Aruba Central
Managed Service Portal

a Hewlett Packard
Enterprise company

User Guide

Copyright Information

Open Source Code

Chapter 1
About This Document

This user guide describes the features of the Managed Service Portal and provides detailed instructions to set up, configure, and manage customer accounts and the devices associated with the customer accounts.

Intended Audience

This guide is intended for customers who configure and use Managed Service Portal.

Related Documents

In addition to this document, the Central product documentation includes the following documents:

- *Aruba Central Getting Started Guide*
- *Aruba Central User Guide*
- *Aruba Central What's New*

Conventions

The following conventions are used throughout this guide to emphasize important concepts:

Table 1: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: ■ Sample screen output ■ System prompts
Bold	■ Keys that are pressed ■ Text typed into a GUI element ■ GUI elements that are clicked or selected

The following informational icons are used throughout this guide:

NOTE

Indicates helpful suggestions, pertinent information, and important things to remember.

CAUTION

Indicates a risk of damage to your hardware or loss of data.

WARNING

Indicates a risk of personal injury or death.

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

Chapter 2
Managed Service Portal

The Managed Service Portal mode provides a consolidated view of the customer accounts associated to a specific service provider. Through the Managed Service Portal, the administrators can provision customer accounts, and manage devices and subscriptions for the customer accounts.

Enabling the Managed Service Portal Mode

To launch the Managed Service Portal UI, click the **Managed Service Mode** menu option from the **User Settings** menu on the header pane.

Drilling Down to Customer Details

Although you can switch between the Managed Service Portal and the Standard Enterprise modes to view the details of the customer accounts, the following operational conditions are applicable:

- The Managed Service Portal administrators can drill down to view the details of a specific customer. To drill down to a specific customer account, click **Customers** and then click the **customer ID**. The end customer details are displayed in the Standard Enterprise view.
- Any configuration changes to the group associated with an end customer in the Managed Service mode are applied to the default group in the Standard Enterprise mode.
- The users must be added only from the **User Management** pane on the Managed Service Portal mode.
- The devices available in Central are referred to as **Available Devices**. The devices allocated to the end customer account are referred to as **Allocated Devices**. The Managed Service Portal administrators can switch between the Managed Service Portal and the Standard Enterprise mode to add, view, and assign the devices.

When you switch to the Standard enterprise mode, the customer account name is shown as a breadcrumb in the header pane. To go back to the Managed Service Portal mode, click the account name.

Disabling Managed Service Mode

To disable Managed Service mode and then switch to the Standard Enterprise mode:

1. On the Managed Service Portal main window, click the user icon (👤) on the header pane.
2. From the user settings menu, click **Disable Managed Service Mode**.
3. Click **Disable**. A notification message indicating that the disable operation results in the loss of end-customer data is displayed. You must delete the end customer data before switching to the standard enterprise mode.

CAUTION

Disabling Managed Service Portal mode results in the loss of end customer data.

To start using Aruba Central, complete the following steps:

- Signing up for Aruba Central on page 9
- Adding Devices to Central on page 10
- Creating Customer and User Accounts
- Assigning Subscriptions
- Assigning Devices to Groups

Signing up for Aruba Central

To sign up as a customer for Central:

1. Go to http://www.arubanetworks.com/products/sme/eval/.
2. Enter your email address and click **Continue**.

- If you are signing up for Central for the first time, the registration page is displayed. Complete the registration process (see step 3 through step 8).
- If you are an existing customer and your email address is already in the Central database, and you have verified your email address, the Central login page is displayed.
- If your email address already exists in the Central database and you have not verified your email address, click **Resend Verification Email** and verify your email address by clicking the **Activate Your Account** link.
- If you are an existing Aruba customer with SSO login credentials and you are signing up for Central for the first time:
  - Validate your account by providing your SSO password. On successful authentication, the registration page is displayed. Complete the registration process to gain access to Central (see step 3 through step 8).
  - If you have forgotten your SSO password, click **Forgot Password** and complete the steps to retrieve your password.
  - To sign up again, click **Try Signing up again** and complete the steps to sign up for an Central account.

3. On the Registration page, enter first name, last name, and address details. If you are a new user, enter the password. For registered users and those with SSO login credentials, the **Password** field is disabled.
4. If you have Aruba Activate user credentials, select **I have an Aruba Activate account** check box and enter your user name and password for the Activate account.

NOTE

You can use your Aruba Activate account to manually import devices into Central. However, Central allows each user account to import devices using Aruba Activate account only once.

5. Select the **I agree to the Terms and Conditions** check box.
6. Click **Sign Up**. On successfully completing the registration, a verification email is sent to your email address.
7. Access your email account and click the **Activate Your Account** link. If the email verification is successful, the **Log in to Aruba Central** button is displayed.

Adding Devices to Central

After you successfully log in to Central, a welcome message is displayed in the Central UI. To bind devices to your subscription, click **Manage Your Devices**. The **Device Provisioning** page is displayed. To view the subscription key details before binding devices, click **Subscription Keys** under **Global Settings** > **Devices & Subscriptions**.

Central supports zero touch provisioning of the devices. It automatically retrieves the devices associated to a customer account. To synchronize the devices from the inventory, click **Sync Now**. If the retrieval of devices is not complete or successful due to process errors, you can manually add the devices.

Central allows you to import devices using your Aruba Activate user credentials, the MAC address and cloud activation key of a device, or the MAC address and Serial Number of a device. You can specify the method for importing devices when adding a device.

For users with the evaluation subscription, the devices are not automatically synchronized. Therefore, the users must manually add the devices.

NOTE

The evaluation subscription with device subscription tokens allows you to add up to 10 APs or 10 Switches, or a combination of 10 APs and Switches. With device subscription tokens, you can access basic network management services such as monitoring, configuration, and report generation.

The service evaluation subscription allows you to access application services, for example, Presence Analytics. With this subscription, you can add up to 20 APs.

For APs that dynamically form a cluster, the users must add the master AP from the **Device Provisioning** page whenever a slave AP joins the cluster, in order for the slave AP to inherit the configuration from the master AP.

To manually add a device, complete the following steps:

1. Click **Global Settings** on the left pane.
2. Click **Devices & Subscriptions**. The **Device Provisioning** page is displayed.
3. Click **Add Devices**. The **Manually Add Devices** window opens.
4. Select one of the following device addition options:

Table 3: *Adding Devices*

Device Addition Option	Description
Aruba Activate Credentials	To retrieve all devices associated to an Activate user account: 1. Select **Aruba Activate Credentials** from the **Add devices using** drop-down list. 2. Enter the username and password of the Activate user account. 3. Click **Next**. The Activate account details and the total number of devices associated with this account are displayed. 4. To add all devices, click **Add <Number> Devices** button. The devices associated with the Activate account are retrieved and added to the list of devices displayed on the **Device Management** page. **NOTE:** You can use this option only once. After the devices are added, Central does not allow you to modify or re-import the devices using your Aruba Activate credentials. If you account is already mapped to an Aruba Activate account, contact Aruba support team.
Bulk addition of devices based on cloud activation key	To retrieve multiple devices from a single purchase order by providing the cloud activation key: 1. Note the Cloud Activation Key and MAC address of the device. To obtain these details: ■ For APs, execute the **show about** command at the AP CLI or click **Maintenance** >**About** in the AP UI. ■ For legacy Switches, execute the **show inventory | include HW** and **show version** commands on the Switch CLI. ■ For the other ArubaSwitches, to view the MAC address and the serial number, run the **sh system | in Base** and **sh system | in Serial** commands at the CLI. You can also view the cloud activation key in the **Maintenance** > **About** tab of the switch UI. The activation key is enabled only if the Switch has access to the Internet. 2. Select **Cloud Activation Key** from the **Add devices using** drop-down list. 3. Enter the **MAC address** and **Cloud Activation Key** of the device. 4. Click **Next**. Central retrieves all devices that belong to the same purchase order and displays the list. A list of blocked devices is displayed if any of the device belongs to another customer account or is used by other services. As Central does not allow you to add blocked devices, you may have to release the blocked devices from another customer account. 5. To continue adding devices, click **Add <x> Devices**. 6. To restart the device addition procedure, click **Start Again**.
Adding up to 32 devices	To manually add devices by using the serial number and MAC address of the device: 1. Select **Device List (Up to 32 Devices)** from the **Add device using** drop-down list. 2. Enter the MAC address and serial number of the device. 3. Click **Next**. The list of available devices is displayed. 4. Click **Add <x> Devices**. **NOTE:** Central allows you to add up to 32 devices.

The provisioning of the legacy ArubaSwitch fails when the provisioning process is interrupted during the initial booting and if the switch has a static IP address with no DNS server configured.

