Hewlett Packard Enterprise believes in being unconditionally inclusive. Terms in this document that are recognized as offensive or noninclusive are used only for consistency with the product. When the product is updated to remove the terms, this document will also be updated.
Table of Contents

Introduction ...................................................................................................................................................... 1
  Purpose of This Guide ................................................................. .......................................................... 1
  Customer Use Cases .......................................................................................................................... 2
ClearPass Overview ......................................................................................................................................... 2
  ClearPass Policy Manager Design Considerations .............................................................................. 2
  ClearPass Guest ........................................................................................................................................ 5
Deploying ClearPass for Wireless Client Authentication ............................................................................. 6
  Configuring ClearPass Policy Manager ............................................................................................... 7
  Integrating ClearPass with Active Directory ...................................................................................... 10
  Connecting ClearPass Server to the Mobility Controller Cluster ....................................................... 16
  Creating a Wireless Authentication Service ......................................................................................... 17
  Creating the Guest Access Self-Registration Page ............................................................................ 19
  Configuring the Mobility Master Captive Portal .................................................................................. 23
  Creating a Service for Guest Access .................................................................................................... 23
  Verifying Wireless Client Connectivity ............................................................................................... 25
Summary ........................................................................................................................................................ 31
Introduction

From the Internet of Things (IoT), to an always-on mobile workforce and bring-your-own-device (BYOD), organizations encounter an increasingly complex IT infrastructure. Mobile, cloud, and IoT have redefined network security and present new challenges and vulnerabilities to the network.

One of the challenges IT faces is implementing network security and policies in a cohesive manner. Network security platforms have disparate management systems that do not communicate with each other and do not give IT administrators easy access to the big picture of what is going on in the network. This lack of integration makes implementing consistent security and access policies difficult.

Aruba ClearPass provides a solution to many of these challenges. ClearPass allows network security policies to be automatically assigned based on user or device role from a central location. This capability ensures that policies are consistent, eliminating the chance of devices having old configurations and minimizing human-introduced errors. The network identifies, authenticates, and grants trust based on the user or device role.

PURPOSE OF THIS GUIDE

This guide provides configuration information for Aruba ClearPass Policy Manager (CPPM) with Microsoft Active Directory (AD) integration for employee and guest wireless clients. It covers the requirements to secure wireless network access for your organization and provides an explanation of those requirements.

The guide provides a simple and secure method for configuring CPPM and integrating AD that is easy to set up and replicate. The configuration addresses the most common use cases and is not intended to be an exhaustive discussion of all options.

Audience

This guide is written for IT professionals responsible for network policy and security for organizations to deploy a centralized network policy. These IT professionals can fill roles such as:

- Systems engineers with network security knowledge, including Microsoft Active Directory, who need a standard set of procedures for implementing AAA solutions.
- Aruba partners with network security knowledge, including Microsoft Active Directory, who sell technology or create implementation documentation.
- Network engineers responsible for wireless network security.
CUSTOMER USE CASES

Employees connect to the organization's network by using company issued devices as well as personal devices (BYOD). The rise of software-as-a-service has led users to expect to access applications and data from any device, in any location. For network security IT professionals, making sure users and devices are secure, and at the same time have an optimal network experience regardless of the location, is important.

This design provides wireless access control for following use cases:

- Wireless clients as the primary access method for employees
- Wireless clients guest access for customers, partners, and vendors

ClearPass Overview

ClearPass is a centrally managed solution for defining network security policy. It pulls in relevant context from multiple sources within an organization, leverages that context to determine the appropriate policy, and then coordinates that policy across multiple enforcement mechanisms. ClearPass integrates with a range of third-party products and solutions to improve user experience and increase security.

With a suite of modules, ClearPass provides a range of options for securing different types of users and devices that access the network. These modules include ClearPass Policy Manager, ClearPass Onboard, ClearPass On-Guard, and ClearPass Guest.

This guide describes ClearPass Policy Manager and ClearPass Guest to deploy the wireless network.

