6ABSCG0006-29A
June 2015

Configuration Guide

Layer 7 Device/OS Fingerprinting in vWLAN

This configuration guide provides configuration information for Layer 7 device and operating system (OS) fingerprinting in ADTRAN Bluesocket virtual wireless local area network (vWLAN) products. Included in this guide are an overview of Layer 7 device/OS fingerprinting, the configuration steps necessary for device/OS fingerprinting support, and methods to view device information in the vWLAN reporting dashboard.

This guide consists of the following sections:

Overview

Layer 7 device/OS fingerprinting is a feature that provides status information, statistics, analytics, and reports based on the device type, operating system, manufacturer, host name, and ownership (corporate/business owned, or "guest") of devices being used on the vWLAN network. In addition, device-specific connection policies can be enforced based on the device type and ownership. This feature allows you track Apple IOS, Android, Windows, MAC OS, and other operating systems while in use on the vWLAN network. Layer 7 device/OS fingerprinting is part of vWLAN's context-aware role-based access control where vWLAN examines user credentials, device type, device ownership, location, and date and time to enforce a policy.

When Layer 7 device/OS fingerprinting is configured in vWLAN, as a device connects to the network, its transmitted Dynamic Host Control Protocol (DHCP) discovery packet is inspected for Option 55 which includes the device's fingerprint information (device type, operating system, and vendor). This information is sent to the vWLAN system which then determines the device's role in the vWLAN network based on the detected device fingerprint and the device configuration options in vWLAN. Roles can be configured so that a matrix of rules is enforced based on the detected device information, allowing network administrators to control network access, bandwidth usage, and other network resources based on a device's reported information.

Hardware and Software Requirements and Limitations

Layer 7 device/OS fingerprinting support is available on vWLAN systems running firmware release 2.6 or later and Bluesocket access point (BSAP) models using firmware 7.0.0.

Layer 7 device/OS fingerprinting takes place only if the connecting device supports it by providing DHCP Option 55 information.

Layer 7 Device/OS Fingerprinting and Device Authentication

Prior to vWLAN firmware release 2.6, when clients connected to an SSID with configured captive portal, clients were placed in the unregistered role and all web traffic was redirected to the captive portal login page. In this configuration, the client initially receives an Network Access Control (NAC) IP address (10.252.X.X by default) with a short lease time from the AP, and then the Hypertext Transfer Protocol (HTTP) request is redirected to https://vWLAN-ip/login.pl. The credentials entered by the client are sent to vWLAN and authenticated against the administrator chosen authentication method. The client is then placed into the proper authenticated role, based on the result of that authentication, and receives an IP address on their target location/network, and begins to pass traffic.

Some client devices do not properly release their NAC IP address to obtain a new IP address in their newly authenticated network, which prevents them from passing traffic. Prior to vWLAN 2.6 release, these devices had to be manually disconnected and reconnected to the vWLAN network to pass traffic once authenticated. With selective deauthentication, included in the Layer 7 device/OS fingerprinting feature in vWLAN 2.6, the BSAPs automatically detect devices that keep their NAC IP address. BSAPs will now quickly deauthenticate them so that they will automatically reconnect to vWLAN, obtain a new IP address from the authenticated network subnet, and begin transmitting data without the need for manual vWLAN administrator or client intervention. You can find more information about this feature in the *Selective Deauthentication* guide available online at https://supportforums.adtran.com.

Using vWLAN firmware 2.6, user roles can now be configured to assign a role to the connecting device based on its fingerprint. Roles configured for any authentication mechanism (Service Set Identifier (SSID), Medium Access Control (MAC), RADIUS 1X, or web authentication) are overwritten by any new role assigned by device fingerprint information.

Layer 7 Device Fingerprinting Limitations

There are some known Layer 7 device fingerprinting limitations caused by device-specific inadequate reporting of DHCP Option 55. These device-specific limitations and their observed behavior are tracked online in the ADTRAN Support community. You can access this information here.

Configuring Layer 7 Device/OS Fingerprinting

When a device connects to vWLAN, the device type (operating system) is added to the vWLAN system. Based on the detected device type, the device is placed into a user role once it connects to the system. Roles can be configured so that access rules are applied to device types upon authentication.

