in parallel

3. Validate with Ok and designate the account that will run this task. (Usually DOMAIN\Administrator)

# A3 Troubleshooting

This chapter discusses the means by which A3 problems can be diagnosed. This chapter assumes that troubleshooting will be performed by IT professionals with experience in network diagnostics and A3 administration. All navigation and settings used in this chapter refer to the A3 administrative interface unless otherwise specified.

## Administration

---

### Unable to Run A3 Administration

1. Check the URL for A3 administration using the VIP address. For example: `https://10.150.1.254:1443 (B)`. An `https://` prefix is required.
  - a. Check that you are using the correct VIP address as entered in [Initial A3 Configuration](#).
  - b. Check that the address is not covered by a local DHCP server.
2. Check access via the direct address of the A3 cluster member. For example `https://10.150.1.4:1443 (A)`. If this succeeds, then get the VIP address (B) from `Configuration > Network Configuration > Interfaces` and try step 1 again.
3. Check that the virtual machine hosting A3 is running and has at least 16 GB of memory.

### Browser Complains That A3 Is Unsafe

1. See [A3 Server Certificate](#) in [Initial A3 Configuration](#) if the client's browser complains about an unsafe site.

### Internet Explorer Cannot Display the A3 Admin Page

1. Internet Explorer versions 8 through 10 may raise an "Internet Explorer cannot display the webpage" error while attempting to access A3 administration interface.
2. Internet Explorer 11 or later must be used for A3 administration.

### Changes Don't Take Effect

1. If there are any **Restart ...** buttons at the bottom of the page where changes were made, make sure to use them.
2. If you're not sure, then use the **Restart All** button on the `Status > Services` page.
3. Within clusters services must be individually restarted on each A3 member.
  - a. Log into the administrative instance for each A3 member using its individual address, not the VIP address.
  - b. Restart the appropriate or all services on each member.
  - c. Wait for services have restarted on each member.

## The Auditing Tab

---

The Auditing tab and RADIUS Debug feature A3 are two of the most valuable troubleshooting tools. Since they are used in most troubleshooting techniques, they are described here and referenced where used.

1. Use the Auditing page to determine if the AP and A3 are communicating correctly and what information A3 is returning to the AP. Select **Auditing > RADIUS Audit Logs**.
  - a. Clicking on a RADIUS log entry for the MAC address of the client in the correct time frame. The page may require a refresh. The **Auth Status** column may show **Reject** or **Accept** for the client. If there is no current entry for the MAC address skip to the next step.
  - b. On the Device Information tab confirm that the Wi-Fi Network SSID is correct.
  - c. On the RADIUS tab,
    - i. If the entry for the MAC address was **Reject**, then look for the error reply.
    - ii. If the entry for the MAC address was **Accept**, note the **Filter-Id** in the **RADIUS Reply**. This is the value that A3 returned to ExtremeCloud IQ.
2. If the Auditing page had no timely entry for the client's MAC address, then use the **Tools > RADIUS Debug** tool's Log **Viewer** facility.
  - a. Leave all fields blank or enter the Client MAC address.
  - b. START the viewer.
  - c. Try the client authentication.
  - d. STOP the viewer.
  - e. Look for errors, especially shared secret failures.

## Getting Started

---

### Clients Don't See Captive Web Portal

#### Basic Issues

1. Recall that if a client has already been authenticated that the authentication must be cleared from A3. Use the following steps:
  - a. Navigate to **Configuration > Clients**.
  - b. Double click on the line corresponding to the client. The client should show a **registered** status.
  - c. Make the following changes to the entry:
    - i. Owner to **default**.
    - ii. Status to **Unregistered**.
    - iii. Role to **No Role**.
  - d. Select **Save**.
2. Check that the client is connected to the appropriate SSID.
3. Use the Auditing tab as described in [The Auditing Tab](#).

4. Check that the SSID is used in the Connection Profile and that the profile uses external authentication sources.
5. Check in ExtremeCloud IQ that the AP has been set up with a **default user profile** that uses the registration VLAN.
6. Check that the client's IP address is in the range associated with the registration VLAN by using **ipconfig** on the client.
7. In most cases, the client's default web browser will pop up with the CNP (captive network assistant) display. Some browsers, however, will require further "encouragement". Use a well known URL (such as <http://cnn.com>) to force the CWP. When using such a URL, make sure to type all of http:// since the browser may auto-complete the entry with https://)
8. See [A3 Server Certificate](#) in [Initial A3 Configuration](#) if the client's browser complains about an unsafe site.

