

Configuration Guide

Configuring vWLAN and ProCloud Analytics

This document describes how to configure a (virtual wireless local area network) vWLAN for ProCloud Analytics and how to set up ProCloud Analytics once the vWLAN has been properly configured. This guide includes instructions using the web-based graphical user interface (GUI).

This document contains the following sections:

Prior to Analytics Configuration

Step 1: Purchase/Install a Registered Hostname Certificate on page 2

Step 2: Enable the Redirect to Hostname Option on page 2

Step 3: Enable the AP to Look Up the vWLAN Name on page 3

Step 4: Add a PTR Record in the DNS Server on page 3

vWLAN Configuration

Step 1: Configuring Accounting Servers on page 4

Step 2: Configuring RADIUS Server Authentication on page 7

Step 4: Creating Destinations on page 15

Step 5: Creating a Destination Group on page 17

Step 6: Editing Roles on page 19

Step 7: Creating an SSID on page 22

Step 8: Modifying the AP Template on page 24

ProCloud Analytics Configuration

Step 1: Log into Your ProCloud Analytics Portal on page 26

Step 2: Configure Authentication Access Methods on page 27

Step 3: Create Your Splash Pages on page 28

Step 4: Create Your Access Journey on page 32

Step 5: Review on page 34

Prior to Analytics Configuration

Step 1: Purchase/Install a Registered Hostname Certificate

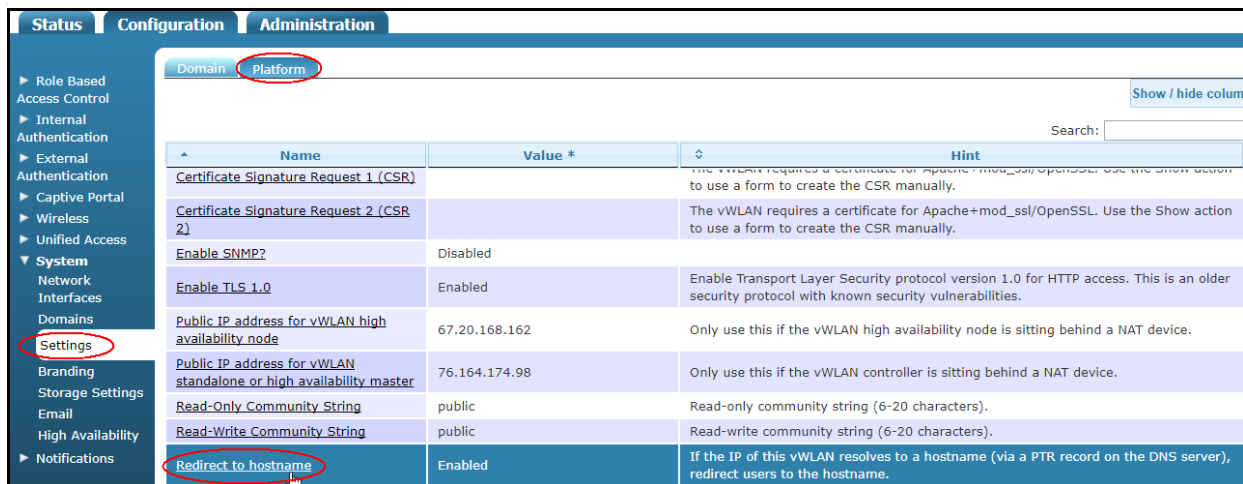
Refer to [Installing and Renewing an SSL Certificate in vWLAN](#) on the ADTRAN Support Forum for more details on this process.

Step 2: Enable the *Redirect to Hostname* Option

The *Redirect to Hostname* option allows users to be redirected to the hostname for which the IP of the vWLAN resolves. From the **Configuration** tab select the **Platform** tab and then **System > Settings**. Select **Redirect to Hostname**.



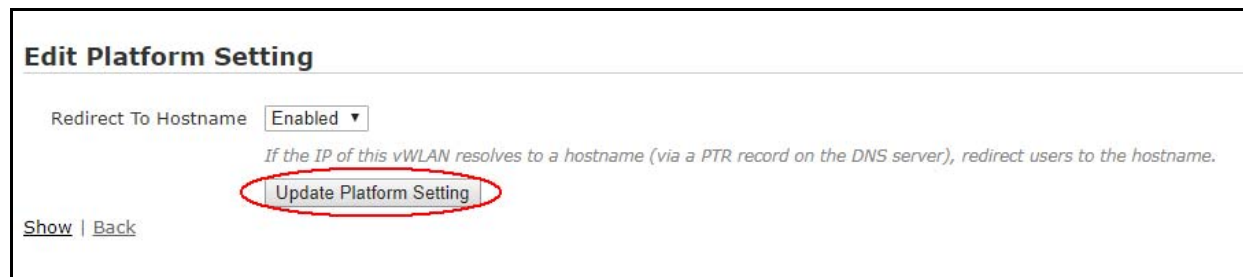
This menu option is only visible in platform administrator accounts.



The screenshot shows the 'Platform' configuration page. The 'Settings' menu item in the left sidebar is circled in red. The 'Redirect to hostname' setting is also circled in red. The table below shows the configuration details for this setting.

Name	Value *	Hint
Certificate Signature Request 1 (CSR)		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL. Use the Show action to use a form to create the CSR manually.
Certificate Signature Request 2 (CSR 2)		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL. Use the Show action to use a form to create the CSR manually.
Enable SNMP?	Disabled	
Enable TLS 1.0	Enabled	Enable Transport Layer Security protocol version 1.0 for HTTP access. This is an older security protocol with known security vulnerabilities.
Public IP address for vWLAN high availability node	67.20.168.162	Only use this if the vWLAN high availability node is sitting behind a NAT device.
Public IP address for vWLAN standalone or high availability master	76.164.174.98	Only use this if the vWLAN controller is sitting behind a NAT device.
Read-Only Community String	public	Read-only community string (6-20 characters).
Read-Write Community String	public	Read-write community string (6-20 characters).
Redirect to hostname	Enabled	If the IP of this vWLAN resolves to a hostname (via a PTR record on the DNS server), redirect users to the hostname.

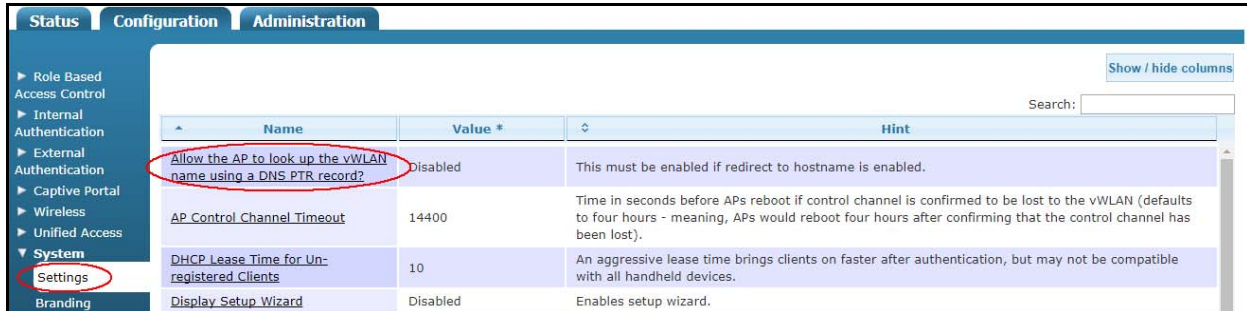
Choose **Enabled** from the drop down menu and select **Update Platform Setting**.



The screenshot shows the 'Edit Platform Setting' page for 'Redirect To Hostname'. The 'Redirect To Hostname' dropdown menu is set to 'Enabled' and is circled in red. The 'Update Platform Setting' button is also circled in red. The hint text below the dropdown reads: 'If the IP of this vWLAN resolves to a hostname (via a PTR record on the DNS server), redirect users to the hostname.'

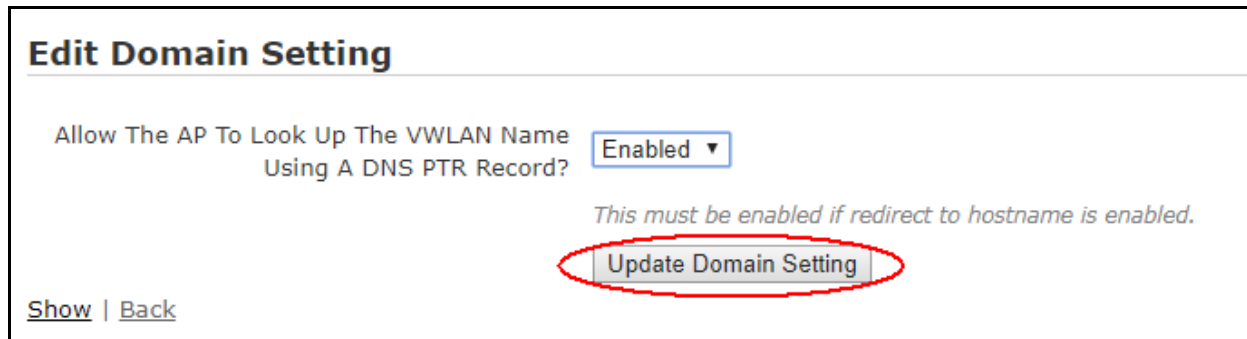
Step 3: Enable the AP to Look Up the vWLAN Name

After Redirect to Hostname has been enabled, the AP needs to be allowed to look up the vWLAN name using a Domain Name Server (DNS) Pointer (PTR) record. From the **Configuration** tab select **System > Settings**. Select **Allow the AP to look up the vWLAN name using a DNS PTR record..**



Name	Value *	Hint
Allow the AP to look up the vWLAN name using a DNS PTR record?	Disabled	This must be enabled if redirect to hostname is enabled.
AP Control Channel Timeout	14400	Time in seconds before APs reboot if control channel is confirmed to be lost to the vWLAN (defaults to four hours - meaning, APs would reboot four hours after confirming that the control channel has been lost).
DHCP Lease Time for Un-registered Clients	10	An aggressive lease time brings clients on faster after authentication, but may not be compatible with all handheld devices.
Display Setup Wizard	Disabled	Enables setup wizard.