Devices can also be categorized by ownership: corporate or other. This allows rules to be configured based on device ownership that allow corporate devices to be given a different role than a non-corporate device of the same type.

There are two components to configuring Layer 7 device/OS fingerprinting on vWLAN: adding a device to the vWLAN system, and specifying the rules applied to the device type as it is placed in a user role. Each device can be added to the vWLAN system individually, or a bulk upload of device information can be performed. These configuration steps can be done in any order, and are outlined in these sections:

- *Configuring Roles for Layer 7 Device/OS Fingerprinting on page 3*
- *Configuring MAC Device Authentication for Device Fingerprinting on page 5*
- *Bulk Import of Devices for Device Fingerprinting on page 7*

Once the devices are added and the role rules are specified, you can use the vWLAN dashboard to track information about each device as it uses the network (refer to *Viewing Layer 7 Devices Using the Reporting Dashboard on page 8*).

Configuring Roles for Layer 7 Device/OS Fingerprinting

Domain roles are the roles of users that are connected to a specific domain, and include such features as firewall behavior, location elements, quality of service (QoS) settings, and class of service (CoS) settings. User roles in vWLAN define the policy enforced per user at the AP before forwarding user traffic, based on traffic flow (location, firewall policies), bandwidth management, and packet marking and prioritization.

The role in which a user is placed is determined by the following items (in order):

1. Layer 7 Device/OS Fingerprint (device type and ownership)

2. MAC authentication

3. Wildcard MAC authentication

4. The default role from the SSID (unless the SSID is 802.1X, then the role from the RADIUS 1X server is used.)

5. If the role remains unregistered at this point, the user can use web-based authentication to log in to any role.

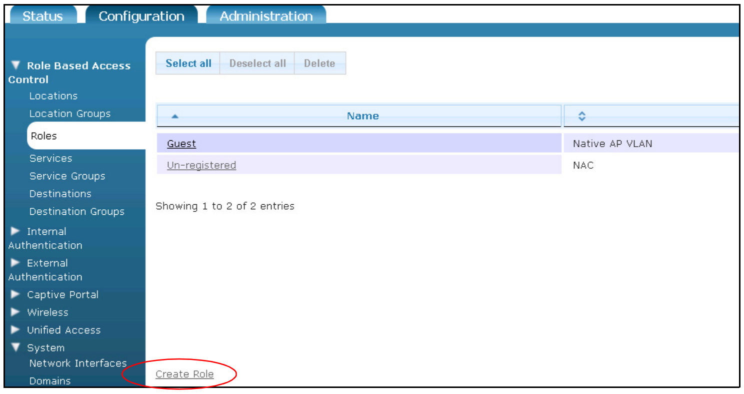
By default, when a user connects for the first time and has not been authenticated, the user's role is unregistered.

When configuring a user role, it is important to realize that the user role determines where and how the client's traffic flows. You must specify the name of a user role, the location associated with the role, the CoS settings for the role, the bandwidth shaping parameters for the role, post-login redirection parameters, the firewall policies applied to the role, and the device rules applied to the role (Layer 7 fingerprint). By default, two roles exist: **Un-registered** (which cannot be deleted) and **Guest**. The unregistered role causes users to have their Internet traffic redirected to vWLAN for authentication. While in the unregistered role, the AP serves the user a DHCP address. When the user moves out of the unregistered role (by being authenticated), the AP locally switches the traffic, and the user receives a DHCP address from the network. In addition to the two default roles, up to 251 roles can be created.

> NOTE
>
> *With the included support of Layer 7 device/OS fingerprinting, BSAPs automatically detect devices that do not authenticate correctly (retain their NAC IP address), and quickly deauthorize them so they will automatically reconnect to vWLAN for authentication. This process is known as selective deauthentication.*

Roles are all configurable from the **Configuration** tab. To configure the user roles, follow these steps:

1. Navigate to the **Configuration** tab, and select **Role Based Access Control** > **Roles**. Any previously configured roles will be listed in the menu. To edit a previously created role, select the role name from the list. To create a new role, either select **Create Role** at the bottom of this menu, or select **Domain Role** from the **Create** drop-down menu (at the top of the menu).