During Zero Touch Provisioning, the Aruba Switches can join Central only if they are running the factory default configuration, and have a valid IP address and DNS settings from a DHCP server.

If the switches ship with a version lower than the minimum supported firmware version, a factory reset may be required, so that the switch can initiate a connection to Central. For information, on the minimum firmware versions supported on the switches, see Supported Platforms.

Creating Customer and User Accounts

This section describes the procedures for configuring through the Managed Service Portal and Standard

Interface view.

In the Managed Service Portal

The customers who sign up for Central and obtain evaluation or paid subscription can log in and manage their devices through the Standard Enterprise interface. However, if these customers have multiple accounts associated with their service, they can use Managed Service portal to create and manage their respective customer accounts, and allocate devices to these accounts.

Adding Customer Accounts

To add customer accounts in the Managed Service Portal mode, complete the following steps:

1. Ensure that you have enabled the Managed Service Mode. To enable access to the Managed Service Portal mode, click the **Managed Service Mode** menu from the user settings menu on the header pane. The Managed Service Portal opens.
2. From the App selector, click **Network Management**, and then click **Customers**. The **Customers** page opens.
3. Click **+ Add Customer**. The **Customer > Create Customer** window opens.
4. Enter the name of the customer in the **Customer Name** text box.
5. Select a group to which you want to associate the customer account.
6. To add users to this account, enter the email address of the user. By default, the users are assigned the read-only privilege.
7. To add another user, click **+ Add User** and then enter the email address of the user.
8. Click **Save**. When the account is created successfully, an email invitation is sent to the user.

The customer accounts created and managed by the Managed Service Portal administrators have limited access to the Standard Enterprise interface.

Assigning Devices to Customer Accounts

The admin users in the Managed Service Portal can allocate the devices in Central to specific customer accounts and assign subscription keys.

To assign a device to a customer account, complete the following steps:

1. Click **Global Settings**>**Devices & Subscriptions**. The **Device Provisioning** page opens.
2. Select the devices type, for example Access Points. A list of APs connected to Central is displayed.
3. Select one or several devices that you want to assign to a customer.
4. Click **Assign to Customer**.
5. Select a customer account from the list. You can also search for customer accounts.

   On selecting a customer account, the Managed Service Portal shows the groups associated with the account. The administrators can assign a device to a specific group associated with a customer account.
6. Select the group to which you want to assign the device.
7. Click **Assign**.

In the Standard Interface View

You can add users to an existing customer account in the Standard Enterprise view. If you have to devices from multiple locations with separate customer accounts, you can also create additional customer accounts.

Adding Users

To configure user accounts through the Standard Central Interface, complete the following steps:

1. Click **Maintenance > User Management**.
2. On the **User Management** pane, click **Add User**. The **Create User** window is displayed.
3. Enter the email address of the user in the **Username** text box.
4. From the **User Scope** drop-down list, select the group to which you want to assign the user.
5. Select the user access level that you want to assign to the user from the **Access Level** drop-down list.

   Central supports following types of users:

   - **Admin**—The admin users have full access to all the groups and have special rights to create or update user details, groups, and to provision devices.
   - **Read/Write**—The users with read/write privileges can access the groups or devices assigned by the Admin user. The users with Read/Write privileges can perform operations that can change the behavior of devices or groups such as modifying the configuration of a device, deleting a device and so on.
   - **Read only**—The users with read-only privileges can access the groups or devices assigned by the Admin user and view details of the groups and devices.
   - **Guest operator**—The guest operators have access to guest management operations only. These users can add guest users and configure splash page profiles.

NOTE

A user cannot have different access rights for different groups.

6. Click **Save**. When the user account is successfully created:

   - New users will receive a welcome email with the registration link. Complete the registration steps described in step 7 through step 11.
   - Users with an existing Central account will receive an email invite with a link to the Central portal. Click the link to access the Central UI.

NOTE

If the user has not received the registration email, click **Resend Invite Email** in the **User Management** pane to resend the invite.

7. To register, click **Register Your Account** link. The **Sign up with Aruba Central** page is displayed.
8. Enter the password, , first name, last name, and address details.
9. Select a country and state.
10. Select the **I agree to the Terms and Conditions** check box.
11. Click **Sign Up**. On successful completion of registration, the user account is created.
12. Log in to Central with the registered credentials.

Creating Additional Customer Accounts

If you want to manage Wi-Fi networks in multiple regions, you can create additional customer accounts. Central allows you to create up to five customer accounts.

To create an additional customer account:

1. Click the **Settings** icon next to your user name on the main pane. Click **Switch Customer**. The customer account selection page is displayed.
2. Click the + icon to add a new account. The **Sign up with Aruba Central** page is displayed.
3. Enter your address, and select the country and state.
4. Enter the city and ZIP code details.
5. Select the **I agree to the Terms and Conditions** check box.
6. Click **Sign Up**. The customer account is added.
7. Repeat the procedure to add another customer account.

To log in with a different customer account, click **Switch Customer** and click the account that you want to access.

Assigning Subscriptions

You can assign any of the following types of subscriptions either through the Managed Service Portal or the Central Standard Interface.

- Device subscriptions—Subscriptions for the devices to avail basic services such as device configuration, monitoring, reporting, and analyzing application usage.
- Service subscriptions—Subscriptions based services for apps such as Presence Analytics, Guest Access, and so on.

To assign subscriptions to the devices, complete the following steps:

1. Click **Global Settings** > **Devices & Subscriptions** > **Subscription Assignment**.

   The **Subscription Assignment** page allows you to assign subscriptions for the devices or services for which the users have subscribed.
2. To assign subscriptions to devices, complete the following steps:
   a. Move the slider to **Devices**.
   b. Select the device to which you want to assign a subscription.
   c. Click **Assign**.
3. To assign service subscriptions, complete the following steps:
   a. Move the slider to **Network Services**.
   b. Select the device to which you want to assign a service subscription token.
   c. Select the desired services.
   d. Click **Assign**.

Assigning Devices to Groups

When the devices are added to Central, they are automatically provisioned. The devices connected to Central are indicated in green in the Standard Enterprise view.

In the Standard Enterprise View

The group assignment in the Standard Enterprise view depends on the following conditions:

- If the device is not connected to Central, the **Assign Group** button is displayed.

- If the device is connected to Central, irrespective of the operational status of the device, the **Assign Group** button is not displayed.
- When a user selects devices that are not connected to Central along with another device that is connected to Central, although the **Assign Group** button is displayed, the group assignment operation is carried out only for the device that is not connected to Central.
- When the device is moved from one group to another, the group column in the **Device Management** page shows the new group name.

To assign devices to a group, complete the following steps:

1. Click **Global Settings** > **Devices & Subscriptions**. The **Device Provisioning** page opens.
2. Select the devices type, for example Access Points. A list of APs connected to Central is displayed.
3. Select the devices for group assignment.
4. Click **Assign Group**. The **Assign Group** pop-up window opens.
5. Select the group to which you want to assign the selected devices.
6. Click **Assign**.
7. To assign the device to a new group, complete the following steps:
    a. Enter the name of the group in the text box and click **(+)**. The newly created group is displayed in the list of available groups.
    b. Select the newly created group and click **Assign**.

In the Managed Service Portal

In the Managed Service Portal, the groups are assigned to a customer account. The provisioning status of the devices for each customer account is displayed in the **All Customers** table on the **Monitoring** > **All Customers** page. If a device is listed under the unprovisioned group for the customer account in the Standard Enterprise mode, the status of this device is displayed in the **All Customers**. To move the device from the unprovisioned group to the default group, the Managed Service Portal Portal administrators must drill down to the customer account and move the device to default in the Standard Enterprise mode.

If a customer account is associated to a new group created in the Managed Service Portal, the configuration of the devices associated with this customer account is pushed to the **default** group in the Standard Enterprise view for that customer. However, the Managed Service Portal administrators can create more groups for a customer account by drilling down to the customer account in the Standard Enterprise view.

Chapter 4
Managed Service Portal Interface

The Managed Service Portal UI provides a concise and basic view of the customer details. To view more details of the devices associated with a specific customer account, the service provider administrators can drill down to view the details of their network and devices in the Standard Enterprise mode.

On enabling to the Managed Service Portal mode, the Monitoring dashboard is displayed.

The Managed Service Portal interface consists of the following elements:

- Header Pane on page 16
- Aruba Central App Selection on page 17
- Data Pane on page 18

Header Pane

The header area of the main window displays the following information:

- Company Logo—On clicking the logo, the monitoring dashboard is displayed.
- Group selection—The group settings icon displays the provisioned groups.

For more information on groups, see Managing Groups on page 19.