### VLAN Setup is Incorrect

1. Use the Auditing tab as described in [The Auditing Tab](#).
2. Check that the registration VLAN has been setup in A3.
  - a. The VLANs were configured during [Initial A3 Configuration](#), during [Setup IP Addresses](#).
  - b. The VLANs can be viewed and adjusted at **Configuration > Network Configuration > Networks > Interfaces**.
3. VLAN setup can be further checked using **Tools > Netstat, Display routing table information** or **Tools > IP Configuration, Display IP configuration**:
  - a. Each of the registration and isolation networks should be listed. For example, 10.100.100.0 in the examples used in this guide.
  - b. The Iface column will also show the eth interface used for each.
  - c. For each Domain that has been joined, a new interface named **<Domain Name>-b** will be listed.
4. Check that switches, routers, and VPN devices have been correctly configured to connect the access point to A3 using the registration VLAN.
5. ExtremeCloud IQ's VLAN probe utility (**Manage > Tools > Utilities > VLAN Probe**) can be used to see if appropriate VLANs are set up at the access point. Limit the range of VLANs probed to save time.
6. Check layer 3 connectivity in a layer 3 deployment using A3's traceroute (**Tools > Traceroute**). Check that A3 is able to reach the far end routers.
7. A3's **Tcpdump (Tools > Tcpdump)** may be needed to further diagnose problems.
  - a. Select the registration network, either **eth0.<reg VLAN #>** if a port group is used or **eth<#>** if a separate interfaces was use. Otherwise leave all other fields blank.
  - b. Run Tcpdump while the client attempts a registration.
  - c. Download the dump and use a display utility, such as **Wireshark**, to inspect the results.
  - d. Look for DHCP discover messages to A3 to establish VLAN connectivity.

# Authentication Issues

---

## Clients No Longer See CWP

1. Recall that if a client has already been authenticated that the authentication must be cleared from A3. Use the following steps:
  - a. Navigate to **Configuration > Clients**.
  - b. Double click on the line corresponding to the client. The client should show a **registered** status.
  - c. Make the following changes to the entry:
    - i. Owner to **default**.
    - ii. Status to **Unregistered**.
    - iii. Role to **No Role**.
  - d. Select **Save**.

## Clients Cannot Successfully Authenticate with the CWP

1. See [Clients No Longer See CWP](#) with respect to multiple authentication attempts.
2. If you are unsure whether services were restarted after an Active Directory, restart all services now.
3. If email, SMS, or sponsored authentication is being used check that [Alerting](#) has been setup. Test the alerting setup with **Tools > SMTP** test.
4. Use the **Tools > Authentication Test** tool.
  - a. Check each Authentication Source in the order listed in the Connection Profile to see which one is matched.
  - b. If **Username** or **Password** is not applicable to a particular type of authentication, just fill in nonsense.
  - c. Note that if the Authentication Source is filtered by an SSID in a **Condition** for an **Authentication Rule**, then the Authentication Test tool will fail.
5. If Domain-based authentication is used, recheck domain setup.
  - a. Use **Tools > NTLM Authentication** to check if the client's name and password are correct. The diagnostics available with this tool are more illuminating than with other methods.
  - b. Check that the Domain join is still valid. In **Configuration > Active Directory Domains**, use the **Unjoin** and **Rejoin** buttons to check. Remember that you'll need administrative credentials to complete the Rejoin.

## Clients Cannot Use Social Login Authentication

1. Check Authentication Sources for each of the social login sources. The **Authorized Domain** setting should include a comma separated list of domains used by the social login site. Check the list against A3's online help.
2. The domains used by social login sites can change over time. Check the URL of the social login site that failed and add its domain to the authentication source's **Authorized Domain** list.


## Some Clients Cannot Join with Active Directory Authentication

1. In a cluster configuration, each A3 member must individually perform a JOIN operation with the Active Directory. Make sure that this is the case by using the Join/Rejoin button on the Configuration > Active Directory Domains page. Remember that you'll need administrative credentials to complete the operation.
2. Recheck domain setup.
  - a. Use **Tools > NTLM Authentication** to check if the client's name and password are correct. The diagnostics available with this tool are more illuminating than with other methods.
  - b. Check that the Domain join is still valid. In **Configuration > Active Directory Domains**, use the **Unjoin** and **Rejoin** buttons to check. Remember that you'll need administrative credentials to complete the Rejoin.