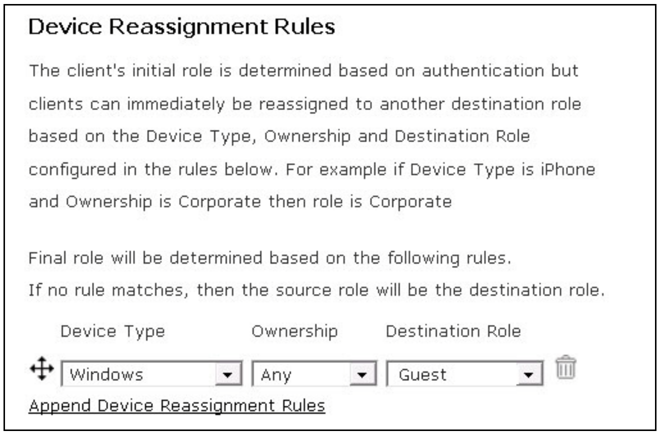
Name	
Guest	Native AP VLAN
Un-registered	NAC

Showing 1 to 2 of 2 entries

6. Define the parameters of the new role. This includes the role name, location elements, and QoS, CoS, and firewall settings. For more information about detailed role configuration, refer to the *vWLAN Administrator's Guide*, available online at https://supportforums.adtran.com.

7. After specifying the role parameters, configure the device rules for the role. The device rules specify the role a detected device is to use based on the device's fingerprint. The fingerprint includes the device's type and ownership (corporate or other). When the device is detected on the vWLAN network, the device is placed in the role that was specified in the **Destination Role** drop-down menu. This role overrides all other role specifications (including those specified in SSID, MAC, RADIUS,

and web authentication methods). Use the drop-down menus to specify the device's type, ownership, and destination role.



Device Reassignment Rules

The client's initial role is determined based on authentication but clients can immediately be reassigned to another destination role based on the Device Type, Ownership and Destination Role configured in the rules below. For example if Device Type is iPhone and Ownership is Corporate then role is Corporate

Final role will be determined based on the following rules.
If no rule matches, then the source role will be the destination role.

Device Type	Ownership	Destination Role
Windows	Any	Guest

8. After you have configured the user role's name, location, CoS and QoS parameters, firewall restrictions, and device role, select **Create Role** at the bottom of the menu to create the role.

9. A confirmation is displayed indicating that the role has been created. The role will now appear in the role list (**Configuration** tab, **Role Based Access Control** > **Roles**), where you can display, edit, or delete the role.

Configuring MAC Device Authentication for Device Fingerprinting

vWLAN maintains a local device authentication database. Each local device authentication database record consists of the following:

- Device name
- MAC address
- Statically assigned role

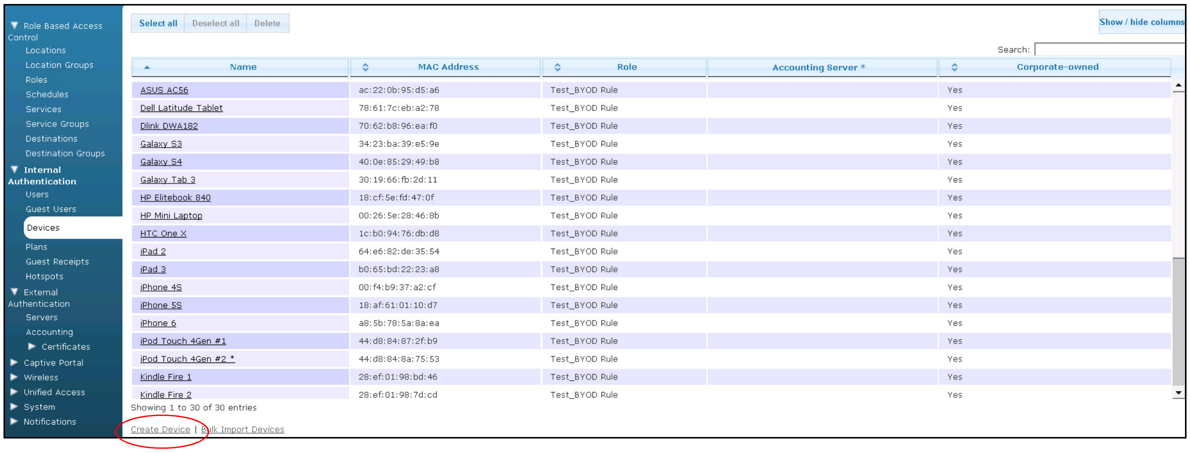
In addition, vWLAN has the ability to use wildcard MAC address authentication to place devices in a role based on the organizationally unique identifier (OUI) or vendor. When configuring a wildcard MAC or a MAC address range for a device, use the wildcard character **%%**. For example, if you were configuring a Polycom phone for MAC authentication, beginning with the OUI of **00:90:7a**, and placing the phone into a determined role, you can use the MAC address **00:90:7a:%%:%%:%%**. Wildcards are only allowed on the last three octets of the MAC address.