Choose **Enabled** from the drop down menu and select **Update Domain Setting**.



Edit Domain Setting

Allow The AP To Look Up The VWLAN Name Using A DNS PTR Record? **Enabled** ▼

This must be enabled if redirect to hostname is enabled.

Update Domain Setting

[Show](#) | [Back](#)



This step needs to be performed for each domain.

Step 4: Add a PTR Record in the DNS Server

Add a PTR record for the hostname of the primary and secondary servers (if applicable) in the DNS server the vWLAN is using.

vWLAN Configuration

To properly configure vWLAN for ProCloud Analytics, you must configure vWLAN exactly as shown in this document.

Accessing the vWLAN Interface

Before you begin, make sure you have your account credentials provided by ADTRAN ProServices. This information includes: user name, password, accounting server IP address and shared secret, and RADIUS server IP address and shared secret.



*If you are configuring this device as a wireless local area network (WLAN) appliance (not a part of ProCloud Services), then the default username is **root@adtran.com** and the default password is **blueblue**.*

To access the vWLAN interface, follow these steps:

1. Enter the IP address of the vWLAN into a browser window in the format:

https://<vWLANipaddress>:3000

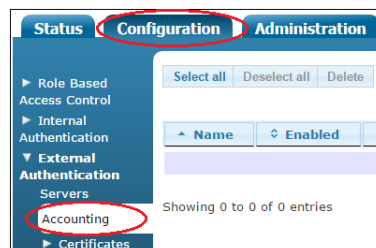
2. Log in with the user name and password provided by ProServices.



Step 1: Configuring Accounting Servers

Use the steps in this section to configure vWLAN to use the RADIUS accounting servers for ProCloud Analytics.

1. From the **Configuration** tab, select **External Authentication > Accounting**.



2. Select **Create Accounting Server** at the bottom of this menu.



3. Enter the following information on the menu:

Parameter	Setting
Name	guest1
Enabled	Checked
IP Address	<i>Provided by ProServices</i>
Port	1813
Shared Secret	<i>Provided by ProServices</i>
Shared Secret Confirmation	Re-enter the shared secret as above.
Timeout	5
Retries	5
Interim Updates Enabled	Checked
Interim Update Interval	300

Create Accounting Server

Name

Enabled

IP Address

Port

Shared Secret

Shared Secret Confirmation

Timeout

Retries

Interim Updates Enabled

Interim Update Interval In Seconds

[Back](#)

4. Select **Create Accounting Server** to create the server. A confirmation displays indicating that the server has been created.

Interim Updates Enabled

Interim Update Interval In Seconds

[Back](#) [Create Accounting Server](#)

5. Select **Create**.

Status **Configuration** **Administration**

Accounting Server was successfully created.

Name guest1

Enabled true

IP Address XXXXXXXX.XXX.XXX

Port 1813

Timeout 5

Retries 5

Interim Update Enabled true

Interim Update Interval 300

[Edit](#) | [Delete](#) | [Create](#) | [Back](#)

© 2015 ADTRAN, Inc.

6. Enter the following information on the menu:

Parameter	Setting
Name	guest2
Enabled	Checked
IP Address	<i>Provided by ProServices</i>
Port	1813
Shared Secret	<i>Provided by ProServices</i>
Shared Secret Confirmation	Re-enter the shared secret as above.
Timeout	5
Retries	5
Interim Updates Enabled	Checked
Interim Update Interval	300

Create Accounting Server

Name

Enabled

IP Address

Port

Shared Secret

Shared Secret Confirmation

Timeout

Retries

Interim Updates Enabled

Interim Update Interval In Seconds

[Back](#)

7. Select **Create Accounting Server** to create the server. A confirmation displays indicating that the server has been created.

Interim Updates Enabled

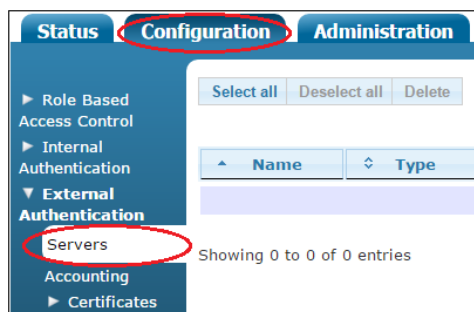
Interim Update Interval In Seconds

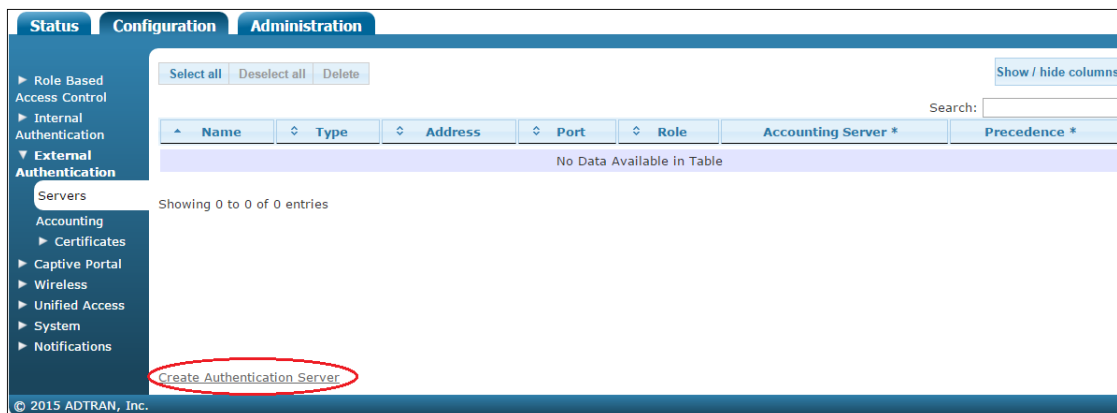
[Back](#)

Step 2: Configuring RADIUS Server Authentication

Use the steps in this section to define the method of authentication used by the remote authentication dial-in user services (RADIUS) accounting servers configured in [Step 1: Configuring Accounting Servers on page 4](#).

1. From the **Configuration** tab, select **External Authentication > Servers**.



2. Select **Create Authentication Server**.

3. Enter the following information on the menu:

Parameter	Setting
Type	RadiusWebAuthServer
Name	guest1
Accounting Server	guest1
IP Address	<i>Provided by ProServices</i>
Port	1812
Shared Secret	<i>Provided by ProServices</i>
Shared Secret Confirmation	Re-enter the shared secret as above.
Timeout Weight	1
Precedence	Highest
Enable Radius MAC Authentication	Unchecked
Role	Guest

Create Authentication Server

Type

Name

Accounting Server

IP Address

Port
Typically, the port should be 1812 or 1645.

Shared Secret/Password

Shared Secret/Password Confirmation

Timeout Weight
*Current total weight is 0, and current total timeout is 10.
Set the weight of the timeout for this server relative to the other auth servers. The total time allocated to authenticate is defined for the entire system.
Each server's timeout will be computed as its percentage of the total weight of all auth servers in this domain.*

Maximum Number of Simultaneous Users Allowed to Authenticate at Once
Blank or 0 = no limit.

Precedence

Enable Radius MAC Authentication

Authentication Rules

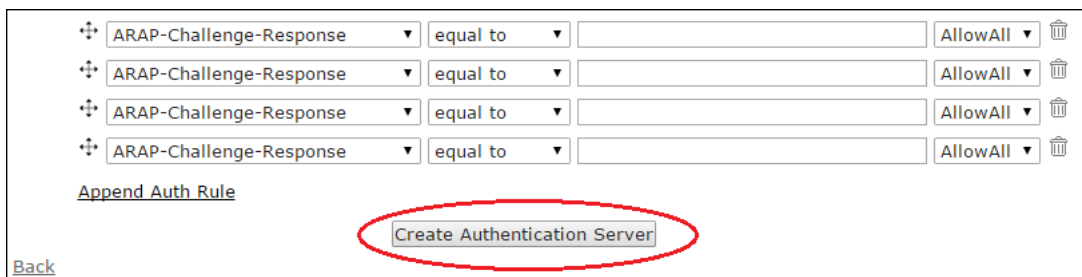
Role

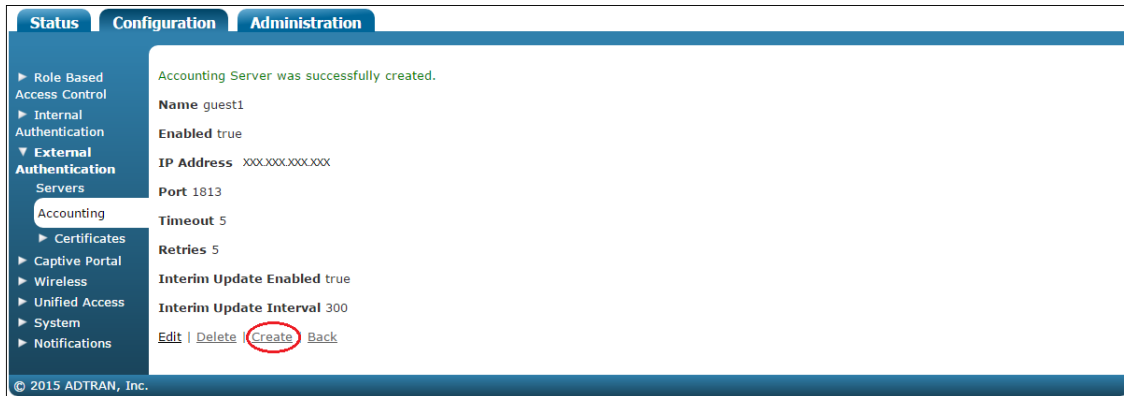
Attribute	Logic	Value	Role
ARAP-Challenge-Response	equal to	<input type="text"/>	AllowAll
ARAP-Challenge-Response	equal to	<input type="text"/>	AllowAll
ARAP-Challenge-Response	equal to	<input type="text"/>	AllowAll
ARAP-Challenge-Response	equal to	<input type="text"/>	AllowAll
ARAP-Challenge-Response	equal to	<input type="text"/>	AllowAll

[Append Auth Rule](#)

[Back](#)

4. Select **Create Authentication Server**. A confirmation displays indicating that the server has been created.



5. Select **Create**.

6. Enter the following information on the menu:

Parameter	Setting
Type	RadiusWebAuthServer
Name	guest2
Accounting Server	guest2
IP Address	<i>Provided by ProServices</i>
Port	1812
Shared Secret	<i>Provided by ProServices</i>
Shared Secret Confirmation	Re-enter the shared secret as above.
Timeout Weight	1
Precedence	Lowest
Enable Radius MAC Authentication	Unchecked
Role	Guest

Create Authentication Server

Type: RadiusWebAuthServer

Name: guest2

Accounting Server: guest2

IP Address: XXXX.XXXX.XXXX.XXXX

Port: 1812
Typically, the port should be 1812 or 1645.