- The number and of APs, customers, and subscriptions.
  - **ACCESS POINTS**—Displays the total number of APs managed by the service provider. On clicking **ACCESS POINTS**, the **Device Management** page is displayed.
  - **SWITCHES**—Displays the total number of Switches managed by the service provider. On clicking **SWITCHES**, the **Device Management** page is displayed.
  - **CUSTOMERS**—Displays the number of customers in the Service Provider's network. On clicking **Customers**, the **Customers** page is displayed.
  - **DEVICE SUBSCRIPTIONS**—Displays the total number of available subscriptions and the number of used subscriptions. On clicking the numbers, the Subscription Keys page is displayed.
- The mobile icon—Allows you to download the Aruba Central mobile app from the following sites:
  - **App Store**—For Apple devices running iOS 9.0 or later.
  - **Google Play Store**—For mobile devices running Android 5.0 Lollipop or later.
- The bubble icon—Displays the following options:
  - **Documentation**—Opens the Central user documentation site.
  - **View / Update Case**—Directs you to the support site to view or update an existing support case.
  - **Open New Case**—Directs you to the support site to open a new support case.
- The help icon—Click the **?** icon to view a short description or definition of the selected terms and fields in a pane or dialog box. To view the online help:

  a. Click the **(?)** at the top.

  b. Move your cursor over a data pane item to view the help text.

  c. To disable the help mode, click **(?)** again.
- The user icon—A drop-down menu with the following options for managing the Central user and customer accounts:

- **Switch Customer**—Allows you to switch to another customer account. For more information, see *Creating Additional Customer Accounts* in the *Aruba Central User Guide*.
- **Change Password**—Allows you to change the password of account.
- **User Settings**—Displays the date, time and timezone. The administrators can also set a timeout value for inactive user sessions.

NOTE

The Managed Service Portal UI is available in English, French, Spanish, Deutsche, and Chinese languages. You can now set your language preference through the **User Settings** menu from the drop-down list on the header pane. Central saves your language preference setting and displays the UI in the language set by you.

- **Terms of Service**—Displays the terms and conditions for using Aruba Central services.
- **Disable Managed Service Mode**—Disables the Managed Service Portal mode and switches to the standard enterprise interface. The Managed Service Portal mode can be disabled only if there are no active customer accounts in Managed Service Portal.
- **Logout**—Allows you to log out your account.

Aruba Central App Selection

The left navigation pane displays the App Selector icon. On clicking the App Selector icon, the available apps are displayed. The contents on the top left navigation pane change dynamically based on the selection of apps.

For example, clicking on **Guest Access** displays the function tabs and menu options for guest network configuration respectively. By default, the Network Management application view is selected.

By default, each function tab appears in a compressed view. Click the tabs to expand or collapse the tab view.

NOTE

The availability of apps is subjected to Service subscriptions. Contact your administrator and the Aruba Central Support team to obtain access to the application services.

Network Management

The following menu options are available in the **Network Management** application view:

Monitoring

The following menu options are available:

- **Overview**—Displays a list of top customers, the subscription renewal schedule, the devices under management, and new customers added in the last 6 months.
- **All Customers**—Displays a complete list of customers in your network and a summary of devices associated with the customer.

Wireless Configuration

The **Wireless Configuration** tab allows you to configure APs, wireless or wired network, intrusion detection and prevention, Radio Frequency (RF) settings, security settings, Dynamic Host Control Protocol (DHCP) profiles, services, and system parameters.

Customers

The **Customers** tab allows you to add, modify, and delete customers. You can also add users to customer accounts.

Maintenance

The **Maintenance** tab allows you to maintain the network and configure user credentials. It includes the following menu options:

- **Firmware**—Displays the list of customers and the firmware upgrade status of the devices associated with the customer account. On selecting a customer account and clicking the **edit** icon, all devices associated with that customer account are displayed.
  - To upgrade firmware for a device, select the device and then click **Upgrade Firmware**.
  - To upgrade all devices, click **Upgrade All**.
- **User Management**—Allows you to view and add user profiles to a customer accounts.
- **Portal Customization**—Allows you to customize the look and feel of the email notifications and the user interface.

Guest Access

The following menu options are displayed in the **Guest Access** application view:

- **Overview**—Displays a dashboard that shows the details of the cloud guest SSIDs, duration for which the guest users are connected, client count, and the type of client devices connected to the cloud guest SSIDs.
- **Splash Page**—Allows you to configure splash page profiles for guest network profiles.
- **Visitors**—Allows you create guest user accounts and assign these users to a guest SSID.

Global Settings

The **Global Settings** tab includes the following menu options:

- **Devices & Subscriptions**— This menu command allows you to perform the following actions:
  - View and manage devices in the inventory.
  - View the details of subscription keys.
  - Assign subscriptions to customers.

Data Pane

Displays detailed information of the tabs and data for the selected menu commands.

Notifications Pane

The notifications pane at the bottom of the page displays alert notifications. For example, if a device does not have the country code parameter configured, the notifications pane displays an alert and allows the users to set a country code for the device.

Managing Groups

Central allows some configuration settings to be managed efficiently at the group level, while others are managed at an individual device level. In Central, the group is a subset of the devices on the wireless LAN, ranging in size from one device to hundreds of devices that share some common configuration settings. When a group is configured, all devices within a group share the same configuration settings.

Provisioning Groups in the Managed Service Portal

Unlike in the Standard Enterprise mode, the groups in the Managed Service Portal are associated with the customer accounts. The devices are first allocated to the customer accounts, and then the groups are assigned to these accounts.

Unlike in the Standard Enterprise mode, the monitoring dashboard or the network view is not determined by the selection of the groups. As devices are mapped to customer accounts, all information pertaining to a customer account is displayed.

In the Managed Service Portal, the provisioning status of the devices for each customer account is displayed in the **All Customers** table. If a device is listed under the unprovisioned group for a customer account in the Standard Enterprise mode, the status of this device is displayed as unprovisioned in the **All Customers** table. To move this device from the unprovisioned group to the default group, the Managed Service Portal administrators must drill down to the customer account and move the device to the default group in the Standard Enterprise mode.

If a customer account is associated to a new group created in the Managed Service Portal, the configuration of the devices associated with this customer account is pushed to the **default** group in the Standard Enterprise view for that specific customer. However, the Managed Service Portal administrators can create more groups for a specific customer by drilling down to a customer account in the Standard Enterprise view.

Creating a Group

To create a group, complete the following steps:

1. Click the icon next to **All Groups** on the left pane.
2. Click **(+)** to create a new group. The **Create New Group** pane appears.
3. Enter a name for the group in **Enter Group Name**.
4. To use this group as a template group, select the **Set this group as a template group** check box and click **Save**.

NOTE

If the group is set as a template group, the configuration is applied to all the devices in the group. For devices in such groups, the configuration wizards in the UI are disabled.

The current version of Central allows template group creation for AP devices only.

5. To create a non-template groups, click **Next** and complete the following steps:
   a. Enter the default device password for the newly created group in the **Password** text box.
   b. To reconfirm the password, re-enter the default device password in the **Retype Password** text box.
   c. Click **Save**.

Editing a Group

To edit or delete a group, complete the following steps:

1. Click the icon next to **All Groups** in the left pane.
2. Select the group to modify or delete, and then click the settings icon.
3. To create a clone of an existing group, complete the following steps:
   a. Select the group and click the clone icon next to the group. The **Create New Group** pop-up window opens.
   b. Enter a name for the group.
   c. Click **Save**.

NOTE

The cloning feature is supported only for the non-template groups. If a group is set as a template group, the cloning icon will not be displayed for that group.

4. To delete a group, select the group to delete and click the delete icon.

Chapter 5
Monitoring Accounts and Subscriptions

The **Monitoring** tab includes the following menu options:

- Overview on page 21
- All Customers on page 21
- Notifications List

Overview

The **Overview** pane displays a list of top customers, the subscription renewal schedule, the devices under management, and the total number of new customers in the managed service network.

Table 4: *Overview Pane*

Graphs	Description
Top Customers List	Displays the ID and name of the customer, the total number of the devices associated with the customer, and the number of devices with valid subscription keys.
Subscription Renewal Schedule Graph	Displays the subscription renewal schedule for the next 12 months. The graph plots the total count of subscriptions that are due for renewal for each month.
Devices under Management Graph	Displays the count of devices that are managed in the network. By default, the device count is shown for the last 6 months. You can also view the data for the last 1, 2, or 3 years.
Customers Added Graph	Displays the total number of customers added to Central in the last six months.

All Customers

The **All Customers** pane displays a summary of the customer accounts associated with a specific service provider.