## Post-Authentication Issues

---

### Clients Assigned to Incorrect Role

1. Recheck Role, Device, Authentication Sources, and Connection Profile settings. Refresh A3's UI for the individual pages to ensure that there have been no browser-related mixups.
2. Recall that if a client has already been authenticated that the authentication must be cleared from A3. Use the following steps:
  - a. Navigate to **Configuration > Clients**.
  - b. Double click on the line corresponding to the client. The client should show a  status.
  - c. Make the following changes to the entry:
    - i. Owner to **default**.
    - ii. Status to **Unregistered**.
    - iii. Role to **No Role**.
  - d. Select **Save**.
3. Check that the client is connected to the appropriate SSID.
4. Check the order in which Authentication Sources are defined in the Connection Profile. These are used in the order in which they are listed. An earlier source may match resulting in an unanticipated role assignment.
5. Use the **Tools > Authentication Test** tool.
  - a. Check each Authentication Source in the order listed in the Connection Profile to see which one is matched.
  - b. If **Username** or **Password** is not applicable to a particular type of authentication, just fill in nonsense.
  - c. Note that if the Authentication Source is filtered by an SSID in a **Condition** for an **Authentication Rule**, then the Authentication Test tool will fail.
6. Check the Device's Roles assignments.
  - a. Navigate to **Configuration > Policies and Access Control > Devices**.
  - b. Select the AP, then **Roles** tab.

- c. Check that **Role by Device Role** is exclusively selected.
  - d. Check that the role name filled into the form matches exactly (including case) that defined in ExtremeCloud IQ.
  - e. The ExtremeCloud IQ setting is located in the **Wireless Network's User Profile settings** under **Assignment Rules**. The **Type** field should be **RADIUS Attribute** and the **Value** should match that used in A3.
7. Use the Auditing tab as described in [The Auditing Tab](#).

## Authenticated Clients Can't Access Internet or Local Sites

If authenticated users cannot access the intended local or internet sites, use one or more of the following techniques:

1. On the client, use **ipconfig** to check that the client has been assigned to the network associated with their production VLAN, and that the gateway is correct. If this is incorrect, see [Clients Assigned to Incorrect Role](#).
2. In layer 2 deployments, use the **ping** utility in A3 to check if there is a systemic network problem that would limit access. Note that **ping** does not always work even when a site is accessible; sites may refuse to respond to ping (ICMP echo) requests.
3. Use ExtremeCloud IQ's **ping** command to test from the perspective of the AP:
  - a. Navigate to Manage > Tools > Utilities.
  - b. Select Device Diagnostics from the drop-down list.
  - c. Check the box beside the AP of concern.
  - d. Click on **DIAGNOSTICS**.
  - e. Select ping.
4. If the **ping** test fails, try using **traceroute** from A3 and/or ExtremeCloud IQ.

## Cluster Problems

1. If all A3 operations stop, refer to [Graceful Shutdown and Restart](#) and [Cluster Backup and Recovery](#) for suggestions.
2. Failure of one or more, but not all, cluster members may be evident from:
  - Slow client authentication
  - Inability to perform configuration updates in the administration GUI
  - A red warning in the administration GUI

The identity of the failed cluster member may be viewed in Configuration > System Configuration > Cluster. Take whatever steps are necessary to restart the cluster members. Normal operation should ensue after all members are completely restarted.

If a member cannot be restarted and must be reloaded, refer to [Cluster Backup and Recovery](#) for suggestions.

# Glossary

Term	Definition
1X	See 802.1X.
802.1X	The IEEE 802.1X standard defines how to provide authentication for devices trying to connect with other devices on LANs or wireless LANs.
<b>- A -</b>	
A3	Extreme Networks software product for authentication, authorization, and accounting. Works in conjunction with Extreme Networks APs and many switches.
A3 services	Software processes running on A3 that perform both internal tasks and interfaces with external services.
access control list	A list of permissions associated with a network connection.
access network	The means by which a client enters the corporate network. This is usually an AP, Wi-Fi controller, or enterprise switch.
ACL	See access control list.
Active Directory	Microsoft's name for an LDAP directory that holds information about corporate organization, users, machines, and devices.
administration rules	Administration rules dictate what administrative privileges will be granted to the user when an authentication source is applied.
AdminProxy	An authentication mechanism used in Microsoft systems for administrator single sign-on.
agent	In the context of A3, a user agent is a client-resident component that aids in certificate deployment and authentication.
alert	An email, sms, or other message sent to one or more administrators triggered by a security event or other action.
Android	An open-source operating system used for smart phones and tablets.
AP	See access point.
Apache	The name of a web server often distributed with Linux-based systems, in particular A3.
auditing	The process of reviewing details of transpired connections.
authentication	The process of verifying a user's identity.
authentication module	A captive portal module used to perform a particular type of authentication.
authentication rules	Authentication rules are associated with most authentication sources. They dictate what actions are performed when the authentication source is triggered.
authentication server	A server or service that validates user credentials.
authentication source	The means by which a user is authenticated. These can be internal, external, billing, and exclusive authentication sources.
authenticator	A device that enforces authentication, only allowing properly identified clients to access the network. Often an Extreme Networks AP.
AuthorizeNet	See billing authentication.