Shared Secret/Password: [Masked]

Shared Secret/Password Confirmation: [Masked]

Timeout Weight: 1
*Current total weight is 1, and current total timeout is 10.
Set the weight of the timeout for this server relative to the other auth servers. The total time allocated to authenticate is defined for the entire system.
Each server's timeout will be computed as its percentage of the total weight of all auth servers in this domain.*

Maximum Number of Simultaneous Users Allowed to Authenticate at Once: 0
Blank or 0 = no limit.

Precedence: Lowest

Enable Radius MAC Authentication:

Authentication Rules

Role: Guest

Attribute	Logic	Value	Role
ARAP-Challenge-Response	equal to		Guest
ARAP-Challenge-Response	equal to		Guest
ARAP-Challenge-Response	equal to		Guest
ARAP-Challenge-Response	equal to		Guest
ARAP-Challenge-Response	equal to		Guest

[Append Auth Rule](#)

[Create Authentication Server](#)

[Back](#)

7. Select **Create Authentication Server**. A confirmation displays indicating that the server has been created.

ARAP-Challenge-Response	equal to		AllowAll
ARAP-Challenge-Response	equal to		AllowAll
ARAP-Challenge-Response	equal to		AllowAll
ARAP-Challenge-Response	equal to		AllowAll

[Append Auth Rule](#)

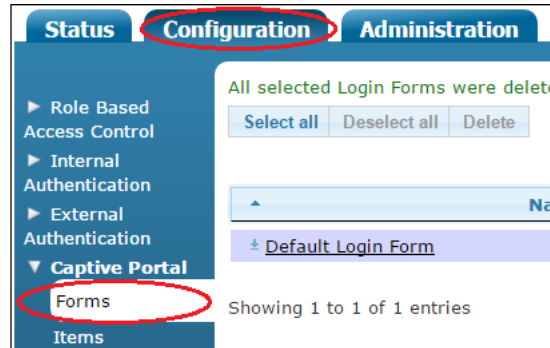
[Create Authentication Server](#)

[Back](#)

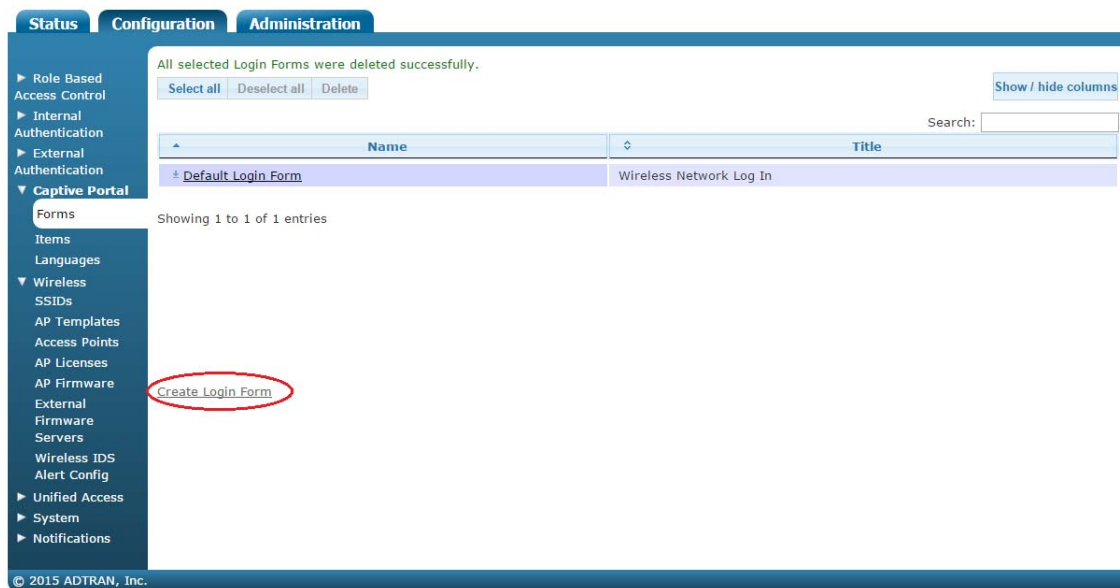
Step 3: Creating the Login Form

Use the steps in this section to create a login form that redirects clients to the URL for ProCloud Analytics.

1. From the **Configuration** tab, select **Captive Portal > Forms**.



2. Select **Create Login Form**.



3. Enter the following information on the menu:

Parameter	Setting
Name	guest
Allow User Logins	Checked
Allow Guest Logins	Unchecked
Redirect Clients to an External URL	Checked
Base URL of External Server	https://analytics.adtranprocloud.com/access/
Client's MAC Address	blue_mac
Client's Access Point MAC Address	blue_ap
Client's Access Point Name	blue_ap_name
vWLAN IP Address	blue_controller
Client's Original URL	blue_destination
Client's IP Address	blue_source
Client's Access Point SSID	blue_ssid
Client's VLAN ID	blue_vlan
Double Encoding of URI Parameters	Unchecked
Include RADIUS Option Vendor option	Unchecked

Create Login Form

Name

Authentication Method

Hotspot account

Allow User Logins

Allow Guest Logins

Default Language

Redirect Clients To An External URL

Redirection To An External Captive Portal Server

Base URL of External Server
Please ensure that the external server is reachable from the access points.
The external server must notify vWLAN when login succeeds using an URL of the form:
https://vWLAN_IP/login.pl?which_form=reg&source=CLIENT_IP&macaddr=CLIENT_MAC
&domain_id=DOMAIN_ID&login_form_id=LOGIN_FORM_ID&bs_name=NAME&bs_password=PASSWORD.

For each of the following items, enter a string for the URI parameter if you wish it to be passed to the external server. Note that the first three items are required.

vWLAN Domain ID

vWLAN Login Form ID

Client's MAC Address

Client's Access Point MAC Address

Client's Access Point Name

vWLAN IP Address

Client's Original URL

Client's IP Address

Client's Access Point SSID

Client's VLAN ID

AP Status

Double Encoding of URI Parameters

Include RADIUS Option Vendor option

4. Select **Create Login Form**. A confirmation displays indicating that the form has been created.

Double Encoding of URI Parameters

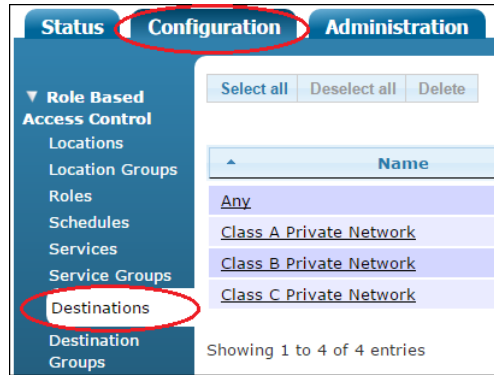
Include RADIUS Option Vendor option

[Back](#)

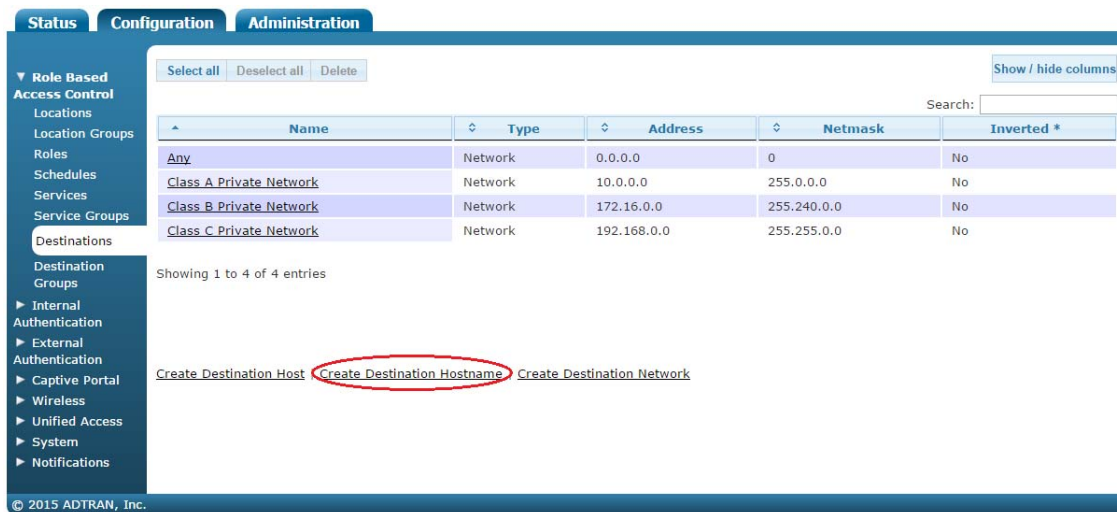
Step 4: Creating Destinations

Use the steps in this section to define which networks are available to your users. These should be the network destinations that you want to allow clients to access without having to first log into your network.