Table 5: *All Customers Pane*

Column	Description
ID	ID associated with the customer account. On clicking the ID, the Managed Service Portal takes you to dashboard of the standard Central interface that displays data for a specific customer account.
Name	Name of the customer account.
Provision Status	Status of the customer account provisioning.
Device (Total)	The total number of devices associated with the customer account.

Column	Description
Licensed Device	The total number of devices with valid licenses and subscription keys in a customer account.
Unprovisioned AP	The number of unprovisioned APs in the customer account.
No Country Code	The number of APs that do not have the country code configured.

Notifications

The **Notifications** pane displays information alerts about the configuration events detected for the devices associated with a customer account.

The following menu options and information are available on the **Notifications** page:

- **Acknowledge All**—This button allows you to acknowledge all notifications at once.
- **Notifications List**—This table displays detailed information about the notifications that are yet to be acknowledged.
- **Settings**—This icon allows you configure notification alerts for the events associated with a device.

By default, the Managed Service Portal shows the notifications for the configuration events that occurred in the last 1 month.

Table 6 describes the information elements in the notifications list:

Table 6: *Notifications List*

Data Pane Content	Description
Notifications Type	Type of the information alert. The notification type can be an alert
Date	Time stamp of the event that triggered the notification alert.
Description	Description of the event that triggered the notification alert.
Search box	Allows to search for notifications and define a filter criteria to display notifications in the table.
Acknowledge All	Acknowledges all notifications at once.
Customer ID	Shows the customer ID of the customer account to which the device is assigned.
Customer Name	Shows the name of the customer account to which the device is assigned.

The UI also shows the alerts and pending actions, such as importing a device, setting country code of APs and so on, in the bottom pane of the UI. Click the links and complete the required actions.

Setting Notification Alerts

To configure a notification alert, complete the following steps:

1. Click the **> Settings** icon.
2. Select a notification type from the **Type**drop-down list.
3. Select an event type from the **Event** drop-down list.
4. Select a group type from the **Group** drop-down list.
5. To receive email notifications, select the **Email** check box and enter the email address.
6. Click **Save**. The notification settings configured in the Managed Service Portal are propagated to the associated customer accounts.

Chapter 6
Configuration

The **Configuration** tab includes the following menu options:

- Wireless—Allows you to configure WLAN SSIDs, RF, DHCP, VPN, and Security parameters of the AP devices associated with the customer account.

NOTE

Both the Managed Service Portal and Standard Enterprise interface allow the admin and read/write users to configure SSIDs.

If a customer account is associated to a new group created in the Managed Service Portal, the device configuration is pushed to the default group in the Standard Enterprise view.

- Switch-MAS—Allows you to configure legacy Aruba Switches such as Mobility Access Switch.
- Switch Aruba—Allows you to configure various models of Aruba Switches.

Chapter 7
Managing Customers Accounts

The **Customers** pane in the Managed Service Portal mode allows you to view, add, edit, or delete end customer accounts.

This section describes the following topics:

- Viewing Customer Account Details
- Adding a Customer Account
- Editing a Customer Account
- Deleting a Customer

Viewing Customer Account Details

The **Customers** pane displays the following details:

Table 7: *Customers Pane*

Data Pane Item	Description
ID	Displays the ID of the customer. To view the details of a customer account in the Central UI, click the ID.
Name	Displays the name of the customer.
Provision Status	Displays the provisioned status of the customer.
Group	Displays the group to which the customer belongs. If the group configuration is not synchronized between the Managed Service Portal and the Standard Central interface, the override icon is displayed. To override the configuration changes, click the override icon.
Create Date	Displays the customer account creation date.

NOTE

The Managed Service Portal administrators can drill down to view the customer account details in the Standard Enterprise mode, to add more users or change the user role of the customers.

Adding a Customer Account

To add an end customer account, complete the following steps:

1. Click **Customers**.
2. On the **Customers** page, click the **+** icon. The **Customer > Create Customer** window opens.
3. Enter the name of the customer in the **Customer Name** text box.
4. Select a group to which you want to assign the customer.

5. To prevent the admin users from editing the SSIDs in the selected group by drilling down to end customer's account, select the **Lock SSID** checkbox. When the SSIDs of a group are locked, Central does not allow even the admin users of a specific end customer account to modify the SSID configuration.

6. To add a user to the customer account, enter the email address and select any of the following roles for the user profile:

- admin—The admin users have full access to all the groups. The admin users can also create or update user details, and groups, and provision devices.
- read only—The read only users have only read access to the groups or devices assigned by the admin user. The read only users can only view the groups and device details.
- read/write—The read/write access to the groups or devices assigned by the admin user. The read/write users can modify the configuration of a device, or delete a device from the provisioned network.
- guest operator—A guest operator users have read/write access to the cloud guest and captive portal configuration and other guest management operations.

7. To add another user, click the **+** icon next to **Users** and select the desired roles.

8. Click **Save**.

The admin and read/write roles are applied to users only at the Managed Service Portal level. When the customer account is drilled-down, only the read only and guest operator roles can be assigned for these user profiles.

NOTE

The customer accounts created and managed through Managed Service Portal have limited access to reports. These users can access the reports generated for the default group only. Therefore, the Managed Service Portal administrators must drill down to the customer account and then generate reports for the default group in the Standard Enterprise mode.

Editing a Customer Account

To edit an end customer account, complete the following steps:

1. Select a customer account from the **Customers** table.
2. Click the edit icon.
3. Modify the account details.
4. Click **Save**.

Deleting a Customer

To delete a customer account, complete the following steps:

1. Select a customer account from the **Customers** table.
2. Click the delete icon.

The **Maintenance** tab displays the maintenance pane for the Central. The **Maintenance** pane consists of the following menu options:

- Viewing Firmware Information on page 27
- Configuring User Accounts for Managed Service Portal on page 28
- Customizing Portal on page 29

Viewing Firmware Information

The **Firmware** pane provides a list of customer accounts and the status of the devices associated with the customer account in the Managed Service Portal mode.

Table 8: *Firmware*

Date Pane Item	Description
ID	ID of customer account.
Name	Name of customer account.
Status	Status of the devices associated with the customer account. This column indicates if the latest version of the firmware is available.

To edit the details and view device information, click the select the row and click the edit icon. The following information is displayed:

Table 9: *Firmware*

Date Pane Item	Description
Name	Name of the Device.
Firmware Version	The current firmware version running on the VC.
Latest Firmware Version	The latest firmware version available on the public firmware server.
Status	Status of the firmware upgrade on the VC.
Upgrade Firmware	Allows you to upgrade the device firmware to the latest supported version. To upgrade firmware for the a device, complete the following steps: 1. Click **Upgrade Firmware**. 2. Select the device and the firmware version.
Upgrade All	Allows you to simultaneously upgrade firmware for multiple devices.
Search Filter	Allows you to define a filter criterion for searching devices based on the host name, MAC address, location, firmware version, and the current upgrade status of the device.

Forcing Firmware Upgrade

Central now allows you to force firmware upgrade for devices in a group. To force a specific firmware version for all AP devices or Switches in a group, complete the following steps:

1. Select a device group from the **Groups** menu.
2. Click **Maintenance** > **Firmware**. The **Firmware** page opens.
3. Click the settings icon next to Firmware. The settings icon is displayed only if the page view is set to individual group level.
4. The **Firmware Compliance Setting** window opens.
5. Select the desired firmware version for APs or Switches.
6. Click **Save**. Central initiates a firmware upgrade operation for the devices that support the selected firmware version. Central also displays a list of unsupported devices on which the firmware upgrade operation cannot be enforced.

Configuring User Accounts for Managed Service Portal

The **User Management** pane in the Managed Service Portal allows you to add, edit, or delete users for the Managed Service Portal.

Supported User Roles

Managed Service Portal supports the following types of users:

- **Administrator**—The administrator users who can create, provision, and manage customer accounts in the Managed Service Portal.
- **Read Only**—These users have only read access to the customer accounts.

NOTE

A user cannot have different access rights for different groups.

Adding a User Account

To configure user accounts for Managed Service Portal, complete the following steps:

1. Click **Maintenance > User Management**.
2. On the **User Management** pane, click **+**. The **New User** window is displayed.
3. Enter the email address of the user in the **Username** text box.
4. Select the user access level that you want to assign to the user from the **Access Level** drop-down list.
   - **Administrator**
   - **Read only**
5. Click **Save**. When the user account is successfully created, the user is added to the customer account and an email invitation is sent to the user.

Editing a User

To edit a user account, select the user and click the edit icon.

Deleting a User

To delete a user account, select the user and click the delete icon. The Managed Service Portal users can deleted only from the Managed Service Portal interface.

Customizing Portal

The **Portal Customization** pane allows you to customize the look and feel of the user interface and the email notifications sent to the customers and users. For example, you can use your company logo in the user interface and company address in the email notifications sent to the customers or users.