Term	Definition
------	------------

**- B -**

BaracudaNG	See firewall.
billing authentication	Authentication after paying for service with a payment provider, such as Paypal.
billing module	A captive portal module that is used to perform billing operations as part of the client authentication process.
billing tier	A level of usage for billing purposes. For example, Gold, Silver, and Bronze tiers that provide lower bandwidth at each step.
Blackhole	An authentication mechanism that denies authentication for the client. This can be used to deny clients access that would otherwise be granted.

**- C -**

CA	See certificate authority.
captive web portal	A set of web pages offered to users in lieu of their requested web site. The CWP is used to perform authentication with users.
certificate	See x.509 certificate.
certificate authority	An entity that generates x.509 certificates. These can be commercial entities such as RSA, or organization's own mechanisms.
chained module	A captive portal module that is used to step through a number of other modules in order.
Checkpoint	See firewall.
choice module	A portal module that offers clients a choice of authentication methods or procedures.
Cisco Mobile Services Engine	A software agent resident on access points and other devices as part of CMSE.
CLI	See command line interpreter.
client	A person or device seeking access to a network.
client certificate	An x.509 certificate issued to a client.
cluster	The use of multiple computer systems, each running the same software to share load and to provide graceful degradation in the face of failure.
CMSE	See Cisco Mobile Service Engine.
comma-separated values	A file type in which the fields are separated by commas or other designated character.
command line interpreter	An interface to a network device that relies on command line instructions.
common name	Used in certificates, usually the host plus domain name. E.g. www.yoursite.com.
compliance	The requirement that clients and devices conform to rules related to operating system, update status, and vulnerability protection.
connection profile	Connection profiles tie access points together with the authentication sources and captive portal to be used.
content security policy	A set of security policies that detects and mitigates certain types of attacks.
CSP	See content security policy.
CSV	See comma-separated values.
CWP	See captive web portal.

**- D -**

deployment	The manner in which a network service, such as A3 is included in a larger network.
device	A client or network component. In A3, it specifies access network components.
device group	A shorthand technique for defining A3 devices; a group of settings related to a type of device. For example, Extreme Networks APs.
device parking	The process of putting devices that are not able to register in a low overhead state.
device profile	Used in Fingerbank, a profile of a device in terms of DHCP data items.

Term	Definition
DHCP	See dynamic host control protocol.
DHCP Option82	A DHCP option that allows a controller to act as a DHCP relay agent to prevent DHCP clients requests from untrusted sources.
DHCP relay agent	A software component that accepts and forwards DHCP requests via layer 3 messages to a remote DHCP server.
distinguished name	A DN is also a fully qualified path of names that trace the entry back to the root of an LDAP/AD tree.
DN	See distinguished name.
DNS	See domain name service.
domain	A Windows domain is a form of a computer network in which all user accounts, computers, printers and other security principals, are registered with a central database.
domain name service	A service that translates network names (such as www.google.com) to IP addresses.
dot1X	See 802.1X.
dynamic host control protocol	A software server that hands out IP addresses in response to client requests using the DHCP protocol.

**- E -**

EAP	See extensible access protocol.
EAP-FAST	The Flexible Authentication via Secure Tunneling (FAST) protocol establishes a tunnel without the need for client or server certificates. See EAP.
EAP-GTC	A technique used in conjunction with Generic Token Cards In this method, the RADIUS server sends a challenge to the security token on the client. The response is sent back and validated by the server. See EAP.
EAP-MD5	An older technique that uses an MD5 hash to authenticate the client to the RADIUS server, but not vice versa. It is currently deprecated. See EAP.
EAP-TLS	Requires client certificates. The client and server perform mutual authentication and form encryption keys based on certificate contents. See EAP.
EAP-TTLS	The Tunneled Transport Layer Security (TTLS) protocol extends TLS. The client need not be authenticated initially by the server using a certificate, although the server's certificate is used by the client. See EAP.
E-CWP	See external captive web portal.
eduroam	Eduroam is a global wireless network access service for research and education.
email authentication	Authentication via a CWP that sends an email message to a client. The client must click on a link in the email to complete authentication.
enforcement	The process of implementing an authentication decision. This is often done in APs and switches.
ESXi	VMware ESXi is an operating system-independent hypervisor based on the VMkernel operating system that interfaces with agents that run on top of it.
exclusive authentication	A set of miscellaneous authentication techniques in A3. An exclusive authentication technique must be used by themselves.
extensible access protocol	The EAP framework makes possible a number of methods for secure exchange of identity.
external authentication	Authentication sources that perform user identification through the captive web portal or other Web interface where the A3 owner does not control the information.
external captive web portal	A captive portal invoked from the access device rather than A3.
ExtremeCloud IQ	A cloud-based service for management of Extreme Networks devices, including APs.