CLEARPASS POLICY MANAGER DESIGN CONSIDERATIONS

CPPM provides user-role and device-based network access control for employees, contractors, and guests across multivendor wired, wireless, and VPN networks. CPPM is the core and foundation of the ClearPass product suite. It supports multiple authentication/authorization sources, single sign-on for users, advanced reporting and troubleshooting, device profiling, basic onboarding, and guest portal services. After the user or device is identified, CPPM can pass user-role or download policy to the network-access device to which the client connects, ensuring the proper policy is applied. You can share user context with third-party systems, further enhancing the security of the network.
Authentication Methods

Authentication is a process of identifying a user through a valid username and password, certificate, or the user’s device MAC address. Aruba Controllers and Aruba Instant support the following authentication methods:

- 802.1X authentication
- MAC authentication
- MAC authentication with 802.1X authentication
- Captive portal authentication
- MAC authentication with captive portal authentication
- 802.1X authentication with captive portal role
- WISPr authentication

This guide describes only the 802.1X and captive portal authentication (for guest access) methods.

802.1X Authentication

802.1X is an Institute of Electrical and Electronics Engineers standard that provides an authentication framework for WLANs. 802.1X uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1X framework that are suitable for wireless networks include EAP-Transport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAP-Tunneled TLS. These protocols allow the network to authenticate the client while also allowing the client to authenticate the network.

802.1X authentication consists of three components:

- The supplicant, or client, is the device attempting to gain access to the network. You can configure the Aruba user-centric network to support 802.1x authentication for wired users and wireless user.

- The authenticator is the gatekeeper to the network and permits or denies access to the supplicants. The Aruba Mobility Controller acts as the authenticator, relaying information between the authentication server and supplicant. Another name for authenticator is network access server (NAS).

- The authentication server provides a database of information required for authentication and informs the authenticator to deny or permit access to the supplicant. The 802.1X authentication server is ClearPass, which is an EAP-compliant remote access dial-in user service (RADIUS) server that can authenticate either users (through passwords or certificates) or client network devices.
EAP data is first encapsulated in Ethernet over LAN (EAPOL) frames between the supplicant and authenticator, then re-encapsulated between the authenticator and the authentication server by using the RADIUS protocol.

**Supported EAP Authentication Frameworks**

Extensible Authentication Protocol (EAP) is an authentication framework, not a specific authentication mechanism. It provides some common functions and negotiation of authentication methods called EAP methods. For a listing of EAP methods, attributes, and RFCs, see the EAP Registry.

This guide uses EAP-PEAP, an 802.1X authentication method that uses a server-side public key to authenticate clients with the server (client certificates are optional). The PEAP authentication creates an encrypted SSL/TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel, ensuring the user credentials are kept secure.

**Note** The EAP type must be consistent between the authentication server (Clear-Pass) and supplicant (wireless client) and is transparent to the authenticator (Mobility Controller).

**Encryption Types**

*Encryption* is the process of converting data into a cryptic format or code when it is transmitted on a network. Encryption prevents unauthorized use of the data. Supported types of encryption are:

- **TKIP**—The Temporal Key Integrity Protocol (TKIP) uses the same encryption algorithm as Wired Equivalent Privacy (WEP). However, TKIP is more secure and has an additional message integrity check.

- **AES**—The Advanced Encryption Standard (AES) encryption algorithm is a widely supported encryption type for all wireless networks that contain any confidential data. AES in Wi-Fi leverages 802.1X or pre-shared key (PSK) to generate per-station keys for all devices. AES provides a high level of security like IPsec clients.
Security Certifications

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless device networks. The Alliance defined these protocols in response to serious weaknesses researchers had found in the preceding system, WEP.

The following table summarizes the recommendations for authentication and encryption combinations for the Wi-Fi networks.