1. From the **Configuration** tab, select **Role Based Access Control > Destinations**.



2. Select **Create Destination Hostname**.



3. Enter the following information on the menu:

Parameter	Setting
Name	AnalyticsPortal
Address	analytics.adtranprocloud.com

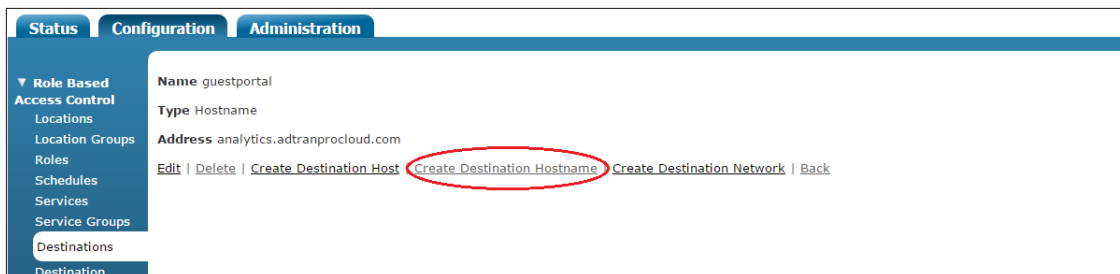
Create Destination - Hostname

Name

Address

[Back](#)

4. Select **Create Destination**. A confirmation displays indicating that the form has been created.
5. Select **Create Destination Hostname**.



6. Repeat Steps 3 and 4 for each of the following:

Name	Address
ADTRAN	www.adtran.com
google1	www.google.co.uk
google2	www.google.com
google3	google-analytics.com
symcd	gn.symcd.com
venuewifi	*.venuewifi.com
owm	*.openweathermap.org
cloudfront	*.cloudfront.net
GoDaddy1	crl.godaddy.com
GoDaddy2	ocsp.godaddy.com
GoDaddy3	certificates.godaddy.com
GoDaddy4	certs.godaddy.com
GoDaddy5	crl.starfieldtech.com
GoDaddy6	ocsp.starfieldtech.com
GoDaddy7	certificates.starfieldtech.com
GoDaddy8	certs.starfieldtech.com

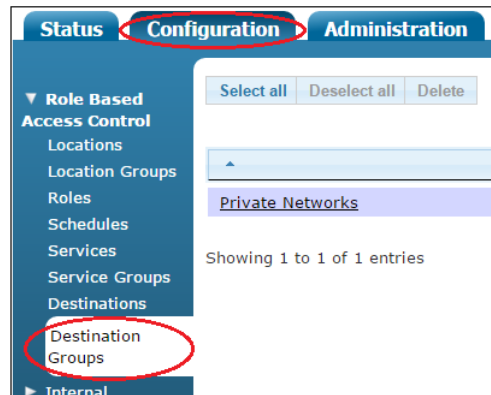
7. If you want to support social network logins, repeat the previous steps to add the destinations shown in the following table for each network you plan to support. For example, if you want to include Twitter, create a destination hostname for each address given for Twitter. Enter whatever you want in the **Name** field (for example, twitter1, twitter2, twitter3).

Facebook	Twitter	LinkedIn	Google	Instagram
facebook.com *.facebook.com *.fbcdn.net *.akamaihd.net connect.facebook.net	twitter.com *.twitter.com *.twimg.com	linkedin.com *.linkedin.com *.licdn.net *.licdn.com	*.googleusercontent.com *.googleapis.com accounts.google.com *.gstatic.com	instagram.com *.instagram.com

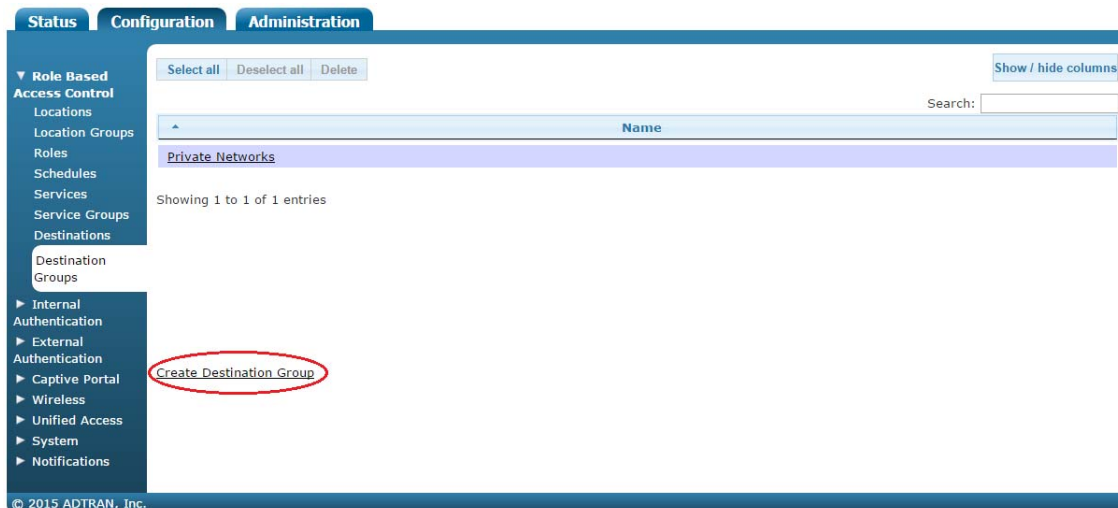
Step 5: Creating a Destination Group

A destination group is a collection of destinations that can be applied to allow traffic to certain network destinations based on a specific role. In the following steps, you will add the destinations created in [Step 4: Creating Destinations on page 15](#) to a group, and in [Step 6: Editing Roles on page 19](#), you will limit un-registered users to these locations.

1. From the **Configuration** tab, select **Role Based Access Control > Destination Groups**.



2. Select **Create Destination Group**.



3. Enter **AnalyticsPortal** in the Name field.

- Select the + sign beside each destination in right-hand list that you want to add to the group. Add all of the destinations to the *AnalyticsPortal* destination group except for **GoDaddy**, **Any**, and **Class A, B, C Private Network** destinations.

Create Destination Group

Name

Destinations **27 items selected** [Remove all](#) [Add all](#)

- ProCloudAnalyticsADTRAN1	+ Any
- ProCloudAnalyticsADTRAN2	+ Class A Private Network
- ProCloudAnalyticsCloudFront1	+ Class B Private Network
- ProCloudAnalyticsFacebook1	+ Class C Private Network
- ProCloudAnalyticsFacebook2	+ GoDaddy1
- ProCloudAnalyticsFacebook3	+ GoDaddy2
- ProCloudAnalyticsFacebook4	+ GoDaddy3
- ProCloudAnalyticsFacebook5	+ GoDaddy4

[Create Destination Group](#)

[Back](#)

- Select **Create Destination Group**. A confirmation displays indicating the group has been created.
- Select **Create**.

Destination Group was successfully created.

Name AnalyticsPortal

Destinations in Group

[ProCloudAnalyticsADTRAN1](#)
[ProCloudAnalyticsADTRAN2](#)
[ProCloudAnalyticsCloudFront1](#)
[ProCloudAnalyticsFacebook1](#)
[ProCloudAnalyticsFacebook2](#)
[ProCloudAnalyticsFacebook3](#)
[ProCloudAnalyticsFacebook4](#)
[ProCloudAnalyticsFacebook5](#)
[ProCloudAnalyticsGoogle1](#)
[ProCloudAnalyticsGoogle2](#)
[ProCloudAnalyticsGoogle3](#)
[ProCloudAnalyticsGoogle4](#)
[ProCloudAnalyticsGoogle5](#)
[ProCloudAnalyticsGoogle6](#)
[ProCloudAnalyticsGoogle7](#)
[ProCloudAnalyticsInstagram1](#)
[ProCloudAnalyticsInstagram2](#)
[ProCloudAnalyticsLinkedIn1](#)
[ProCloudAnalyticsLinkedIn2](#)
[ProCloudAnalyticsLinkedIn3](#)
[ProCloudAnalyticsLinkedIn4](#)
[ProCloudAnalyticsOpenWeather1](#)
[ProCloudAnalyticsSymCd1](#)
[ProCloudAnalyticsTwitter1](#)
[ProCloudAnalyticsTwitter2](#)
[ProCloudAnalyticsTwitter3](#)
[ProCloudAnalyticsVenueWifi1](#)

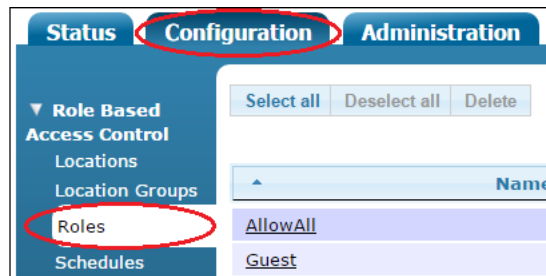
[Edit](#) | [Delete](#) [Create](#) [Back](#)

- Repeat Steps 3 through 5 to create a destination group named **GoDaddy** and add all of the GoDaddy destinations created in *Step 4: Creating Destinations on page 15* (**GoDaddy1** through **GoDaddy8**).