> NOTE *In scenarios where the same MAC address can match a wildcard MAC address, and a standard MAC device, the MAC device takes precedence.*

The Layer 7 device/OS fingerprinting feature allows you to specify the type of device when adding it to the vWLAN system. Detected device information includes the device type, operating system, and vendor information. When the new device is added, you can specify whether the device is a corporate device, or another type of device (**other**). This feature allows vWLAN to detect the ownership of the device when it connects to the vWLAN network, and automatically associates the device with a user role (configured in **Configuration** > **Roles**). In addition, you can add devices to vWLAN using a bulk import method.

To configure a device for use in device authentication, follow these steps:

1. Navigate to the **Configuration** tab, and select **Internal Authentication** > **Devices**. Any previously configured devices will be listed in the menu. To edit a previously created device, select the device name from the list. To create a new device, either select **Create Device** at the bottom of this menu, or select **Domain Device** from the **Create** drop-down menu (at the top of the menu).

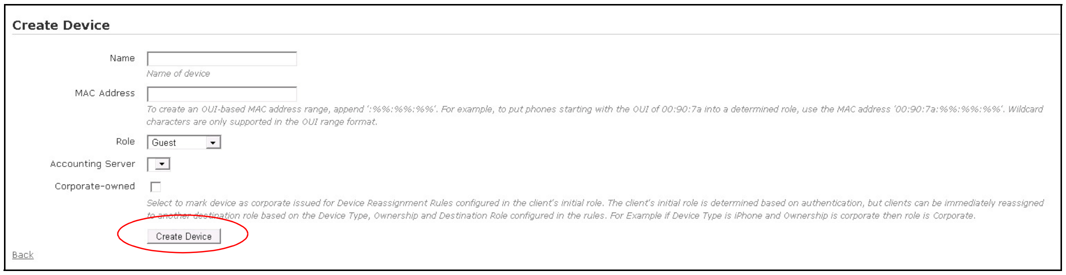


Name	MAC Address	Role	Accounting Server *	Corporate-owned
ASUS AC56	ac:22:0b:95:d5:a6	Test_BYOD Rule		Yes
Dell Latitude Tablet	78:61:7c:eb:a2:78	Test_BYOD Rule		Yes
Dlink DWA182	70:62:b8:96:ea:f0	Test_BYOD Rule		Yes
Galaxy S3	34:23:ba:39:e5:9e	Test_BYOD Rule		Yes
Galaxy S4	40:0e:85:29:49:b8	Test_BYOD Rule		Yes
Galaxy Tab 3	30:19:66:fb:2d:11	Test_BYOD Rule		Yes
HP Elitebook 840	18:cf:5e:fd:47:0f	Test_BYOD Rule		Yes
HP Mini Laptop	00:26:5e:28:46:8b	Test_BYOD Rule		Yes
HTC One X	1c:b0:94:76:db:d8	Test_BYOD Rule		Yes
iPad 2	64:e6:82:de:35:54	Test_BYOD Rule		Yes
iPad 3	b0:65:bd:22:23:a8	Test_BYOD Rule		Yes
iPhone 4S	00:f4:b9:37:a2:cf	Test_BYOD Rule		Yes
iPhone 5S	18:af:61:01:10:d7	Test_BYOD Rule		Yes
iPhone 6	a8:5b:78:5a:8a:ea	Test_BYOD Rule		Yes
iPod Touch 4Gen #1	44:d8:84:87:2f:b9	Test_BYOD Rule		Yes
iPod Touch 4Gen #2 *	44:d8:84:8a:75:53	Test_BYOD Rule		Yes
Kindle Fire 1	28:ef:01:98:bd:46	Test_BYOD Rule		Yes
Kindle Fire 2	28:ef:01:98:7d:cd	Test_BYOD Rule		Yes