Table 1  Recommended authentication and encryption combinations

<table>
<thead>
<tr>
<th>Network type</th>
<th>Security type</th>
<th>Authentication</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>WPA2 Enterprise</td>
<td>EAP-PEAP</td>
<td>AES</td>
</tr>
<tr>
<td>Guest network</td>
<td>Open</td>
<td>Captive portal</td>
<td>None</td>
</tr>
<tr>
<td>Voice network or handheld devices</td>
<td>WPA (if required for legacy device support) or WPA2 Enterprise</td>
<td>802.1X or PSK as supported by the device</td>
<td>AES if possible, TKIP if necessary (with security settings assigned for a device role)</td>
</tr>
</tbody>
</table>

CLEARPASS GUEST

ClearPass Guest enables customers, contractors, and other visitors to gain secure guest access to wireless and wired networks. ClearPass Guest creates a rich experience for guests that is easy to manage and administer, allowing automated or supervised guest access and differentiated policies for each type of guest. ClearPass Guest features full-featured enterprise workflows that allow for full audit trails to answer who/what/when/where/why/how visitors and their devices access the network, without IT interaction.

Guest Manager features for managing guest accounts let you:

- View and manage active sessions.
- Create single or multiple guest accounts and receipts.
- Create and edit bulk accounts.
- Export a list of accounts.
- Import new accounts from a text file.
- View guest accounts and edit individual or multiple guest accounts.
- View and edit individual or multiple MAC addresses of devices.
You can also customize many features. This guide describes the configuration of self-registration for guest clients.

**Note**  ClearPass Guest is bundled in CPPM version 6.7 and later.

### Deploying ClearPass for Wireless Client Authentication

ClearPass provides a centrally managed solution for defining network security policy. ClearPass pulls in relevant context from multiple sources within an organization, leverages that context to determine the appropriate policy, and then coordinates that policy across multiple enforcement mechanisms. Figure 2 shows the typical place in a network for ClearPass deployment.

**Figure 2**  *Typical ClearPass placement in the network*
The following procedures describe configuring ClearPass to integrate with Active Directory for employee and guest wireless access.

### Procedures

**Configuring ClearPass Policy Manager**

1.1 Set Up ClearPass  
1.2 Set up Activation and License Installation

ClearPass Policy Manager is available as a hardware appliance or a virtual appliance. To increase scalability and redundancy, you can deploy these appliances as a cluster.

For information about installing hardware virtual appliances, see [Setting Up the ClearPass Hardware Appliances](#).

For more information about installing virtual appliances, see [Installing or Upgrading to ClearPass 6.7 on a Virtual Machine](#).

#### 1.1 Set Up ClearPass

You first configure the system setup for the ClearPass platform. Use the information from the following table in the procedures below.

**Table 2 Example ClearPass and Active Directory IP addresses**

<table>
<thead>
<tr>
<th>Device</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClearPass</td>
<td>10.2.120.10/24</td>
</tr>
<tr>
<td>Active Directory</td>
<td>10.2.120.40</td>
</tr>
</tbody>
</table>
Step 1: Open a console session on the ClearPass server and complete the initial configuration.

Enter hostname: Example-CPPM
Enter Management Port IP Address: 10.2.120.10
Enter Management Port Subnet Mask: 255.255.255.0
Enter Management Port Gateway: 10.2.120.1
Enter Data Port IP Address:
Enter Data Port Subnet Mask:
Enter Data Port Gateway:
Enter Primary DNS: 10.2.120.40
Enter Secondary DNS:
New Password: [password]
Confirm Password: [password]

Do you want to configure system date time information? [y|n] y

Please select the date time configuration options.

1) Set date time manually
2) Set date time by configuring NTP servers

Enter the option or press any key to quit: 2
Enter Primary NTP Server: 10.2.120.40
Enter Secondary NTP Server:
Do you want to configure the timezone? [y|n]: y

Step 2: Configure the time zone.

Step 3: Complete the remaining steps of the configuration.

Do you want to enable FIPS Mode? [y|n]: n

Proceed with the configuration [y[Y]/n[N]/q[Q]]
y[Y] to continue
n[N] to start over again
q[Q] to quit

Enter the choice: y
1.2 Set up Activation and License Installation

Step 1: In a web browser, navigate to the management IP address for ClearPass, and then click ClearPass Policy Manager.

Step 2: In the ClearPass Platform Action Key window, enter your license key, and then click Add License.