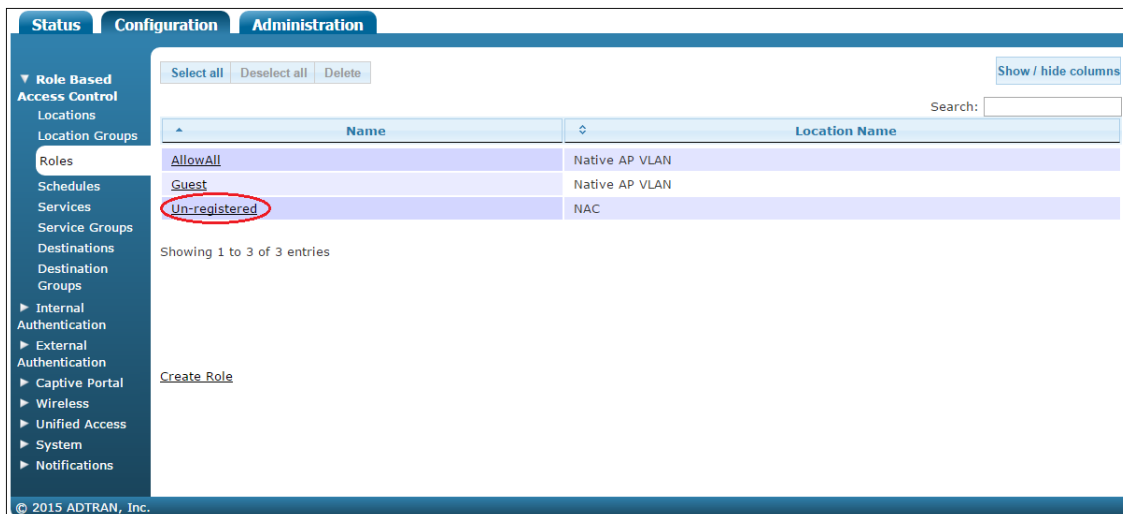
Step 6: Editing Roles

User roles in vWLAN define the policies enforced per user at the wireless access point (AP). When configuring vWLAN for ProCloud Analytics, you need to define the traffic allowed for the following user roles: **Guest** (a client who has logged into the network) and **Un-registered** (a client who has not logged into the network).

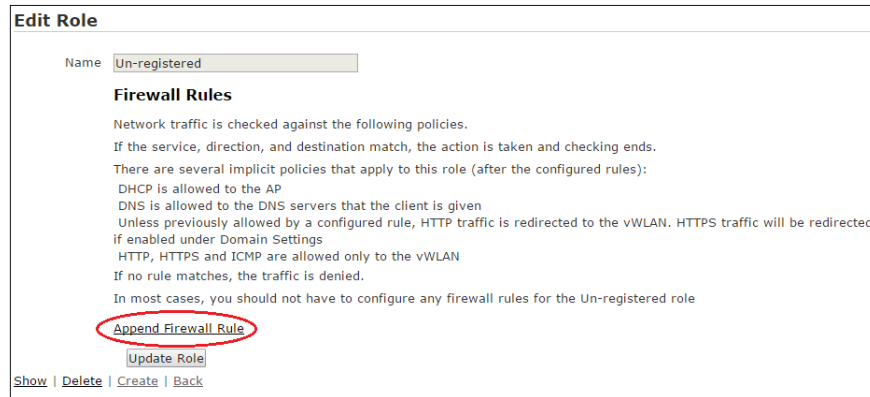
1. From the **Configuration** tab, select **Role Based Access Control > Roles**.



2. Select the **Un-registered** role.

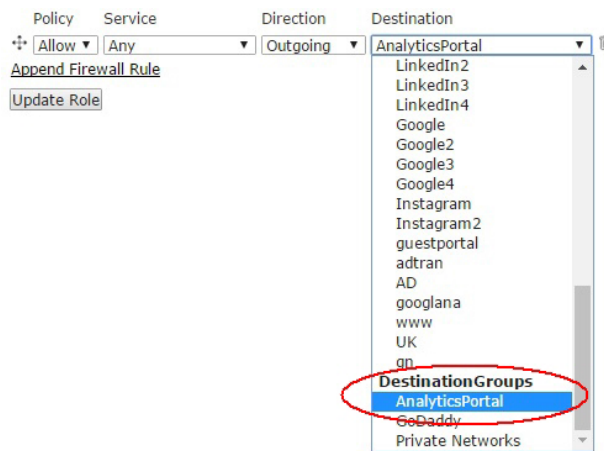


3. Select **Append Firewall Rule**.



4. Use the drop-down lists to add the following rules. After entering a rule, select **Append Firewall Rule** to add the next rule.

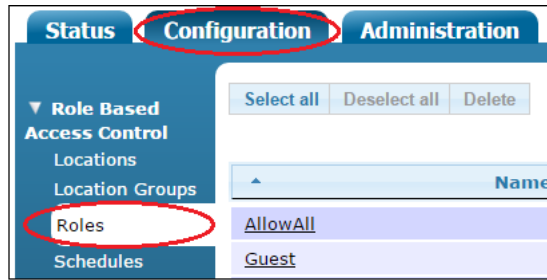
Policy	Service	Direction	Destination (Select from the DestinationGroups)
Allow	HTTP	Outgoing	AnalyticsPortal
Allow	HTTPS	Outgoing	AnalyticsPortal
Allow	HTTP	Outgoing	GoDaddy
Allow	HTTPS	Outgoing	GoDaddy



5. Select **Update Role**. A confirmation displays indicating that the role has been updated.



- From the side navigation panel, select **Roles** again.



- Select the **Guest** role.

Name	Location Name
AllowAll	Native AP VLAN
Guest	Native AP VLAN
Un-registered	NAC

- Under the **Post Login Redirection** section, enter the following in the **Thank You HTML** field:
http://analytics.adtranprocloud.com/access/?res=success

Edit Role

Name:

Schedule:

Location:

Machine Authentication Enforcement:

Allow Client To Client:
Allows Client to Client traffic on the same AP.

Class of Service

Over The Air Fairness:
De-prioritize traffic for clients in the role. This will give clients in other roles better wireless performance. Only applies to 1800 Series APs.

CoS Priority In Override:
What to prioritize Wireless based on.

CoS Priority In:

CoS Priority Out Override:
What to remark Wired based on.

CoS Priority Out:

Bandwidth Shaping

QoS Rate In: Mbits/second
Bandwidth Limit in Incoming/Downstream (AP to Client) direction. Set to zero for no bandwidth limit.

QoS Rate Out: Mbits/second
Bandwidth Limit in Outgoing/Upstream (Client to AP) direction. Set to zero for no bandwidth limit.

Post Login Redirection

Thank You HTML:

If HTML text is entered here, it will be displayed after a user has logged in on the thank-you page. The user will not be automatically redirected.

URL Redirect:
URL to redirect after login. This value overrides the default URL found under settings.

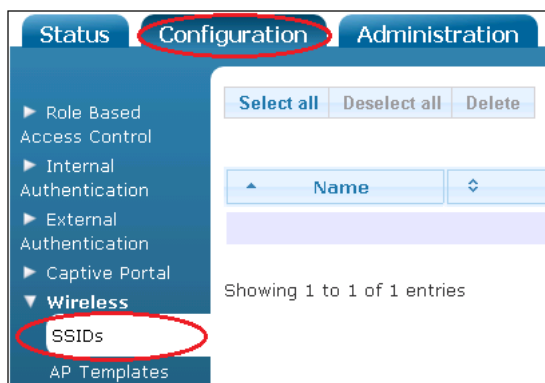
- Select **Update Role** at the bottom of the menu. A confirmation displays indicating that the role has been updated.



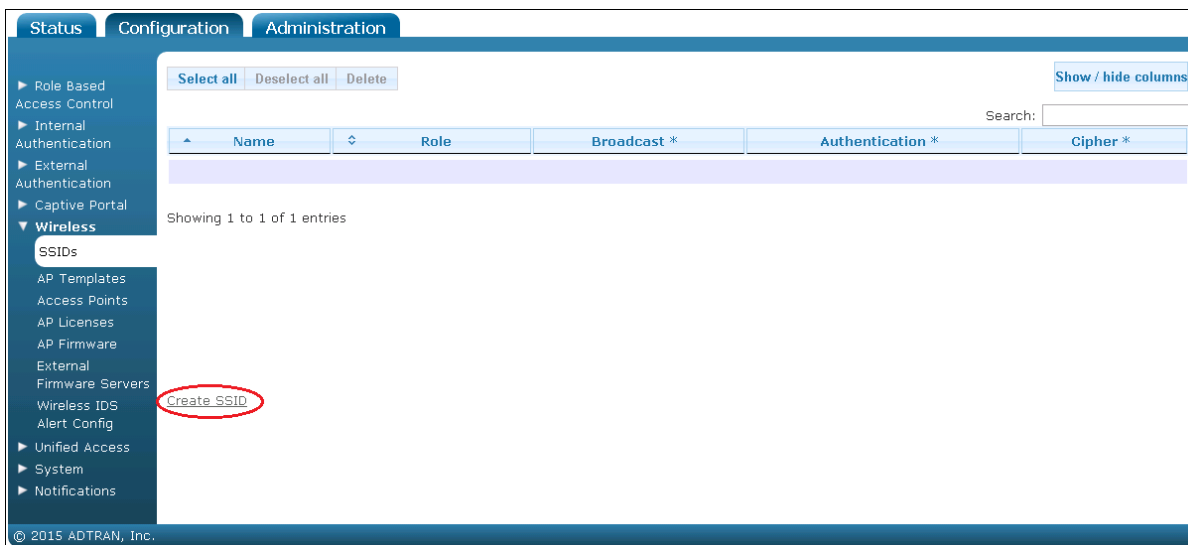
Step 7: Creating an SSID

A service set identifier (SSID) provides a unique set of connection parameters by broadcasting independent security attributes. The SSID must be associated with the AP using an AP template. Use the following steps to create the SSID. This SSID will then be associated with the AP Template in [Step 8: Modifying the AP Template on page 24](#).

1. From the **Configuration** tab, select **Wireless > SSIDs**.



2. Select **Create SSID**.



3. Enter the following information on the menu:

Parameter	Setting
Name/ESSID	GuestWifi
Broadcast SSID	Checked
Convert Broadcast/Multicast Traffic to Unicast	Disable
Authentication	Open System
Cipher	Disabled

Parameter	Setting
Login Form	guest
Role	Un-registered
Standby SSID	Unchecked
DynamicSteering	Checked
Tunnel WLAN Traffic	Unchecked

Create SSID

Name/ESSID

Broadcast SSID

Convert Multicast/Broadcast Network Traffic To Unicast

Authentication

Cipher

Login Form

Role

Standby SSID

DynamicSteering
Enables band/client steering, load balancing, and sticky client prevention technology (including 802.11k and 802.11v). Requires SSID assigned to both radio bands on the AP template. Not supported on 18XX model APs.

Tunnel WLAN Traffic
Not supported on 18XX and 3XXX model APs.