Showing 1 to 30 of 30 entries

Create Device | Bulk Import Devices

2. Enter the name of the device, the MAC address of the device, and the device's assigned role. Optionally, associate the device with an accounting server by selecting an accounting server from the **Accounting server** drop-down menu. Optionally specify whether the device is a corporate-owned device (by selecting the **Corporate-Owned** check box), or specify the device is owned by someone else (by leaving the check box deselected). By default, the device is not configured as a corporate-owned entity. The role associated with the device can be specified in this menu, but if there is a role specified for the detected device type (refer to *Configuring Roles for Layer 7 Device/OS Fingerprinting on page 3*), that role will take precedence.



Name	 *Name of device*
MAC Address	 *To create an OUI-based MAC address range, append ':%%:%%:%%'. For example, to put phones starting with the OUI of 00:90:7a into a determined role, use the MAC address '00:90:7a:%%:%%:%%'. Wildcard characters are only supported in the OUI range format.*
Role	Guest
Accounting Server	
Corporate-owned	☐ *Select to mark device as corporate issued for Device Reassignment Rules configured in the client's initial role. The client's initial role is determined based on authentication, but clients can be immediately reassigned to another destination role based on the Device Type, Ownership and Destination Role configured in the rules. For Example if Device Type is iPhone and Ownership is corporate then role is Corporate.*
	Create Device

3. Select **Create Device**. A confirmation is displayed indicating that the device has been created. The device will now appear in the device list (**Configuration** tab, **Internal Authentication** > **Devices**), where you can display, edit, or delete the device.

4. The device will now be authenticated using MAC device authentication.

NOTE *In vWLAN, 802.1X authentication can override MAC authentication. Therefore, if you match MAC authentication, and then complete 802.1X authentication, your role is determined by RADIUS 1X and not the device.*

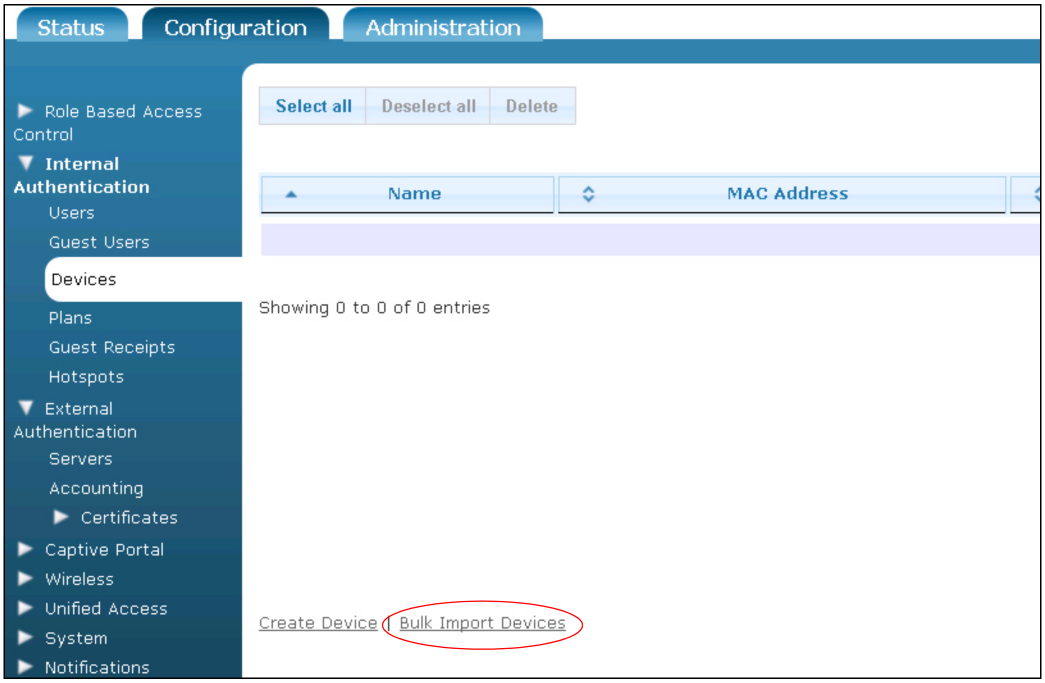
Bulk Import of Devices for Device Fingerprinting