Step 3: In the Admin Login window, enter the following information, and then click Log In.
   - Username—admin
   - Password—[password]

Step 4: Click the Activate Now hyperlink, and then in the Online Activation window, again click Active Now.

Step 5: After the “Product has been successfully activated” message appears, repeat Step 3 and log in.

Step 6: Navigate to Administration > Server Manager > Licensing, and then click Add License.

Step 7: In the Add License window, select the product, enter your license key, and then click Add.

Step 8: Repeat Steps 6-7 for any additional license keys.
Integrating ClearPass with Active Directory

2.1 Join the Active Directory Domain

2.2 Install RADIUS Certificate

2.3 Create a User Account for ClearPass

2.4 Add Active Directory as an Authentication Source for ClearPass

This section details how to use Microsoft Active Directory as the primary method of user authentication by integrating it with ClearPass Policy Manager. Joining ClearPass Policy Manager to an Active Directory domain allows the administrator to authenticate users and devices that are members of an Active Directory domain. Users can then authenticate to the network using 802.1X and PEAP-MSCHAPv2 with their Active Directory credentials. You must join ClearPass Policy Manager to the domain from an account that has the ability to join a device to the domain.

When performing PEAPv0+MSCHAPv2 authentication, ClearPass negotiates and uses the highest Server Message Block (SMB) protocol version that is supported by the ClearPass server when joining an Active Directory domain. Currently, ClearPass supports SMBv1, SMBv2, and SMBv3 protocols. When performing EAP-PEAP-MS-CHAPv2 authentication, ClearPass uses NT LAN Manager (NTLM). To use NTLM, ClearPass must have Active Directory domain membership.

The Microsoft Active Directory server acts as the domain controller and is responsible for responding to requests for authentication from users and device accounts (for example, logging in and checking permissions) within the Windows Server domain.

2.1 Join the Active Directory Domain

Step 1: In ClearPass Policy Manager, navigate to Administration > Server Manager > Server Configuration, and then click Set Date & Time.

Step 2: Select Synchronize time with NTP server, and then click Save.

Step 3: Navigate to Administration > Server Manager > Server Configuration, and then click the ClearPass server name. For example, Example-CPPM.

Step 4: In the Server Configuration window, click Join AD Domain.
Step 5: In the Join AD Domain window, enter the following information, and then click **Save**.

- Domain Controller—*dc01.example.local*
- Password—*[password]*

Step 6: When the **Added host to the domain** message appears in the Join AD Domain window, click **Close**.

![Join AD Domain](image)

Step 7: In the Server Configuration window, enter the following information for the ClearPass server.

- Hostname—*Example-CPPM*
- FQDN—*example-CPPM.example.local*

Step 8: Click **Save**, and then click **Close**.

### 2.2 Install RADIUS Certificate

It is good practice to use SSL to establish a secure connection between Active Directory and ClearPass. To use SSL, you must install and verify an AD server certificate on the ClearPass server.

Step 1: Navigate to **Administration > Certificates > Certificate Store** and then click **Create Certificate Signing Request**.
Step 2: In the Create Certificate Signing Request window, enter the following information, and then click Submit.

- Common name—radius.example.local
- Private key password—[password]
- Verify private key password—[password]

Step 3: In the Create Certificate Signing Request window, click Download CSR.

**Caution** Do not close the Create Certificate Signing Request window. You will need to access the information in this window to complete Step 10 later in this procedure.

Step 4: Open a web browser, navigate to the Certificate Authority by using http://<ip address of AD server>/certsrv, and then log in.

**Note** Make sure Certification Authority Web Enrollment and IIS roles are installed.
Step 5: In the Welcome window, click Download a CA certificate, certificate chain, or CRL.

Step 6: In the Download a CA certificate, certificate chain, or CRL window, under Encoding method, select Base 64.

Step 7: Click Download CA certificate, and then click Home.

Step 8: In the Welcome window, click Request a certificate.

Step 9: In the Request a Certificate window, click advanced certificate request.