[Back](#)

4. Select **Create SSID** at the bottom of the menu. A confirmation displays indicating that the SSID has been created.

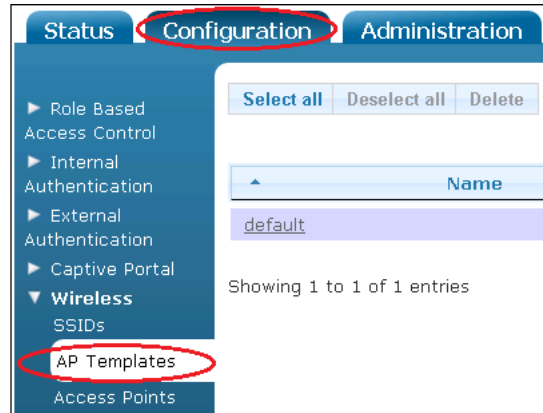
Tunnel WLAN Traffic
Not supported on 18XX and 3XXX model APs.

[Back](#)

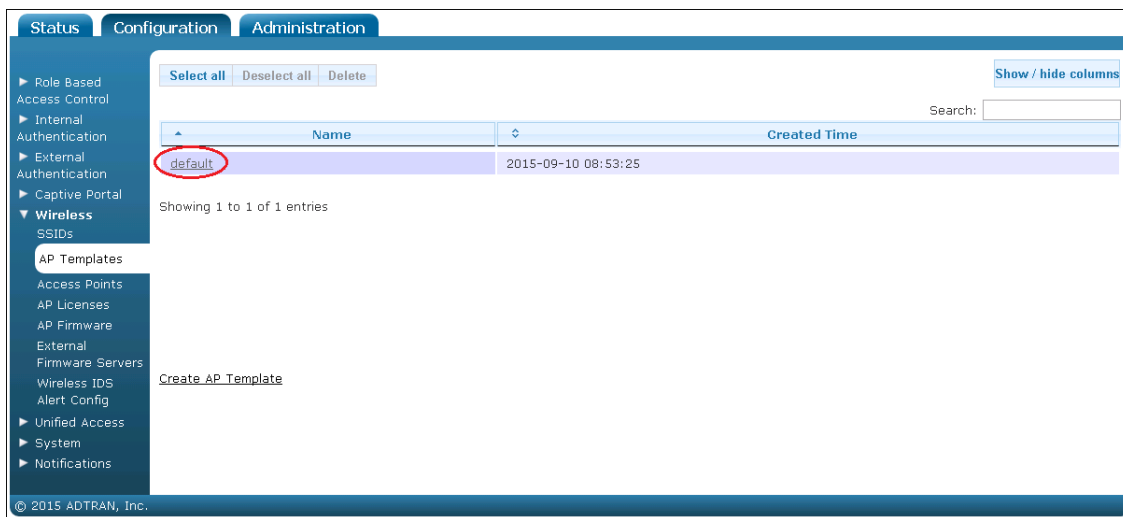
Step 8: Modifying the AP Template

Use the steps in this section to modify the default AP Template to use the SSID created in [Step 7: Creating an SSID on page 22](#).

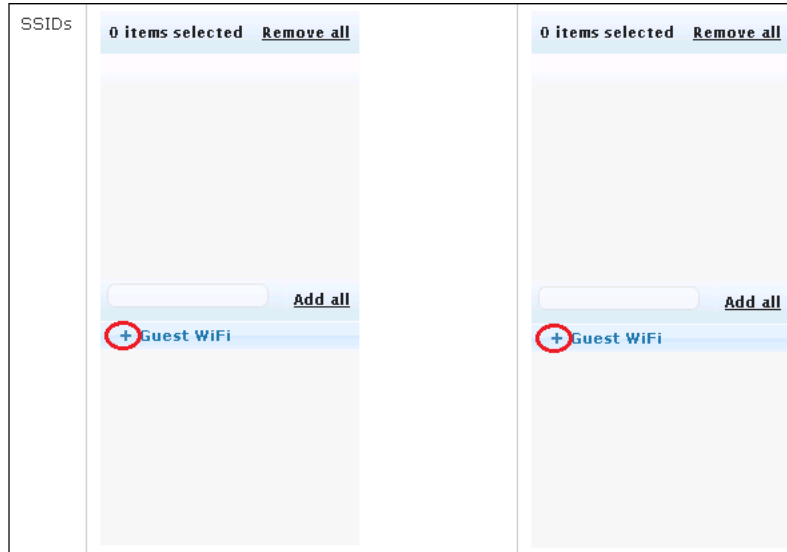
1. From the **Configuration** tab, select **Wireless > AP Templates**.



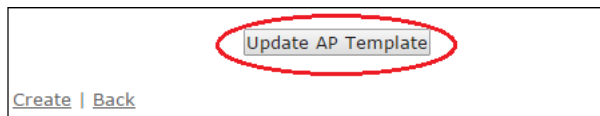
2. Select the **default** template from the list of templates.



- In the **SSID** section, select the + sign beside the **Guest WiFi** entry in the **Add** list for each radio to add the Guest WiFi SSID to the AP template.



- Select **Update AP Template** at the bottom of the menu. A confirmation displays indicating the AP template has been updated.



- For the updated template to take affect, you will need to apply the template to the APs on the **Jobs** menu. Access the **Jobs** menu by selecting the **Domain Tasks** link from the upper-right of the menu. Alternatively, you can access the **Jobs** menu by selecting **Jobs** from the **Administration** tab.



NOTE *Applying these changes to the APs will cause the APs to reboot.*

- Select the **Actions** arrow next to the job **Must apply configuration to APs**.

Domain		Platform
Select all		Deselect all
		Delete
		Show / hide columns
		Search:
Message	Broadcast	Updated Time *
<input checked="" type="checkbox"/> Must apply configuration to APs	true	2015-10-09 14:22:53

Showing 1 to 1 of 1 entries

ProCloud Analytics Configuration

Proceed with this section only after your vWLAN has been successfully configured by ADTRAN Pro Services or by exactly following the steps outlined in the previous *Prior to Analytics Configuration* section in this document.

Step 1: Log into Your ProCloud Analytics Portal

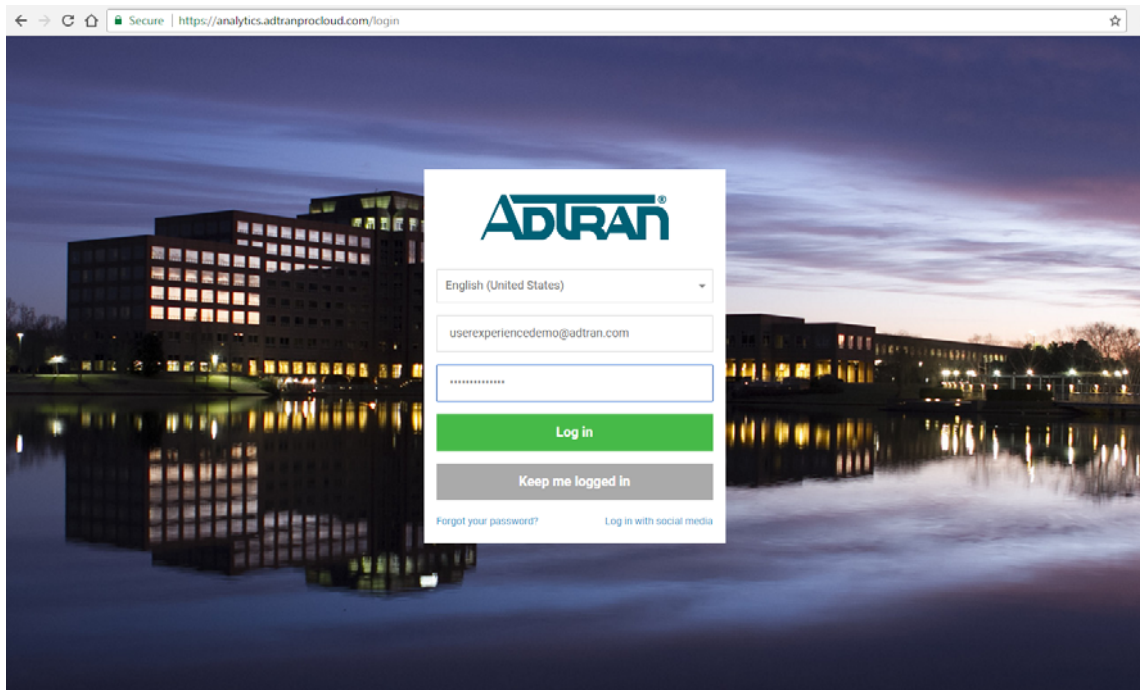
ADTRAN ProServices will assign a user name and password for your ProCloud Analytics account. Navigate to the ProCloud Analytics landing page at <https://analytics.adtranprocloud.com> and enter your user name and password.

The following credentials are used for demonstration purposes in this guide:

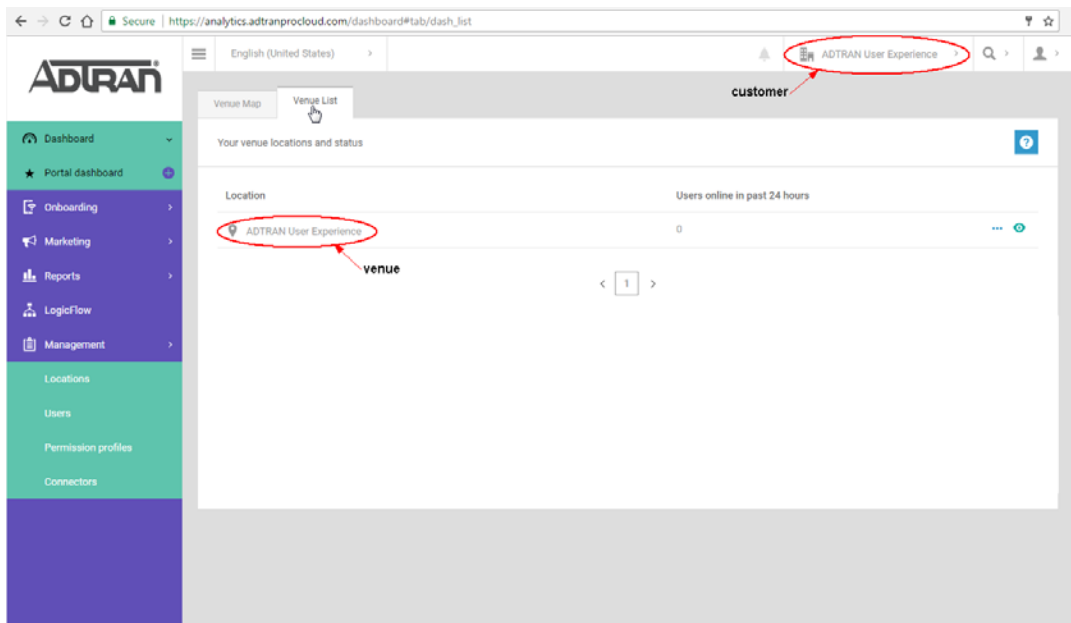
Username: **userexperiencedemo@adtran.com**

Password: **Adtrantest002!**

These demo credentials are always active in case you need to login to clarify a menu item/action.