**- F -**

Term	Definition
Facebook	See social login.
filter engine	An A3 file that is used to process information from VLAN, RADIUS, Apache, DHCP, DNS, and devices.
Fingerbank	A shared database of DHCP fingerprints that identify devices.
fingerprint	In Fingerbank, a specification of the DHCP-specific options handled by a device - which can be used to identify the device type, vendor, or model.
firewall	Network software that denies, permits, or restrict access from one side of a network to another. A3's firewall integration can be used to implement single-sign on (SSO).
FortiGate	See firewall.

**- G -**

Github	See social login.
Google	See social login.

**- H -**

headless IoT devices	Devices that lack an interactive interface, requiring special authentication techniques.
HiveManager	A deprecated name for ExtremeCloud IQ.
Htpassword	An authentication technique that uses a flat file with name and password commonly used in basic authentication on Apache HTTP servers.
HTTP	See hypertext transport protocol.
hypertext transport protocol	The communications protocol on which the Web is based. HTTP sets rules for how information is passed between the server and the browser software.

**- I -**

Iboss	See firewall.
IDS	An intrusion detection system detects network traffic and system modifications due to malicious traffic.
intrusion detection system	See IDS.
IoT	Internet of Things. See headless IoT devices.
Instagram	See social login.
integration	In A3, the process by which third-party networking products are integrated into A3 operation.
internal authentication	Authentication sources that use internal information and servers. In this case, the A3 owner controls the authentication data.
internet of things	See IoT.
isolation	The process of placing devices that have been refused authentication on an isolated network so that they may repair any problem.

**- J -**

jamf	A commercial Apple management solution for IT.
JSON RPC	See firewall.
JuniperSRX	See firewall.

**- K -**

Kerberos authentication	Authentication using the Kerberos protocol and associated services.
Kickbox	See social login.

**- L -**

Term	Definition
layer 2	A layer in the OSI network stack that utilizes local network communications using MAC addresses.
layer 3	A level in the OSI network stack where communications occur based on IP addresses across multiple networks.
LDAP	See lightweight directory access protocol
lightweight directory access protocol	A protocol that provides access to hierarchically organized data bases such as Active Directory.
LinkedIn	See social login.
load balancer	A device that sits between a service requester and multiple servers, dividing work between the servers.

**- M -**

MAC authentication	A method of authentication whereby clients and devices are associated with their MAC addresses as opposed to directory or certificate contents.
MDM	See mobile device management.
Mirapay	See billing authentication.
mobile device management	A central management systems used to configure, update, and control client devices. These are responsible for ensuring that the correct, updated software is installed on clients. A3 can request client status from such system, restricting client access.
MobileIron	A commercial provisioning tool supported by A3.
MSE	See Cisco Mobile Services Engine.

**- N -**

NAC	See network access control.
Nessus	A commercial scanning tool supported by A3.
netstat	A network tool that reports on network status.
network access control	The technology associated with denying, allowing, and/or restricting access to network resources.
network time protocol	A protocol by which computers obtain the current time from reliable sources.
node	In A3 a node is any client or network device identified during normal or scanning operation.
NTLM	NTLM uses a challenge-response mechanism for authentication, in which clients are able to prove their identities without sending a password to the server.
NTP	See network time protocol.
null authentication	A form of authentication using a CWP in which the user merely agrees to terms of service.

**- O -**

OAuth2	A convention used by multiple social media sites to forward user information on request.
OOB	See out-of-band.
OpenID	See social login.
OpenVAS	A scanning tool supported by A3.
OPSWAT	A vulnerability scanning tool supported by A3.
Option82	See DHCP Option 82.
out-of-band	A network technique where communications is handled by other than the normal in-band communications method.
OVA	A single file distribution of an OVF file package.
OVF	A file format that supports exchange of virtual appliances across products and platforms.

**- P -**

Term	Definition
Palo Alto	See firewall.
parking	See device parking.
passthrough	The ability to allow certain internet address to pass through A3 for the process of authentication.
password of the day	An authentication technique that generates a password on a regular basis. The password is sent to the administrator who distributes it to users.
PayPal	See billing authentication.
PEAP	See protected extensible authentication protocol.
ping	A network tool that measures round-trip message time between systems, using the ICMP protocol.
Pinterest	See social login.
PKI	See public key infrastructure.
portal	See captive web portal.
portal module	Any of a number of modules used to construct a captive web portal site.
POTD	See password of the day.
protected extensible authentication protocol	Encapsulates EAP within a potentially encrypted and authenticated TLS tunnel. Any of the EAP methods may be used within the tunnel.
provisioner	An A3 description of an agent that will set up clients for authentication and communications.
provisioning	A method of automatically providing clients with identification information, certificates, and software.
proxy	An intermediary that sits between clients and the servers that they which to access, usually for buffering or security purposes.
public key infrastructure	The comprehensive system required to provide public-key encryption and digital signature services.
public/private keys	Public and private keys are interrelated such that data encrypted with a public key can only be unencrypted with the corresponding private key, and vice versa.