To customize the look and feel of the portal, complete the following steps:

1. Click **Maintenance** > **Portal Customization**. The **Portal Customization** pane opens.
2. Under **Customization**, configure the following information:
   - **Product Name**—Name of the product.
   - **Provider Name**—Name of the company.
   - **Contact Link**—The URL to the company website that shows the contact address of the company.
   - **Sender Email Address**—The email address from which the notifications are sent.
   - **Mailing Address**—The postal address of the company.
   - **Service Link**—The URL to the company website showing the service related information.
   - **Terms and Conditions Link**—The URL to the company website listing the terms and conditions.
3. If you want customize the logo of your portal, click **Skinning**.
4. Browse to your local directory and upload the logo image.
5. Click **Save Settings**.

Viewing Audit Trails

The **Audit Trail** page shows the logs for all the events triggered in Central at the **All Groups** level. To view the details of a particular event, click the details icon under the **Details** column.

Viewing Audit Trails in Managed Service Portal

The **Audit Trail** logs are displayed for the following types of operations in the Managed Service Portal:

- Addition, modification, and deletion of customer accounts
- Addition, modification and deletion of users associated with a customer account
- Subscription assignment to devices
- Modification of groups associated with a customer account
- Configuration push, override , and updates for the devices associated with a customer account
- Addition, modification, and deletion of Managed Service Portal admin users

The **Audit Trail** page in the Managed Service Portal displays the following information:

Table 10: *Audit Trail Pane in the Managed Service Portal*

Data Pane Content	Description
Time	Time stamp of the events for which the audit trails are shown.
Username	The username of the admin user who applied the changes.
IP Address	IP address of the client device.
Classification	Type of modification and the affected device management category.
Target	The group or device to which the changes were applied.
Details	A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates.
Customer ID	The ID of the customer account to which the device is assigned.
Customer Name	Name of the customer account to which the device is assigned.

Chapter 9
Guest Access

The guest management feature allows guest users to connect to the network and at the same time, allows the administrator to control guest user access to the network.

Central allows administrators to create a splash page profile for guest users. Guest users can access the Internet by providing either the credentials configured by the guest operators or their respective social networking login credentials. For example, you can create a splash page that displays a corporate logo, color scheme and the terms of service, and enable logging in from a social networking service such as Facebook, Google +, Twitter, and LinkedIn.

Businesses can also pair their network with the Facebook Wi-Fi service, so that the users logging into Wi-Fi hotspots are presented with a business page, before gaining access to the network.

To enable logging using Facebook, Google+, Twitter, and LinkedIn credentials, ensure that you create an application (app) on the social networking service provider site and enable authentication for that app. The social networking service provider will then issue a client ID and client secret key that are required for configuring guest profiles based on social logins.

Guest operators can also create guest user accounts. For example, a network administrator can create a guest operator account for a receptionist. The receptionist creates user accounts for guests who require temporary access to the wireless network. Guest operators can create and set an expiration time for user accounts. For example, the expiration time can be set to 1 day.

For more information, see the following topics:

- Guest Access Dashboard on page 31
- Creating Apps for Social Login on page 32
- Configuring a Cloud Guest Splash Page Profile on page 36

Guest Access Dashboard

The **Overview** page in the **Guest Access** application provides a dashboard displaying the number of guests, guest SSID, client count, type of clients, application usage, and guest connection for the selected group.

Table 11 describes the contents of the **Guest Access Overview** page:

Table 11: *Guest Access Overview Page*

Data Pane Item	Description
Time Range	Time range for the graphs and charts displayed on the **Overview** pane. You can choose to view graphs for a time period of 1 day, 1 week, and 1 month.
Guests	Number of guests connected to the SSIDs with Cloud Guest splash page profiles.
Guest SSID	Number of guest SSIDs that are configured to use the Cloud Guest splash page profiles.
Avg. Duration	The average duration of client connection on the SSIDs with Cloud Guest splash page profiles.

Data Pane Item	Description
MAX Concurrent Guests	Maximum number of client devices connected concurrently on the guest SSIDs.
Guest Connection Graph	Time stamp for the client connections on the cloud guest for the selected time range.
Guest Count by Authentication	Number of client devices based on the authentication type configured on the cloud guest SSIDs.
Guest count by SSID	Number of guest connections per SSID.
Client Type	Type of the client devices connected on the guest SSIDs.
Application Usage	The application usage by the guest clients connected to the APs on which the Deep Packet Inspection feature is enabled.

Creating Apps for Social Login

The following topics describe the procedures for creating applications to enable the social login feature:

- Creating a Facebook App on page 32
- Creating a Google App on page 33
- Creating a Twitter App on page 35
- Creating a LinkedIn App on page 36

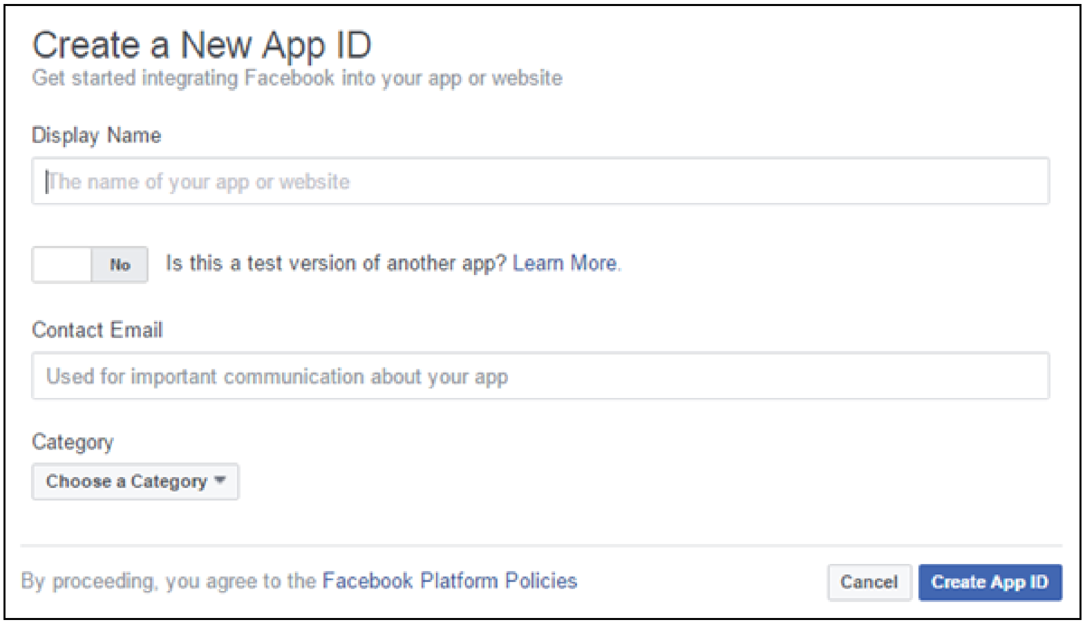
Creating a Facebook App

Before creating a Facebook app, ensure that you have a valid Facebook account and you are registered as a Facebook developer with that account.

To create a Facebook app, complete the following steps:

1. Visit the Facebook app setup URL at https://developers.facebook.com/apps.
2. From **My Apps**, select **Add a New App**.
3. Select **Website** as the type of app. If you have already created any apps, the list of apps is displayed.
4. To create a new app, click **Skip and Create App ID**.
5. In the subsequent pane, enter a name for the application. For example, SampleNetworks.
6. Click **Create New Facebook App ID**.
7. On the **Create a new App ID** pop-up pane:
   a. Specify a display name.
   b. Select **No** for **Is this a test version of another app?**
   c. Enter the contact email address.
   d. Select **Business** from the **Category** drop-down list.

Figure 1 *App ID Creation*



Create a New App ID

Get started integrating Facebook into your app or website

Display Name

The name of your app or website

Is this a test version of another app? Learn More.

Contact Email

Used for important communication about your app

Category

By proceeding, you agree to the Facebook Platform Policies

e. Click **Create App ID**. The **Security Check** page is displayed.

8. Complete the security check and click **Submit**. The **Setup SDK** page is displayed.
9. Scroll down to the **Tell Us about Your Website** section and enter the URL of your main site as shown in the following figure. For example, www.arubanetworks.com.
10. Click **Next**.
11. In the subsequent screen, click **Skip to Developer Dashboard** under **Next Steps**. The **App Dashboard** is displayed.
12. Click **Add Product**, and then click **Facebook Login** > **Get Started**.
13. On the **Getting Started** page, enter a valid Oauth redirect URL and append /oauth/reply at the end of the URL and click **Save Changes**.
14. Under Getting Started, click **app review** .
15. To make the app public, select **Yes** under **Make <app name> public**?
16. On the left pane, click the **Settings** icon. Note the app ID and app secret key. The app ID and secret key are required for configuring Facebook login in the Central UI.