After logging in, you will see your portal dashboard.

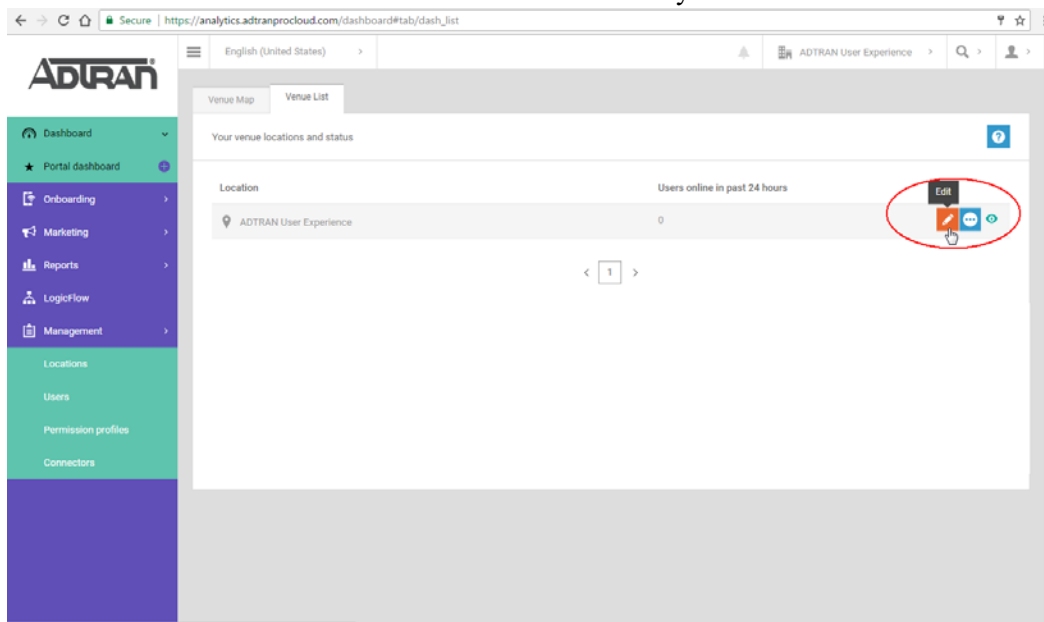


When setting up your ProCloud Analytics account, ADTRAN creates your *customer* and *venue*, and adds your APs to the hardware section of the venue. In the illustration above, the company name is **ADTRAN User Experience** and the venue is also named **ADTRAN User Experience**.

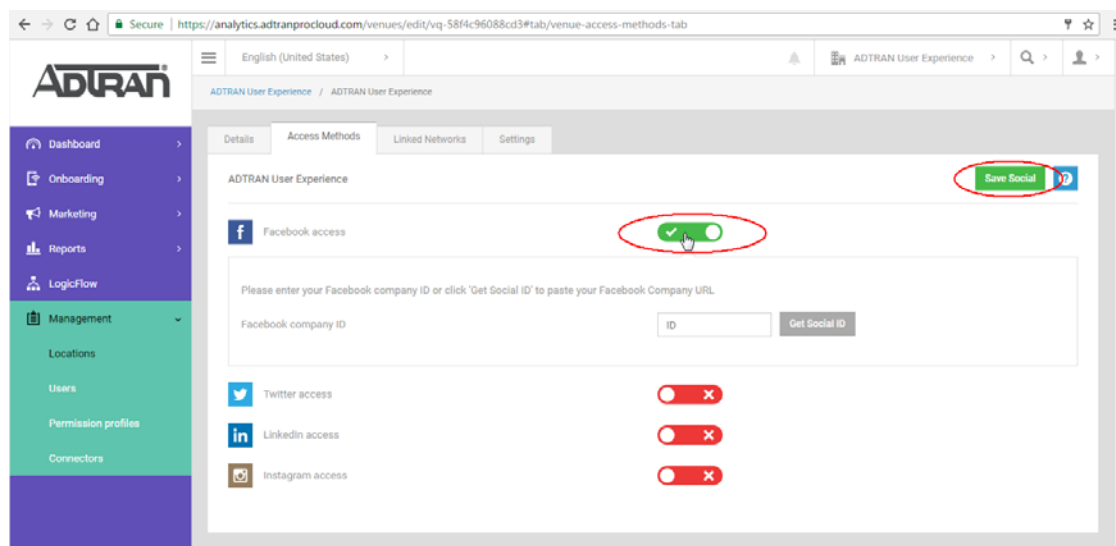
Step 2: Configure Authentication Access Methods

Use the steps in this section to set up the authentication access methods allowed for your users.

1. Select the **Venue List** tab and hover over the ... button next to your venue. Select **Edit** to edit the venue.



2. Select the Access Methods tab and mouse click the red slider next to each access method you want to enable. An access method is active when the slider is green with a checkmark. You will need your company's social network URL or company ID for Facebook, Twitter, and LinkedIn access methods. An ID is not required for the Instagram User ID field. Select **Save Social** when you are finished making changes to this page.



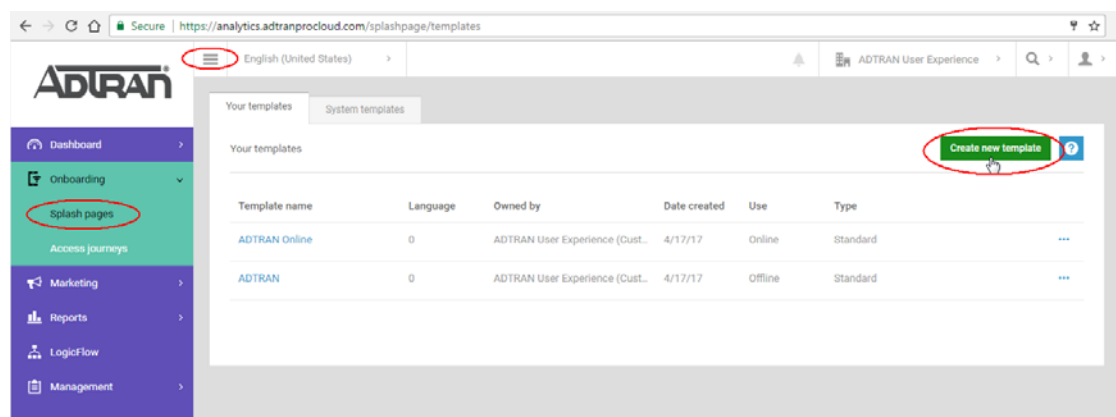
Step 3: Create Your Splash Pages

Splash pages are the pages presented to a user before (offline) and after (online) they authenticate. Use the steps in this section to configure offline and online splash pages.

1. From the left-hand menu bar, select the arrow to the right of *Onboarding* to expand the menu options. Select **Splash Pages** and then select **Create new template**.



If you do not see a left-hand menu bar, select the icon with three horizontal lines at the top of the page to display the menu bar.



2. Complete the dialog box with your splash page parameters.
 - a. Enter a name for your splash page. Consider using the words *Offline* or *Online* in the name to help you differentiate between templates when later viewing the template list.
 - b. Select the *Use* for the template. **Offline** means that this splash page will be presented to the user prior to authentication. The offline splash page presents the user with various ways to log-in to your Wi-Fi network. **Online** means that this splash page will be presented to the user after authentication. The online splash page can have links to other websites or simply display a message thanking your users and confirming login success.



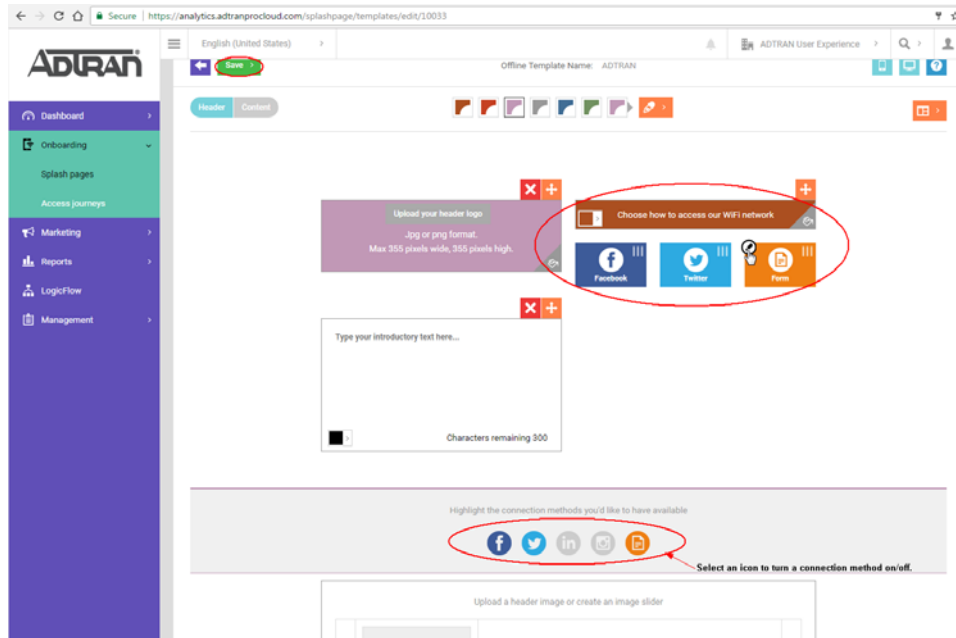
ADTRAN recommends creating both an offline and an online splash page templates. This guide outlines the creation of an offline template first followed by the creation of an online template. Additional configuration for these templates is discussed in [Step 4: Create Your Access Journey on page 32](#).