Step 10: In the Submit a Certificate Request or Renewal Request window, copy and paste the text found in the Create Certificate Signing Request window from Step 3 into the Saved Request box.

Step 11: In the Certificate Template field, select Web Server, and then click Submit.

Step 12: In Certificate Issued window, select Base 64 encoded, and then click Download certificate.

Step 13: Return to the on ClearPass Create Certificate Signing Request window and then click Close.

Step 14: Navigate to the Administration > Certificates > Trust List and then click Add.

Step 15: In the Add Certificate window, click Choose File, select certnew.cer from the list of downloaded certificates, and then click Add Certificate.

Step 16: Navigate to the Administration > Certificates > Certificate Store and then click Import Certificate.

Step 17: In the In the Import Certificate window, enter the following information, and then click Import.

- Certificate type—Server Certificate
- Server—Example-CPPM
- Type—RADIUS/EAP Server Certificate
- Upload method—Upload Certificate and Use Saved Private Key
- Certificate file—certnew(1).cer (for Windows) or certnew-1.cer (for Macintosh)

In the Certificate Store window, the message “Server Certificate updated successfully” appears.
2.3 Create a User Account for ClearPass

Active Directory needs to have a user account for ClearPass in order for ClearPass to establish a secure connection. The following procedure explains how to create an account in Active Directory for ClearPass by using a Windows 2012 Server.

**Note** Microsoft Active Directory features are not installed by default on Windows Server 2012. You must install Active Directory manually before starting this procedure. For more information, see the Microsoft website.

Step 1: On a Microsoft Windows Server 2012 server, open the **Active Directory Users and Computers** window.

Step 2: Navigate to **Active Directory Users and Computers > example.local**, right-click on **Users**, and then select **New > Users**.
Step 3: In the New Object—User window, enter the following information, and then click Next.

- First name—Example
- Last name—CPPM
- Full name—Example CPPM
- User logon name—example-CPPM@example.local

Step 4: In New Object—User window, enter the following information, and then click Next.

- Password—[password]
- Confirm password—[password]

Step 5: In the New Object—User window, click Finish.

2.4 Add Active Directory as an Authentication Source for ClearPass

After ClearPass joins the Active Directory domain, you must add the Active Directory as an authentication source in ClearPass in order to process authentication and authorization requests through Active Directory.

Step 1: Navigate to Configuration > Authentication > Sources, and then click Add.

Step 2: In the Authentication Sources window, on the General tab, enter the following information, and then click Next.

- Name—AD_example.local
- Type—Active Directory

Step 3: On the Primary tab, enter the following information for the AD account.

- Hostname—dc01.example.local
- Connection Security—AD over SSL
- Port—636
- Connection Security—check
- Bind DN—example-CPPM@example.local
- Bind Password—[password]
Step 4: Click Search Base Dn, and then in the LDAP Browser window, select dc=example,dc=local.

Step 5: Expand CN=Users to verify that the account information was entered correctly, and then click Close.

Step 6: In the Authentication Sources window, on the Primary tab, click Next.

Step 7: On the Attributes tab, click Next.

Step 8: On the Summary tab, click Save.

**Procedures**

**Connecting ClearPass Server to the Mobility Controller Cluster**

3.1 Add ClearPass to the Mobility Controller Cluster as a RADIUS Server

3.2 Add Mobility Controller Cluster to ClearPass

ClearPass needs to be added to the mobility controllers as a RADIUS server so that the controllers can use ClearPass to authenticate users accessing the wireless network. The mobility controllers then need to be added to ClearPass Policy Manager so that ClearPass accepts RADIUS authentication from the mobility controllers.

### 3.1 Add ClearPass to the Mobility Controller Cluster as a RADIUS Server

Step 1: Navigate to Managed Network > [group level for controller cluster] > Configuration > Authentication > Auth Server > All Servers, and then click Add.

Step 2: In the New Server window, enter the following information, and then click Submit.

- Name—Example-CPPM
- IP address—10.2.120.10 (IP address of the ClearPass server.)
- Type—RADIUS

Step 3: Navigate to Managed Network > Configuration > Authentication > Auth Server > All Servers, and then select Example-CPPM.
Step 4: In the Server Options window, enter the following information, and then click **Submit**.