**- R -**

RADIUS	see Remote Authentication Dial-In User Service.
Rapid7	A scanning system supported by A3.
RBAC	See role-based access control.
realm	A user account location, often a Microsoft domain or internet domain name.
regex	See regular expression.
regexp	See regular expression.
registration	The process by which a device, or node, becomes known to A3 and associated with a user.
regular expression	A special text string for describing a search pattern. You can think of regular expressions as wild cards on steroids.
Remote Authentication Dial-In User Service	A networking protocol that provides centralized Authentication, Authorization, and Accounting management for users who connect and use a network service.
rogue DHCP	A DHCP server on a network not under control of the network administrators.
role	A means of distinguishing users, most often used to match their activity in an organization.
role-based access control	RBAC is used to restrict access to networked resources based on a user's role within the enterprise.
root CA	A self-signed certificate that designates the start of a x.509-based public key infrastructure. A number of well-known public root CAs exist and organizations may create their own.
root CA certificate	An x.509 certificate that identifies a root CA.
root module	The top level portal module used in an authentication tree.

Term	Definition
<b>- S -</b>	
sAMAccountName	The user login name contained in AD/LDAP directories.
SAML authentication	A standard protocol for web browser single sign-on using secure tokens.
scanner	Software used to check computers or networks for vulnerabilities.
SCEP	A protocol used for enrollment and other PKI operations.
security event	Any of a set of programmed exceptions, including scanner-found vulnerabilities, network irregularities, and over usage.
SentinelOne	A scanner supported by A3.
secure socket layer	SSL provides a secure channel between two machines or devices. SSL has been replaced by TLS (transport layer security), but both techniques are often referred to as SSL.
SEPM	See Symantec Endpoint Protection Manager.
server certificate	An x.509 certificate that defines a server to client systems. It also references the certificate authority that generated it.
services	See A3 services.
shared secret	A password shared by two or more communicating entities. A3 and ExtremeCloud IQ use a shared secret for RADIUS communications.
single sign-on	In A3 Firewall single sign-on is an integration in which A3 can inform firewalls of successful authentications that allow firewalls to permit future access without additional authentication.
SMS	Short messaging service - a text messaging service component of most mobile devices.
SMS authentication	A means by which a user receives a personal identification number (PIN) used in an associated web page to authenticate their identity.
SNMP	An application-layer protocol used to manage and monitor network devices and their functions.
social login	A form of single sign-on using existing information from a social networking service such as Facebook, Twitter or Google+, to sign into a third party website instead of creating a new login account specifically for that website.
sponsor email authentication	An authentication technique in which a user fills in identification for himself and a company sponsor. The sponsor receives an email to approve access.
SSL	See secure socket layer.
SSO	See single sign-on.
Stripe	See billing authentication.
supplicant	An entity at one end of a LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link.
Symantec Endpoint Protection Manager	A client-server solution that protects laptops, desktops, and servers in your network against malware, risks, and vulnerabilities.
syslog	Short for system log, it is an aggregation of log messages from many services that can be scanned for problems and auditing.
<b>- T -</b>	
TLS	See secure socket layer.
traceroute	A network utility that displays the route that packets take from a source to a destination.
transport layer security	See secure socket layer.
trigger	A condition that causes actions to occur.
<b>- U -</b>	
user	A person or autonomous device seeking access to a network.
user agent	See agent.

Term	Definition
------	------------

**- V -**

vCenter	VMware vCenter Server is advanced server management software that provides a centralized platform for controlling VMware vSphere environments.
violation	A deprecated term for security events.
VLAN	A group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they can be located on a number of different LAN segments.

**- W -**

WatchGuard	See firewall.
Web Auth	A web-browser API for the creation and use of strong authentication credentials based on public key cryptography.
web services	In A3, the ability of external services to access A3's database.
whitelist	A list of internet addresses that are allowed access despite any other restrictions.
Windows	A Microsoft operating system used on desktop, laptop, and server computers.
Windows Management Interface	A set of specifications from Microsoft for consolidating the management of devices and applications in a network from Windows computing systems.
WISPr	A protocol that allows users to roam between wireless internet service providers in a fashion similar to that which allows cellphone users to roam between carriers.
WMI	See Windows Management Interface.
WRIX	Wireless Roaming Intermediary eXchange is a modularized set of standard service specifications designed to facilitate commercial roaming between operators.