In addition to adding devices to vWLAN one at a time, you can choose to import several devices at one time using the bulk import option. This option imports a comma separated value (CSV) file that should include the device name, MAC address, assigned role, and associated accounting server (optional). The CSV file should look like the following example:

```
finename19,00:0c:22:55:b0:13,5,2
finename20,00:0c:22:55:b0:14,5
finename21,00:0c:22:55:b0:15,5,2
finename22,00:0c:22:55:b0:16,5,2
finename23,00:0c:22:55:b0:17,5,2
finename24,00:0c:22:55:b0:18,5,2
```

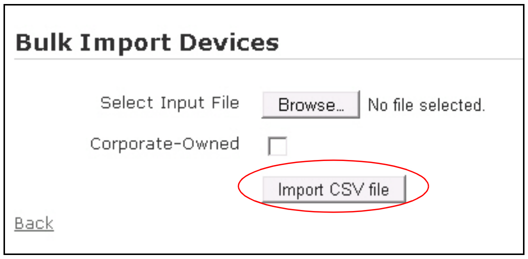
To import a CSV file of devices, follow these steps:

1. Navigate to the **Configuration** tab, and select **Internal Authentication** > **Devices**. Select **Bulk Import Devices** at the bottom of this menu.



Showing 0 to 0 of 0 entries

2. In the **Bulk Import Devices** menu, use the **Browse** button to locate the CSV file that contains the information for the devices you are adding to vWLAN. Next, specify whether the devices are corporate-owned or not by selecting the **Corporate-Owned** check box. Select **Import CSV file** to import the file.



Bulk Import Devices

Select Input File: Browse... No file selected.

Corporate-Owned: □

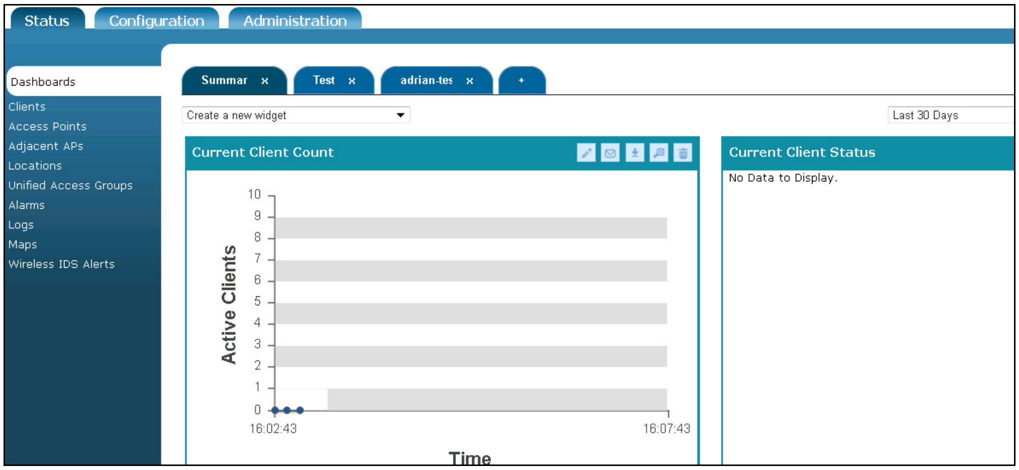
3. The imported devices will now appear in the device list (**Configuration** tab, **Internal Authentication** > **Devices**).