- **IP address—** **10.2.120.10** (IP address of the ClearPass server added previously.)
- **Shared key—** [password]
- **Retype key—** [password]

Step 5: Click **Pending Changes**, then click **Deploy changes**, and then click **Close**.

### 3.2 Add Mobility Controller Cluster to ClearPass

The following procedure configures ClearPass to recognize the mobility controller cluster for authentication purposes. The information from the following table includes the IP subnet address used in the procedure below.

**Table 3 Example mobility controller cluster subnet address**

<table>
<thead>
<tr>
<th>Device</th>
<th>IP/subnet address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility controller</td>
<td>10.2.160.0/24</td>
</tr>
</tbody>
</table>

Step 1: Navigate to **Configuration > Network > Devices**, and then click **Add**.

Step 2: In the Add Device window, on the Device tab, enter the following information, and then click **Add**.

- **Name—** **AMS-Office-SC-Cluster**
- **IP or Subnet Address—** **10.2.160.0/24**
- **RADIUS Share Secret—** [password] (Use the Shared Key password you entered in Step 4 of the previous procedure.)

### Procedures

**Creating a Wireless Authentication Service**

4.1 Create a Wireless Service for Employees

In ClearPass Policy Manager, a **policy** defines the rules or specific conditions that must be met before the actions specified in the policy's profiles can be activated. A policy is then associated with a service. Services tie all of the elements together: authentication sources, authorization sources, role-mapping, and enforcement policies. Services are the highest-level element in the Policy Manager policy model.
Unique categorization rules (per service) enable Policy Manager to test access requests (requests) against available services to provide robust differentiation of requests by access method, location, or other network vendor specific attributes.

By wrapping a specific set of policy components, a service can coordinate the flow of a request from authentication to role and health evaluation to determine the enforcement parameters for network access.

This procedure configures a wireless authentication service for employee network access.

**4.1 Create a Wireless Service for Employees**

You can use either ClearPass local authentication or Active Directory authentication for the wireless service. Steps for both methods are included.

**Option 1: ClearPass Local Authentication**

**Step 1:** Navigate to Configuration > Services, and then click the **Add**.

**Step 2:** In the Services window, on the Service tab, enter the following information, and then click **Next**.

- **Type**—802.1X Wireless
- **Name**—Example-Employee-SVC

**Step 3:** On the Authentication tab, click **Select to Add** drop-down and then select the following information.

- **Authentication Sources**—[Local User Repository][Local SQL DB]

**Step 4:** Click **Save**.

**Step 5:** Navigate to Configuration > Identity > Local Users, and then click the **Add**.

**Step 6:** In the Add Local User window, enter the following information, and then click **Add**.

- **User ID**—employee
- **Name**—Example Employee1
- **Password**—[password]
- **Verify Password**—[password]
Option 2: Windows Active Directory Authentication

Step 1: Navigate to Configuration > Services, and then click the Add.

Step 2: On the Service tab, enter the following information, and then click Next.
  • Type—802.1X Wireless
  • Name—Example-Employee-SVC

Step 3: On Authentication tab, click Select to Add drop-down and then select the following information.
  • Authentication Sources—AD_example.local[Active Directory]

Step 4: Click Next.

Step 5: On the Roles tab, click Next.

Step 6: On the Enforcement tab, click Next.

Step 7: On the Summary tab, click Save.

This section concludes wireless configuration for employee access. For information about testing configurations, see the procedure group “Verifying Wireless Client Connectivity”.

Note This document is meant to get ClearPass up and running with minimum options configured.