**- X -**

x.509 certificate	A file that documents the identity of an entity, along with a public key that can be used to communicate securely.
-------------------	--

# Index

## Numerics

802.1X .....	48
Authentication Servers .....	49
Authenticator .....	48
Configuration Example .....	54
Supplicants .....	48

## A

A3 cluster virtual IP address .....	26
A3 Configuration .....	55, 122
A3 Configuration Flow .....	53
A3 Installation .....	11
A3 permanent IP address .....	20
A3 permanent virtual IP address .....	20
A3 server address .....	26
A3 Server Certificate .....	30
A3 server domain name .....	20
A3 server name .....	26
access control list .....	9
Access point .....	86
Access Point address .....	26
Access switch .....	26
ACL .....	9
Active Directory .....	42
Authentication .....	102
Domain .....	103
Domain Join .....	102
Server .....	26
Source .....	113
AD .....	42
Addressing	
Layer 2 and Layer 3 .....	27
Layer 3 only .....	28
AdminProxy .....	46
Alerting .....	29
Android Play Store .....	86
Apple devices .....	85
Authentication .....	68
Methods .....	38
Servers .....	49
Sources .....	97, 104, 113
Authenticator .....	48
AuthorizeNet .....	46
Automatic Registration Security Event .....	126



Barracuda	.89
Billing Authentication Sources	.46
AuthorizeNet	.46
Mirapay	.46
PayPal	.47
Stripe	.47
Blackhole	.46

**B**

Captive Web Portal	.20, 86
Certificates	.57
Checkpoint	.90
Cisco ASA	.18
Cisco DPSK	.86
Clickatell	.39
Client networks	.26
Cloud	.28
Clusters	.20, 27
Connection Profile	.67, 85, 98, 106, 114, 118, 123
Corporate Profile	.118
Creating a Local User	.111
CWP	.86

**C**

default_registration_policy	.67
Deployment Modes	.3
Inline Deployment	.6
Layer 3 Across a Routed Network	.4
Devices	.98, 105, 122
DHCP Servers	.19, 26
DHCP relay agent	.4
DNS Servers	.19, 26
DNS setup	.29
Domain and Time Zone	.28
Download A3 Software	.11

**D**

EAP	.49
EAP-TLS	.42
Authentication	.117
Authentication Source	.117
E-CWP	.7, 121
education roaming	.128
eduroam	.46, 128
Authentication Source	.131
Connection Profile	.132
Local Authentication Source	.131
Local Connection Profile	.132
Email	.19
authentication	.97
Authentication Source	.38
employee role	.26

**E**

Enforcement Devices	18
Enforcement Modes	7
RADIUS Enforcement	8
WebAuth (ACL) Enforcement	9
Equipment Requirements	10
Exclusive Authentication Sources	46
AdminProxy	46
Blackhole	46
eduroam	46
External Authentication Sources	38
Email	38
Null	38
SMS	38
Social login	39
Sponsor	38
external captive web portal	7, 121
Extreme Networks Community	10
Extreme Networks Requirements	10
ExtremeCloud IQ	10, 18, 28
A3-Guest	31
A3-Guest-Rule	33
A3-RADIUS	32
A3-RADIUS-SERVER-GROUP	32
Assignment Rule	33
Configuration	31, 54, 55, 121
Corp-Policy	31
Default User Profile	32
Deploy Policy	34
Guest Profile	33
Isolation Profile	33
MAC Authentication	31
Network Policy	31
Open Unsecured	32
RADIUS Server	32
RADIUS Server Group	32
Shared Secret	32

## F

Facebook	39
Fingerbank	75, 86
Firewall Integration	89
Barracuda	89
Checkpoint	90
FortiGate	91
JSON-RPC	93
Palo Alto	94
firewall rules	5
Firewalls	18, 89
Fixed Role	68
FortiGate	91

## G

Github	39
--------	----

Google	40
Google OAuth2 Authentication Test	101
Guest Access Configuration Example	54
Guest Access with Captive Web Portal	96
Guest Profile	118
guest role	26