Viewing Layer 7 Devices Using the Reporting Dashboard

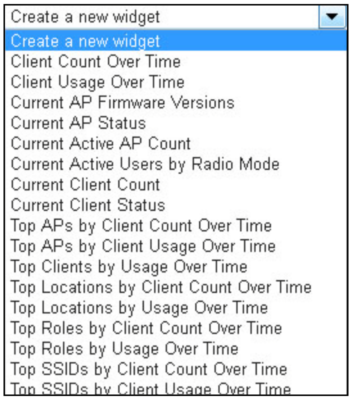
The vWLAN reporting dashboard is a collection of customized widgets that are available for you to view vWLAN information at a glance. Dashboards are used by administrators to view information about users, APs, roles, locations, SSIDs, bandwidth usage, and many other parameters used within the domain. Up to 12 widgets (2 x 6) can be configured on any one dashboard. Widgets can display either current information in real time or historical information over time. Current widgets update in real time while being viewed, and historical, over-time widgets present historical data over a specified amount of time (last 7 days, last 30 days, etc.). In addition, the details of any users, APs, roles, etc. can be viewed by selecting the item displayed in the widget. Domain administrators can configure which widgets are displayed, and thus which features of the domain to track, by selecting a widget to create. Creating multiple widgets allows you to create a perspective of the vWLAN network, both historically and in real time. With the exception of the logo, each administrator's dashboard is completely separate from any others and can be fully customized to the individual's preference.

To use the reporting dashboard, follow these steps:

1. Navigate to the **Status** tab and select **Dashboards**.



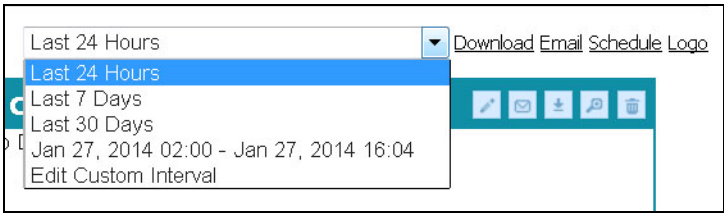
2. To specify which information is summarized on the dashboard, create the appropriate widget from the **Create a new widget** drop-down menu.


Create a new widget
Create a new widget
Client Count Over Time
Client Usage Over Time
Current AP Firmware Versions
Current AP Status
Current Active AP Count
Current Active Users by Radio Mode
Current Client Count
Current Client Status
Top APs by Client Count Over Time
Top APs by Client Usage Over Time
Top Clients by Usage Over Time
Top Locations by Client Count Over Time
Top Locations by Usage Over Time
Top Roles by Client Count Over Time
Top Roles by Usage Over Time
Top SSIDs by Client Count Over Time
Top SSIDs by Client Usage Over Time

The widgets used for Layer 7 device fingerprinting summarize the following information:

- **Current Clients by Device OS** is a summary of associated wireless client’s operating systems. This is a current widget that displays information in real time.
- **Current Clients by Device Type** is a summary associated wireless client’s device types. This is a current widget that displays information in real time.
- **Current Client Statistics by Device Ownership** is a summary of associated wireless client’s device ownership (corporate or other). This is a current widget that displays information in real time.
- **Client Count by Device Type Over Time** is a summary of client counts based on device type. This is a historical widget.
- **Client Count by Device Ownership Over Time** is a summary of client counts based on device ownership (corporate or other). This is a historical widget.
- **Top Device Operating System by Client Count Over Time** is a summary of the type of operating system used by devices connected to vWLAN. This is a historical widget.
- **Top Device Type by Client Count Over Time** is a summary of the top ten types of devices used by clients connected to vWLAN. This is a historical widget.
- **Top Device Operating System by Usage Over Time** is a summary of the top ten device operating systems used by clients. This is a historical widget.
- **Top Device Types by Usage Over Time** is a summary of the top ten device types used by clients. This is a historical widget.

3. The information displayed by the widgets can be customized. To customize the historical reports of the report dashboard widgets, you can specify a time frame using the drop-down menu at the top right of the **Dashboard** menu. Here you can specify that information for the last 24 hours, last 7 days, last 30 days, a specific date range, or a customized time frame is displayed. Information for the last 2 months can be displayed on the report dashboard.



*You can configure vWLAN to email copies of the information collected in the dashboard or have that information available for download. Refer to the **Customizing the Report Dashboard Widgets** section of the vWLAN Administrator’s Guide, available online at https://supportforums.adtran.com.*