Procedures

Creating the Guest Access Self-Registration Page

5.1 Create a Guest Self-registration Page for Wireless Network Access Using ClearPass

ClearPass Guest is a centralized visitor management solution that is included with ClearPass Policy Manager starting with version 6.7. This solution enables you to define settings that allow guests to self-register for guest network accounts. To initiate this process, the guest logs on to the mobility controller (Network Access Server), which
captures the guest and redirects them to a captive portal login window. From the login window, guests without an account can browse to the self-registration window to create a new account. After the guests create the accounts, the guests are automatically redirected to the mobility controller to log in with their new accounts. The mobility controller performs authentication and authorization for the guest account in ClearPass Guest. After authorization is complete, the guest is able to access the network. The guest can then choose to print or download a receipt or have the receipt information delivered by SMS or email.

**Figure 3**  Sequence Diagram for Guest Network Access

This procedure configures ClearPass Guest to allow guests to self-provision access to the wireless network.

### 5.1 Create a Guest Self-registration Page for Wireless Network Access Using ClearPass

**Step 1:** Open **ClearPass Guest**.

**Step 2:** Navigate to **Configuration > Pages > Self-Registrations**, and then click the **Create new self-registration** link.
Step 3: In the Customize Self-Registration window, on the **Basic Properties** page, enter the following information, and then click **Save and Continue**.

- **Name**—*Example-Guest Self Registration*
- **Registration Page**—*Example_Guest_Registration*

![Customize Self-Registration window](image)

Step 4: On the Register Page UI page, click **Save and Continue**.

Step 5: Repeat Step 4 for the Receipt Page UI, Receipt Actions, and Sponsorship Confirmation pages.
Step 6: On the Login page, enter the following information, and then click Save and Continue.

**Note** For Default URL, enter the URL for the page that you want to be displayed after the guest registration process has been completed.

- IP Address—securelogin.arubanetworks.com
- Default URL—http://www.arubanetworks.com
- Force default destination for all clients—Check

Step 7: On the Login Form page, click Save and Continue.

Step 8: On the Self-Service Portal page, click Save Changes.

Step 9: In Customize Self-Registration window, click Launch this self-registration window.

Step 10: Navigate to the web browser window that launched and copy the URL that appears in the address box. You use this redirect URL in Procedure 4.1.

- Copy URL—https://10.2.120.10/guest/Example_Guest_Registration.php
Procedures

Configuring the Mobility Master Captive Portal

6.1 Configure Mobility Master Captive Portal

This procedure configures the captive portal in Mobility Master to redirect the login window to the ClearPass Guest self-registration page created in previous procedure. This procedure covers only the captive portal configuration. For more detailed guest SSID configuration information, see the “Configure WLAN for guest SSID” procedure in Mobile First Campus for Large Networks.

6.1 Configure Mobility Master Captive Portal

Step 1: Log in to the Mobility Master, navigate to Managed Network > (group level for controller cluster) > Configuration > WLANs, and then click the name of SSID.

Step 2: On the Security tab, in the Captive Portal Options section, enter the following information, and then click Submit.

- CPPM host—10.2.120.10 (IP address/hostname)
- CPPM page—/guest/Example_Guest_Registration.php (remaining URL)

Step 3: Click Pending Changes, click Deploy Changes, and then click Close.

Procedures

Creating a Service for Guest Access

7.1 Create Guest Access Services

As described in “Create Wireless Authentication Service” section, a Service ties together elements of authentication sources, authorization sources, role-mapping, and enforcement policies. The fastest way to create a service for wireless guest access is by using the Service Templates & Wizards feature, which will be used in this section.
In “Create Wireless Authentication Service” section, Service for wireless employee access is created without using Service Templates & Wizards to expose the options with in a Service.

### 7.1 Create Guest Access Services

**Step 1:** Navigate to Configuration > Service Templates & Wizards, scroll down, and then click Guest Access.

**Step 2:** In the Service Templates—Guess Access window, on the General tab, enter the following information, and then click Next.

- Name Prefix—**Example-Guest**

**Step 3:** On the Wireless Network Settings tab, enter the following information, and then click Add Service.

- Wireless SSID for Guest access—**Example-Guest**
- Select Wireless Controller—**AMS-Office-SC-Cluster**

**Step 4:** Navigate to Configuration > Service, click Reorder, and then scroll down and click Guest Access.

Requests received by ClearPass are evaluated against each enabled service, starting from the top of the service list. After ClearPass finds a match, that service is used and any remaining services are ignored.
Step 5: Click Example-Guest Guest Access, click [Insight Operator Logins] to move Example-Guest Guest Access to the 6th position in the list, and then click Save.