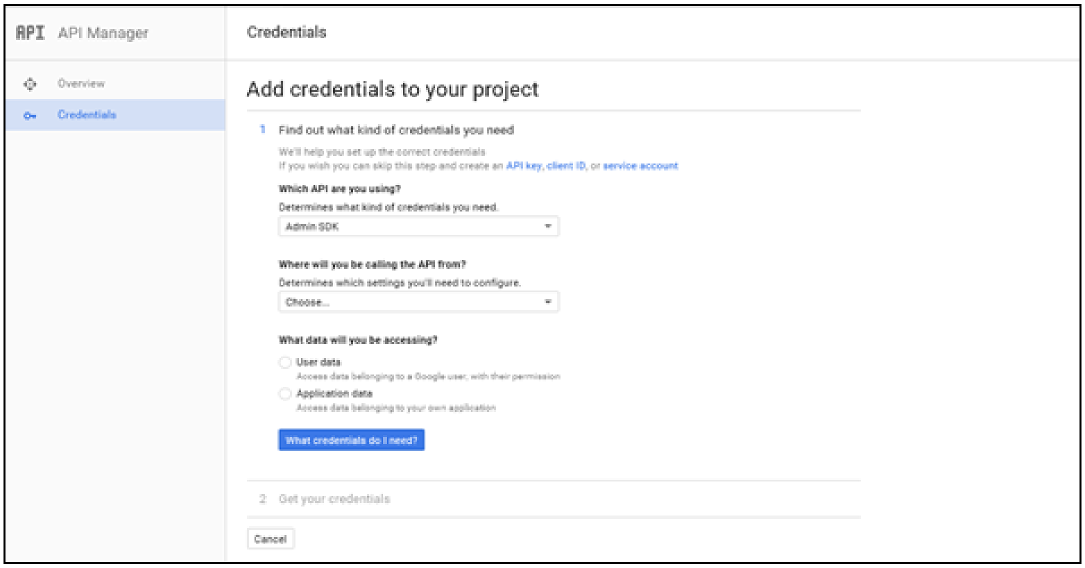
Creating a Google App

Before creating a Google app for Google+ based login, ensure that you have a valid Google+ account.

To create a Google+ app, complete the following steps:

1. Access the Google Developer site at https://code.google.com/apis/console.
2. Create a project if not already created.
3. Click the **Google API** settings icon > **API Manager**. The **Google API** window opens.
4. Under **Google Apps APIs**, click **Admin SDK**. The Admin SDK overview screen opens.
5. Click **Enable**.
6. Click **Go to Credentials**. The following page opens.

Figure 2 *Google+ Admin SDK Credentials*



API Manager

Overview

Credentials

Credentials

Add credentials to your project

1 Find out what kind of credentials you need

We'll help you set up the correct credentials
If you wish you can skip this step and create an API key, client ID, or service account

Which API are you using?
Determines what kind of credentials you need.
Admin SDK

Where will you be calling the API from?
Determines which settings you'll need to configure.
Choose...

What data will you be accessing?

○ User data
Access data belonging to a Google user, with their permission

○ Application data
Access data belonging to your own application

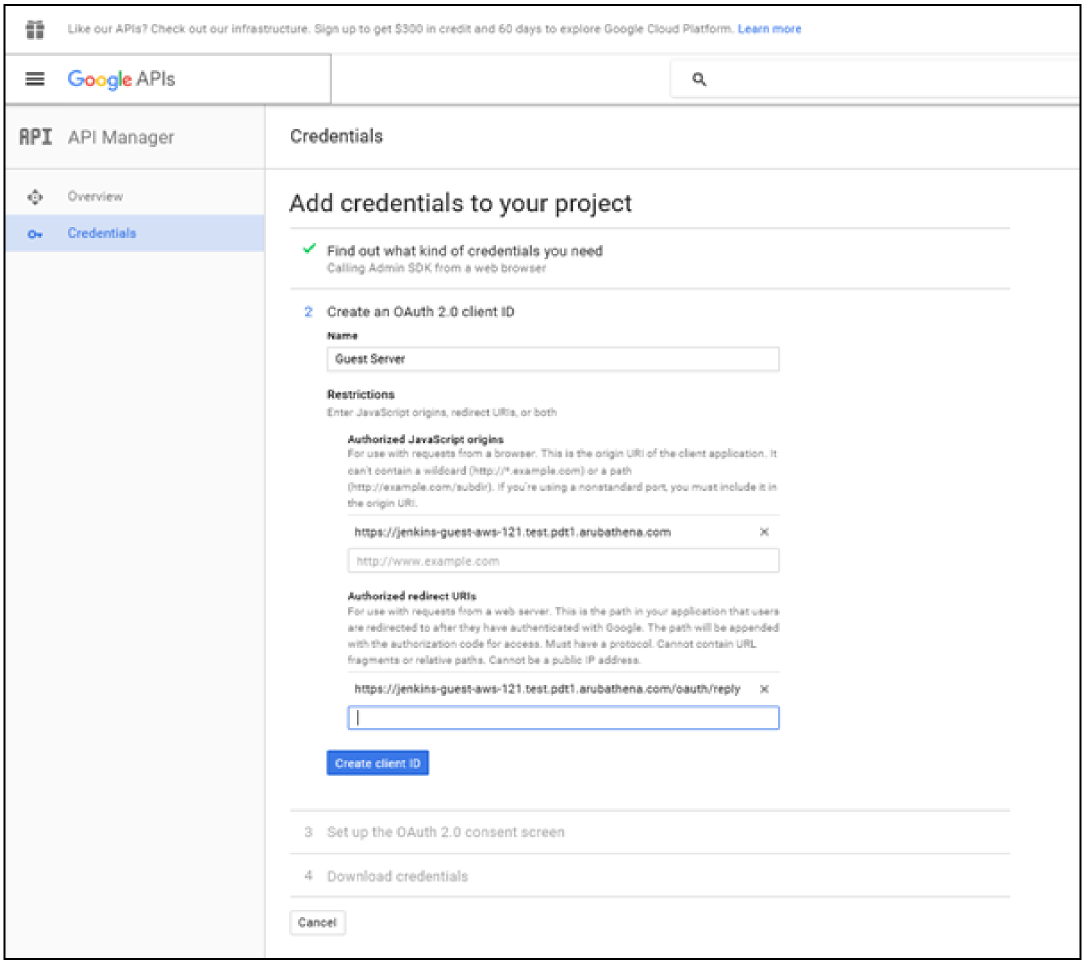
What credentials do I need?

2 Get your credentials

Cancel

7. Under the **Where will you be calling the API from** section, select **Web Browser**.
8. Under the **What data you will be accessing** section, select **User Data**.
9. Click **What Credentials do I need**. The following page opens.

Figure 3 *OAuth URLs*



Like our APIs? Check out our infrastructure. Sign up to get $300 in credit and 60 days to explore Google Cloud Platform. Learn more

Google APIs

API Manager

Overview

Credentials

Credentials

Add credentials to your project

✓ Find out what kind of credentials you need
Calling Admin SDK from a web browser

2 Create an OAuth 2.0 client ID

Name
Guest Server

Restrictions
Enter JavaScript origins, redirect URIs, or both

Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

https://jenkins-guest-aws-121.test.pdt1.arubathena.com ×

http://www.example.com

Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

https://jenkins-guest-aws-121.test.pdt1.arubathena.com/oauth/reply ×

Create client ID

3 Set up the OAuth 2.0 consent screen

4 Download credentials

Cancel

10. Enter the **OAuth 2.0 Client ID Name**.

11. Under **Authorized JavaScript Origins**, enter the base URL with FQDN of the cloud guest instance that will be hosting the captive portal. For example, https://%hostname%/.

12. Under **Authorized Redirect URIs**, enter the cloud server OAuth reply URL that includes the FQDN of the cloud server instance with /oauth/reply appended at the end of the URL.

NOTE

Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, https://example1.cloudguest.examplenetworks.com/oauth/reply.

13. Click **Create Client ID**.

14. Under **Set up the OAuth 2.0 consent screen**, provide your **Email Address** and product name, and then click **Continue**. The client ID is displayed.

15. Click **Done**. A page showing the OAuth IDs opens.

16. Click the **Oauth ID** to view the client ID and client secret key. The client ID and client secret key are required for configuring Google+ login in the Central UI.

Creating a Twitter App

Before creating a Twitter app, ensure that you have a valid Twitter account.