## H

Headless IoT Devices	125
Htpasswd	42
HTTP	42

## I

IDS	17
Infrastructure Devices	19
DHCP Servers	19
DNS Servers	19
Email	19
Routers	19
Switches	19
Initial A3 Configuration	27
Inline Deployment	6
Instagram	40
Installation	10
A3 Installation	11
Download A3 Software	11
Equipment Requirements	10
Extreme Networks Requirements	10
Instantiation	11
Network Interfaces	11, 13
Internal Authentication Sources	42
Active Directory	42
Authorization	42
EAP-TLS	42
Htpasswd	42
HTTP	42
Kerberos	42
LDAP	42
Password of the Day	42
POTD	42
RADIUS	42
SAML	42
Internet of Things	17
intrusion detection systems	17
iOS	85
IoT	17
Isolation Profile	33

## J

Jamf	86
JSON-RPC	93

Kerberos .....42  
 Kickbox .....40

**K**

Layer 2 or Layer 3? .....19  
 Layer 2 Topology .....25  
 Layer 3 Across a Routed Network .....4  
 Layer 3 Topology .....26  
 LDAP .....18, 42  
 License .....27  
 Lightweight Directory Access Protocol .....18  
 LinkedIn .....40  
 Local User Authentication .....110, 111

**L**

MAC Authentication .....31, 54  
 Management VLAN .....26  
 Manual Use of Security Event .....127  
 marketing role .....26  
 MDM .....18, 85, 86  
 Mirapay .....46  
 Mobile Device Management .....18, 85  
 Mobile Device Managers .....86  
     Cisco DPSK .....86  
     Jamf .....86  
     MobileIron .....87  
     OPSWAT .....87  
     SentinelOne .....88  
     SEPM .....88  
 MobileIron .....87

**M**

NAC .....1  
 Nessus .....76  
 Network Access Control .....1  
 Network Implementation .....24  
 Network Interfaces .....11, 13  
 Network Policy .....31  
 Network Topology .....17, 21  
 Null Authentication .....97  
 Null Authentication Source .....38  
 Null Authentication Test .....124

**N**

OOB .....3, 5  
 OpenID .....41  
 OpenVAS .....76  
 OPSWAT .....87  
 out-of-band .....3, 5  
 OVA .....11  
 OVF .....11

**O**

Palo Alto	.94
Password of the Day	.42
PayPal	.47
Pinterest	.41
PKI	.57, 58
PKI Providers	.86
Portal Modules	.66, 67
Authentication	.68
Connection Profile Settings	.67
default_registration_policy	.67
Fixed Role	.68
Provisioning	.68
Root	.67
Select Role	.68
Source by Authentication Class	.69
Source by Class	.68
Source by Type	.69
POTD	.42
Provisioners	.85
Provisioning	.68, 85
Connection Profiles	.85
Public Key Infrastructure	.57, 58
Public/Private Keys	.58

**P**

RADIUS	.42
RADIUS Enforcement	.8
Rapid7	.77
Realms	.103
Registration and Isolation VLANs	.28
Registration network	.20
relay agent	.4
Restart services	.29
Roles	.97, 104
Root Portal Module	.67
Routers	.19, 26

**R**

sales role	.26
SAML	.42
Scan Engines	.76
Nessus	.76
OpenVAS	.76
Rapid7	.77
secure socket layer	.57
Select Role	.68
self-signed CA	.57
SentinelOne	.88
SEPM	.88
server certificate	.20, 30
Setup IP Addresses and VLANs	.27
Shared secret	.26

**S**

SMS	
authentication	.97
Authentication Source	.38
Test	.100
Social Login	
Clickatell	.39
Facebook	.39
Github	.39
Google	.40
Instagram	.40
Kickbox	.40
LinkedIn	.40
OpenID	.41
Pinterest	.41
Twilio	.41
Twitter	.41
WindowsLive	.41
Social Login Authentication	.51, 98
Social login authentication source	.39
Sponsor Authentication Source	.38
Sponsor Source	.114
Sponsored Access	.113
SSID	.26
SSL	.57
SSL certificate	.20, 30
Stripe	.47
Suplicants	.48
Switches	.19
Symantec Endpoint Protection Manager	.88

## T

Table of Addresses and VLANs	.23, 26
Testing Active Directory	.106
Testing EAP-TLS	.118
Testing E-CWP Access	.123
Testing Local User Authentication	.112
Testing Sponsored Access	.114
trusted CAs	.57
Twilio	.41
Twitter	.41

## U

Use Case 1	
Guest Access with Captive Web Portal	.96
Use Case 2	
Active Directory Authentication	.102
Use Case 3	
Local User Authentication	.110
Use Case 4	
Sponsored Access	.113
Use Case 5	
EAP-TLS Authentication	.117
Use Case 7	

---

Headless IoT Devices .....	125
User Manager .....	110

**V**

vCenter .....	10
virtual Ethernet interfaces .....	11

**W**

WebAuth (ACL) Enforcement .....	9
WindowsLive .....	41

**X**

X.509 Certificates .....	49
--------------------------	----