This section concludes wireless configuration for guest access. To test the configuration, please refer to “Verify Wireless Client Connectivity” section.

Procedures

Verifying Wireless Client Connectivity

8.1 Verify Employee Wireless Client Connectivity

8.2 Verify Guest Wireless Client Connectivity

After you create a new service, it is important to test the new configuration to verify wireless client connectivity for both employees and guests. The following procedures verify wireless client connectivity for guests and employees. The figures in these procedures demonstrate using a Windows 10 client and Internet Explorer.

8.1 Verify Employee Wireless Client Connectivity

Step 1: On a client device, connect to an employee network.
Step 2: Enter the user name and password for an employee’s user account created in Active Directory, and then click OK.

Step 3: Open a browser and brows to www.arubanetworks.com. Once the webpage appears, the connection is successful.

### 8.2 Verify Guest Wireless Client Connectivity

Step 1: Connect a wireless client to a guest network.

Step 2: In the browser window that displays the message about an insecure site, opt to go to the web page regardless.

**Note** To avoid a certificate error message from being displayed, you must purchase and install a certificate from a Certificate Authority.
Step 3: On the **Self-Registration** page, enter the required user information, select *I accept the terms of use*, and then click **Register**.

Step 4: Verify your information and then click **Log In**.

If the guest connection succeeds, the message “Authentication successful” appears in the web browser, and the browser is automatically redirected to the pre-selected page.
ClearPass provides tools to monitor the status and activities of wireless clients connected to the network. One of the main tools to monitor client connectivity is Access Tracker. Access Tracker provides a real-time display of per-session access activity. Another useful tool included with ClearPass is Audit Viewer. Audit Viewer provides a dynamic report about the actions, device names, Policy Manager component categories, and timestamps of users that have connected to the network.

For more information about all ClearPass monitoring tools, see the “Live Monitoring” section of the 6.7 ClearPass Policy Manager User Guide.

### 9.1 Use Access Tracker

Step 1: Navigate to Monitoring > Live Monitoring > Access Tracker.
Step 2: To view detailed information about successful logins, in the Access Tracker window, click an entry where the value of Login Status is ACCEPT.

![Request Details](image1)

Step 3: To view detailed information about unsuccessful logins, in the Access Tracker window, click an entry where the value of Login Status is REJECT.

![Request Details](image2)
Step 4: To view error messages for a login attempt, in the Access Tracker window, click a login entry, and then select the **Alerts** tab in Request Details window.

![Request Details Window](image)

### 9.2 Use Audit Viewer

Step 1: Navigate to **Monitoring > Audit Viewer**.

![Audit Viewer](image)
Step 2: In the Audit Viewer window, click one of the actions listed to view more detailed information about the action.

![Audit Viewer Window](image)

**Summary**

Traditional network security methods focus on the perimeter and attempt to close off the network to threats by relying heavily on static policies. Aruba’s approach moves away from a physical model, where policy is tied to ports or VLAN interfaces, to a user- and device-centric model, where the policy follows the user regardless of how they connect to the network. With this approach, there is no need to pre-configure VLANs, ACLs, and QoS on individual ports. When a user or device connects to the network, the policy is downloaded to the network access layer and moves with the user.

With ClearPass Policy Manager, user and device policies are centralized. CPPM pulls in relevant context from multiple sources within an organization, leverages that context to determine the appropriate policy, and then coordinates that policy across multiple enforcement mechanisms.

This guide outlines fundamental ClearPass wireless access control configurations. These configurations include using Microsoft Active Directory integration as the primary authentication method for employees and wireless client guests to access a network. To minimize the complexity of the initial setup, most procedures use default profiles. After administrators become more familiar with the ClearPass workflow, they can customize advanced options and policies to provide users and devices with an optimal network experience.
You can use the feedback form to send suggestions and comments about this solution brief.