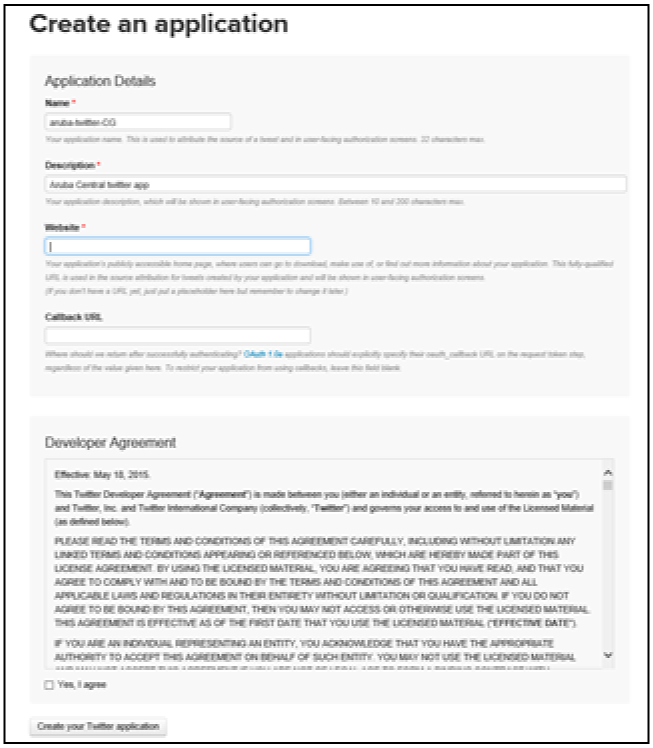
To create a Twitter app, complete the following steps:

1. Visit the Twitter app setup URL at https://apps.twitter.com.
2. Click **Create New App**. The **Create an application** web page is displayed.
3. Enter the application name and description.
4. For OAuth 2.0 Redirect URLs, enter the HTTPS URL of the cloud guest server to which you want to connect this social authentication source, and append /oauth/reply at the end of the URL.

NOTE

Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, https://exa.example.com/oauth/reply.

Figure 4 *Twitter App Creation*



Create an application

Application Details

Name *

aruba-twitter-CG

Your application name. This is used to attribute the source of a tweet and in user-facing authorization screens. 32 characters max.

Description *

Aruba Central twitter app

Your application description, which will be shown in user-facing authorization screens. Between 10 and 200 characters max.

Website *

Your application's publicly accessible home page, where users can go to download, make use of, or find out more information about your application. This fully-qualified URL is used in the source attribution for tweets created by your application and will be shown in user-facing authorization screens.
(If you don't have a URL yet, just put a placeholder here but remember to change it later.)

Callback URL

Where should we return after successfully authenticating? OAuth 1.0a applications should explicitly specify their oauth_callback URL on the request token step, regardless of the value given here. To restrict your application from using callbacks, leave this field blank.

Developer Agreement

Effective: May 18, 2015.

This Twitter Developer Agreement ("Agreement") is made between you (either an individual or an entity, referred to herein as "you") and Twitter, Inc. and Twitter International Company (collectively, "Twitter") and governs your access to and use of the Licensed Material (as defined below).

PLEASE READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY, INCLUDING WITHOUT LIMITATION ANY LINKED TERMS AND CONDITIONS APPEARING OR REFERENCED BELOW, WHICH ARE HEREBY MADE PART OF THIS LICENSE AGREEMENT. BY USING THE LICENSED MATERIAL, YOU ARE AGREEING THAT YOU HAVE READ, AND THAT YOU AGREE TO COMPLY WITH AND TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT AND ALL APPLICABLE LAWS AND REGULATIONS IN THEIR ENTIRETY WITHOUT LIMITATION OR QUALIFICATION. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, THEN YOU MAY NOT ACCESS OR OTHERWISE USE THE LICENSED MATERIAL. THIS AGREEMENT IS EFFECTIVE AS OF THE FIRST DATE THAT YOU USE THE LICENSED MATERIAL ("EFFECTIVE DATE").

IF YOU ARE AN INDIVIDUAL REPRESENTING AN ENTITY, YOU ACKNOWLEDGE THAT YOU HAVE THE APPROPRIATE AUTHORITY TO ACCEPT THIS AGREEMENT ON BEHALF OF SUCH ENTITY. YOU MAY NOT USE THE LICENSED MATERIAL

☐ Yes, I agree

5. Select **Yes, I agree** to accept the Developer Agreement terms.

6. Click **Create a Twitter application**.

7. Click **Manage Keys and Access Tokens**. The **Keys and Access Tokens** tab opens. The consumer key (API key) and consumer secret (API key) are displayed.

8. Note the ID and the secret key. The API key and API secret key are required for configuring Twitter login in Central UI.

Creating a LinkedIn App

Before creating a LinkedIn app, ensure that you have a valid LinkedIn account.

To create a LinkedIn app, complete the following steps:

1. Visit the LinkedIn app setup URL at https://developer.linkedin.com.

2. Click **My Apps**. You will be redirected to https://www.linkedin.com/secure/developer/apps.

3. Click **Create Application**. The **Create a New Application** web page is displayed.

4. Enter your company name, application name, description, website URL, application logo with the specification mentioned, application use, and contact information.

5. Click **Submit**. The **Authentication** page is displayed.

6. Note the client ID and client secret key displayed on the **Authentication** page.

7. For **OAuth 2.0 Redirect URLs**, enter the HTTPS URL of the cloud guest server to which you want to connect this social authentication source and append /oauth/reply at the end of the URL.

8. Click **Add** and then click **Update**. The API and secret keys are displayed.

9. Note the API and secret key details. The API ID and secret key are required for configuring LinkedIn login in the Central UI.

Configuring a Cloud Guest Splash Page Profile

Note for the Managed Service Portal Users

Both the Managed Service Portal and the Central Standard Enterprise Portal allow the configuration of Splash Page profiles. However, the customer accounts inherit the Splash Pages configuration from the Managed Service Portal.

Changes to the Splash Pages in the Managed Service Portal are propagated to all associated customer accounts. The Splash Page configuration inherited from the Managed Service Portal cannot be edited by the admin users of the end customer accounts.

The Managed Service Portal admin users can delete only those Splash Pages that are not linked to any customer account.

This topic describes the following procedures:

- Adding a Cloud Guest Splash Page Profile on page 36
- Configuring a Cloud Guest Splash Page Profile on page 36
- Associating a Splash Page Profile to an SSID on page 41

Adding a Cloud Guest Splash Page Profile

To create a splash page profile:

1. Click **Guest Access** on the bottom left pane. The guest access configuration and management menu options are displayed.

2. Click **Splash Page**. The **Splash Page** pane is displayed.
3. To create a new Splash page, Click the + icon. The **New Splash Page** pane is displayed.
4. On the **Configuration** tab, configure the parameters described in the following table:

Table 12: *Splash Page Configuration*

Data Pane Content	Description
Name	Enter a unique name to identify the splash profile.
Type	Configure any of the following authentication methods to provide a secure network access to the guest users and visitors. ▪ **Anonymous** ▪ **Authenticated** ▪ **Facebook Wi-Fi**
Anonymous	Configure the **Anonymous** login method if you want to allow guest users to log in to the Splash page without providing any credentials. For anonymous user authentication, you can also enable a pre-shared key to allow access. To enable a pre-shared key based authentication, set the **Guest Key** to on and specify a password.
Authenticated	Configure authentication and authorization attributes, and login credentials that enable users to access the Internet as guests. You can configure an authentication method based on sponsored access and social networking login profiles. The authenticated options available for configuring the cloud guest splash page are described in the following rows.
Username/Password	The **Username/Password** based authentication method allows pre-configured visitors to obtain access to wireless connection and the Internet. The visitors or guest users can register themselves by using the splash page when trying to access the network. The password is delivered to the users through print, SMS or email depending on the options selected during registration. To allow the guest users to register by themselves: 1. Enable **Self-Registration**. 2. Set the **Verification Required** to **ON** if the guest user account must be verified. 3. Specify a verification criteria to allow the self-registered users to verify through email or phone. ▪ If email-based verification is enabled and the **Send Verification Link** is selected, a verification link is sent to the email address of the user. The guest users can click the link to obtain access to the Internet. ▪ If phone-based verification is enabled, the guest users will receive an SMS. The administrators can also customize the content of the SMS by clicking on **Customize SMS**. 4. Specify the duration within the range of 1-60 minutes, during which the users can access free Wi-Fi to verify the link. The users can log in to the network for the specified duration and click the verification link to obtain access to the Internet. By default, the expiration date for the accounts of self-registered guest users is set to infinite during registration. The administrator or the guest operator can set the expiration date after registration.
Social Login	**Social Login**—Enable this option to allow guest users to use their existing login credentials from social networking profiles such as Facebook, Twitter, Google+, or LinkedIn and sign into a third-party website. When a social login based profile is configured, a new login account to access the guest network or third-party websites is not required. ▪ **Facebook**— Allows guest users to use their Facebook credentials to log in to the splash page. To enable Facebook integration, you must create a Facebook app and obtain the app ID and secret key. For more information on app creation, see Creating a Facebook App. Enter the app ID and secret key for client ID and client Secret respectively to complete the integration.

Table 12: *Splash Page Configuration*

Data Pane Content	Description
	- **Twitter**—Allows guest users to use their Twitter credentials to log in to the splash page. To enable Twitter integration, you must create a Twitter app and obtain the app ID and secret key. For more information, see Creating a Twitter App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration. - **Google+**—Allows guest users to use their Google+ credentials to log in to the splash page. To enable Google+ integration, you must create a Google app and obtain the app ID and secret key. For more information, see Creating a Google App on page 33. 1. Enter the app ID and secret key for client ID and client secret respectively. 2. To restrict authentication attempts to only the members of a Google hosted domain, enter the domain name in the **Gmail for Work Domain** text box. Ensure that you have a valid domain account licensed by Google Domains or Google Apps. For more information see: - https://apps.google.com/intx/en_in/ - https://domains.google.com/about/ 3. Specify a text for the Sign-In button. - **LinkedIn**—Allows guest user to use their LinkedIn credentials to log in to the splash page. To enable LinkedIn integration, you must create a LinkedIn app and obtain the app ID and secret key. For more information, see Creating a LinkedIn App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration.
Facebook Wi-Fi	If you want to enable network access through the free Wi-Fi service offered by Facebook. Select the **Facebook Wi-Fi** option. The Facebook Wi-Fi feature allows you to pair your network with a Facebook business page, thereby allowing the guest users to log in from Wi-Fi hotspots using their Facebook credentials. After selecting the Facebook Wi-Fi option, complete the following steps to continue with the Facebook Wi-Fi configuration. 1. Click the **Configure Now** link. 2. Sign in to your Facebook account. 3. If you do not have a business page, click **Create Page**. For more information on setting Facebook Wi-Fi service, see **Setting up Facebook Wi-Fi for Your Business** at https://www.facebook.com/help/126760650808045. If the Facebook Wi-Fi business page is set up, when the users try to access the Internet, the browser redirects the user to the Facebook page. The user can log in with their Facebook account credentials and can either check in to access free Internet or skip checking in and then continue. **NOTE:** AP devices support Facebook Wi-Fi services on their own, without Central. However, for enabling social login based authentication, the guest splash pages must be configured in Central. For more information on Facebook Wi-Fi configuration on an AP, see the *Aruba Instant User Guide*.
Allow Internet In Failure	To allow users access the Internet when the external captive portal server is not available, click the **Allow Internet In Failure** toggle switch. By default, this option is disabled.
Override Common Name	To override the default common name, click the **Override Common Name** toggle switch and specify a common name. The common name is the web page URL of the guest access portal. By default, the common name is set to **securelogin.arubanetworks.com**. The guest users can override this default name by adding their own common name. If your devices are managed by AirWave and you want to use your own certificate for the captive portal service, ensure that the captive portal certificate is pushed to the Instant AP from the AirWave management system. When the appropriate certificate is loaded on the AP, perform the following actions: 1. Run the **show captive-portal-domains** command at the Instant AP command prompt. 2. Note the common name or the internal captive portal domain name. 3. Add this domain name in the **Override Common Name** field on the **Splash Page**

Table 12: *Splash Page Configuration*

Data Pane Content	Description
	configuration page. 4. Save the changes.
Authentication Success Behavior	If **Anonymous** or **Authenticated** option is selected as the guest user authentication method, specify a method for redirecting the users after a successful authentication. Select one of the following options: ▪ **Redirect to Original URL**— When selected, upon successful authentication, the user is redirected to the URL that was originally requested. ▪ **Redirect URL**—Specify a redirect URL if you want to override the original request of users and redirect them to another URL.
Authentication Failure Message	If the **Authenticated** option is selected as the guest user authentication method, enter the authentication failure message text string returned by the server when the user authentication fails.
Session Timeout	Enter the maximum time in Day(s): Hour(s): Minute(s) format for which a client session remains active. The default value is 0:8:00. When the session expires, the users must re-authenticate. If MAC caching is enabled, the users are allowed or denied access based on the MAC address of the connective device.
Share This Profile	Select this check box if you want to allow the users to share the Splash Page profile. The Splash Page profiles under All Groups can be shared across all the groups.
Simultaneous Login Limit	To set limit for the simultaneous logins from the same user for authenticated Splash Page profiles, select a value from the **Simultaneous Login Limit** drop-down list.
Daily Usage Limit	To configure the connection time or data usage limit per day for the guest users, specify the following parameters: ▪ By Time—Specify the number of hours, minutes and the timezone. ▪ By Data—Specify the data usage limit.
Whitelist URL	To allow a URL, click + and add the URL to the whitelist. For example, if the terms and conditions configured for the guest portal include URLs, you can add these URLs to the whitelist, so that the users can access the required web pages.

5. Click **Next**. The **Customization** pane appears. Configuring a Cloud Guest Splash Page Profile on page 36.

NOTE

You can edit or delete a splash page profile by clicking the respective icons in the **Splash Page Profile** pane.

Customizing a Splash Page Design

To customize a splash page design, on the **Guest Access > Splash Page > New Splash Page > Customization** pane, configure the parameters described in the following table:

Table 13: *Splash page customization*

Data Pane Content	Description
Background Color	To change the color of the splash page, select a color from the **Background Color** palette.
Button Title	Specify a title for the sign in button.
Button Color	To change the color of the sign in button, select a color from the **Button Color** palette.
Page Font Color	To change the font color of the text on the splash page, select a color from the **Page Font Color**.
Font Color	Select the font color of the splash page.
Logo	To upload a logo, click **Browse**, and browse the image file.
Background Image	Click **Browse** to upload a background image.
Page Title	Add a suitable title for the splash page.
Welcome Text	Enter the welcome text to be displayed on the splash page.
Terms & Conditions	Enter the terms and conditions to be displayed on the splash page. The text box also allows you to use HTML tags for formatting text. For example, to highlight text with italics, you can wrap the text with the <i> </i> HTML tag. Specify an acceptance criteria for terms and condition by selecting any of the following options from the **Display "I Accept" Checkbox**: ■ **No, Accept by default** ■ **Yes, Display Checkbox** If the **I ACCEPT** check box must be displayed on the Splash page, select the display format for terms and conditions.
Ad Settings	If you want to display advertisements on the splash page, enter the URL of the advertisement and upload the image for the advertisement.

6. Click **Preview** to preview the customized splash page or click **Finish**.

Previewing and Modifying a Splash Page Profile

To preview a splash page profile, complete the following steps:

1. Select **Guest Access > Splash Page**. A list of splash Page profiles is displayed.
2. Ensure that the pop-up blocker on your browser window is disabled.
3. Click the preview icon next to profile you want to preview. The Splash Page is displayed in a new window.

The **Splash Pages** page also allows you to perform any of the following actions:

- To view the Splash Page configuration text in an overlay window, click the settings icon next to the profile. You can copy the configuration text and apply it to AirWave managed APs using configuration templates.
- To modify a splash page profile, click the edit icon next to the profile form list of profiles displayed in the Splash Page Profiles pane.
- To delete a profile, select the profile and click the delete icon next to the profile.

Associating a Splash Page Profile to an SSID

To associate a splash page profile with an SSID, complete the following steps:

1. Select **Configuration > Access Points > Networks** and then click **Create New**. The **Create a New Network** pane is displayed.
2. For **Type**, select **Wireless**.
3. Enter a name that is used to identify the network in the **Name(SSID)** box.
4. For **Primary Usage**, select **Guest** and click **Next**.
5. In the **VLANs** tab, if required, configure a VLAN assignment mode, and then click **Next**.
6. In the **Security** tab:
   a. Select **Cloud Guest** from the **Splash Page Type** list.
   b. Select the splash page profile name from the **Guest Captive Portal Profile** list and click **Next**.

NOTE

If the user configures the default Aruba certificate, the **You are using Aruba default certificate. You shall configure new certificate** alert message is displayed for the user to configure a new certificate.

   c. To enable encryption, set **Encryption** to **Enabled** and configure encryption parameters.
   d. To exclude uplink, select an uplink from **Disable If Uplink Type Is**.
   e. Click **Next**.
7. In the **Access** tab, if required, modify and create access rules set the configuration if required, and then click **Finish**.

Glossary of Terms

The following table provides a brief description of the terminology used in this guide.