- c. Select **Customer** next to **Ownership Scope**.
- d. Select your customer's name next to **Owned by**.
- e. Select **Standard** or **Custom HTML** next to **Type**. ADTRAN recommends selecting the standard template.
- f. Select **Create Now**.

Create a new Template

Name	<input type="text" value="ADTRAN"/>
Use	<input type="text" value="Offline"/> ?
Ownership scope	<input type="text" value="Customer"/> ?
Owned by	<input type="text" value="ADTRAN User Experience"/> ?
Type	<input type="text" value="Standard"/> ?

- You are now previewing your offline splash page, which can be customized with your content. Be sure to select the connection methods you wish to allow for authentication. If a user does not use social media, there is a **Form** option. You can edit the information this form requires by selecting the pencil icon located on the upper-left corner of the Form icon. When you are finished making changes to this page, select **Save** in the upper-left corner of the screen and then select **Save template**.



- Repeat Step 2 on [page 29](#) or duplicate your offline splash page to create your online splash page. The main difference in the online splash page setup is you will specify a different **Name**, and **Use** is set to **Online**. The **Ownership scope** and **Owned by** settings should match those of the offline splash page.

Create a new Template

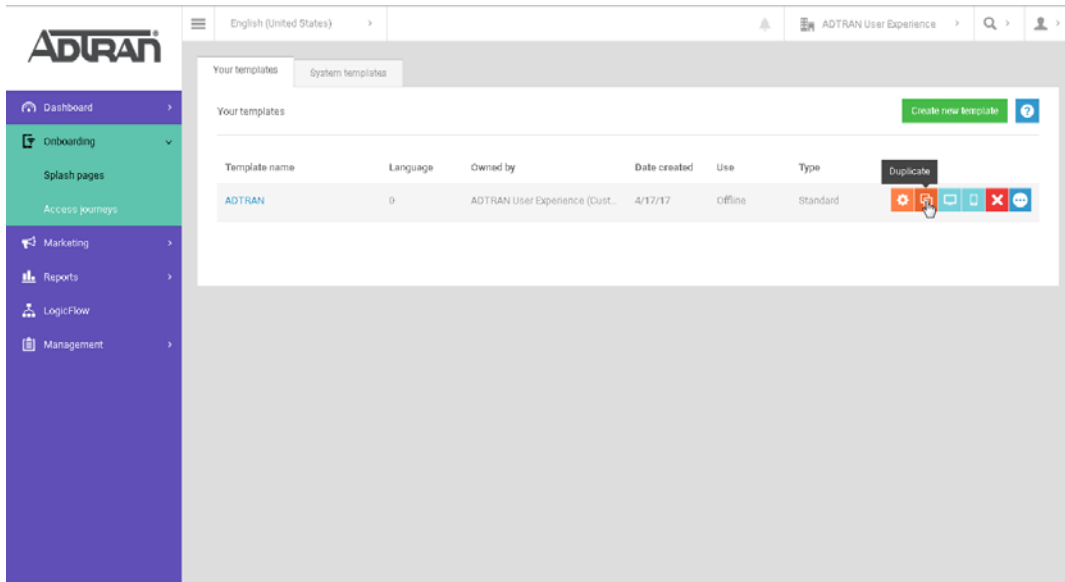
Name

Use ?

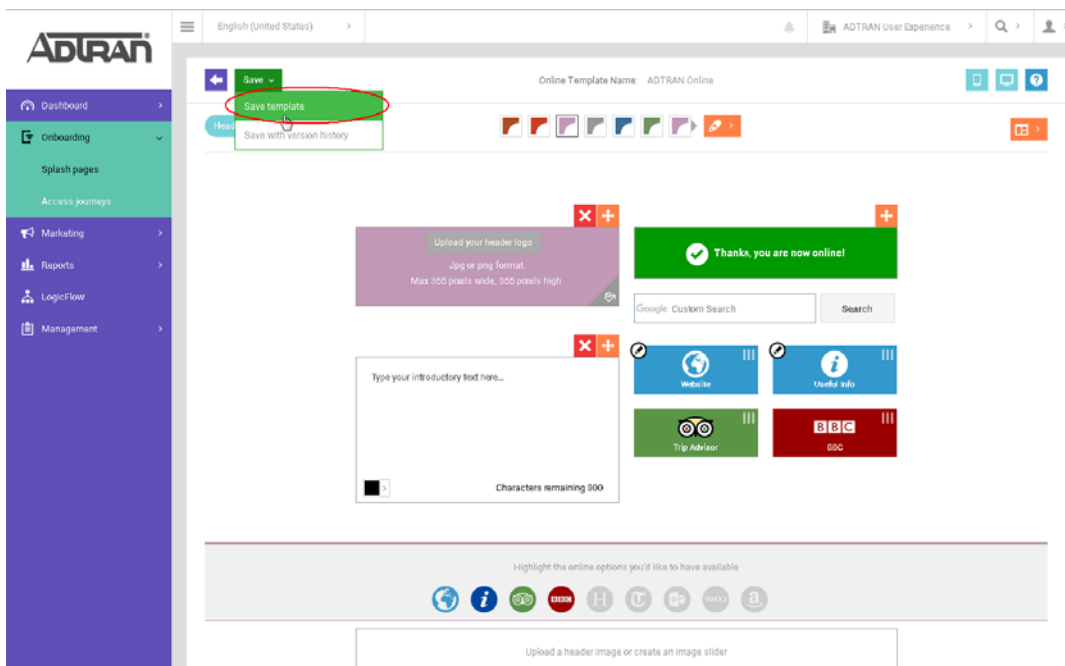
Ownership scope ?

Owned by ?

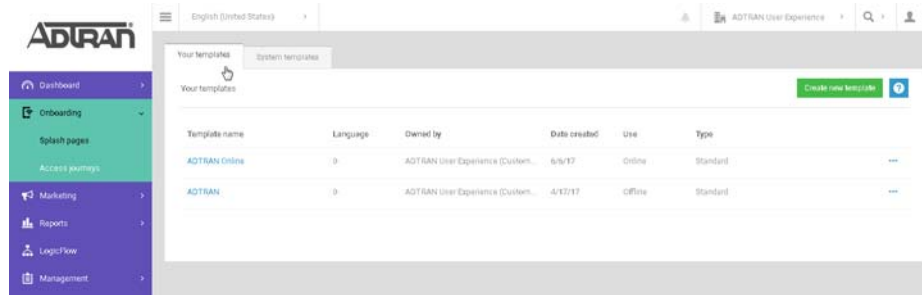
You can duplicate your offline splash page and make a few changes to the template to make it your online splash page. Hover over the ... icon and select **Duplicate**. Change the **Use** to **Online**, complete the form, and select **Create New**.



5. You are now previewing your online splash page. The online splash page is slightly different than the offline splash page. In addition to informing the customer that they are now online, it also provide links to various websites that you can edit. You will not see authentication methods displayed on the online splash page. Once you are satisfied with customization of the online splash page, select **Save template**.



6. Your offline and online splash pages are now complete. You should see them both displayed under **Onboarding > Splash pages**.



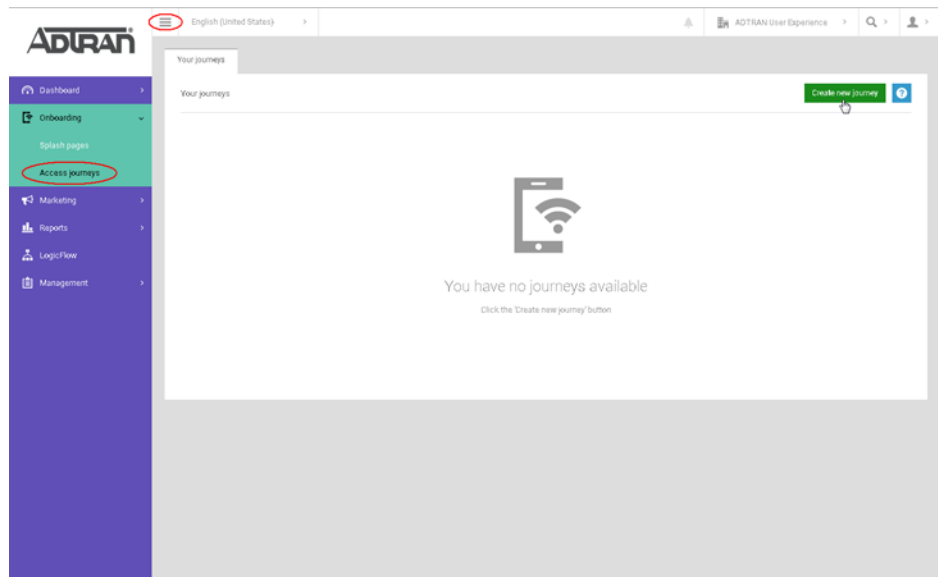
Step 4: Create Your Access Journey

Access journeys allow you to specify a splash page to use for a venue and offer additional configuration options, such as custom terms of service and redirects.

1. From the left-hand menu bar, select the arrow to the right of **Onboarding** to expand the menu options. Select **Access journeys** and then select **Create new journey**.



If you do not see a left-hand menu bar, select the icon with three horizontal lines at the top of the page to display the menu bar.



- Specify a name for the access journey, select **Customer** next to **Ownership scope**, and select the name of the customer for whom you are creating this access journey next to **Owned by**. Select **Create New**.

Create a new journey

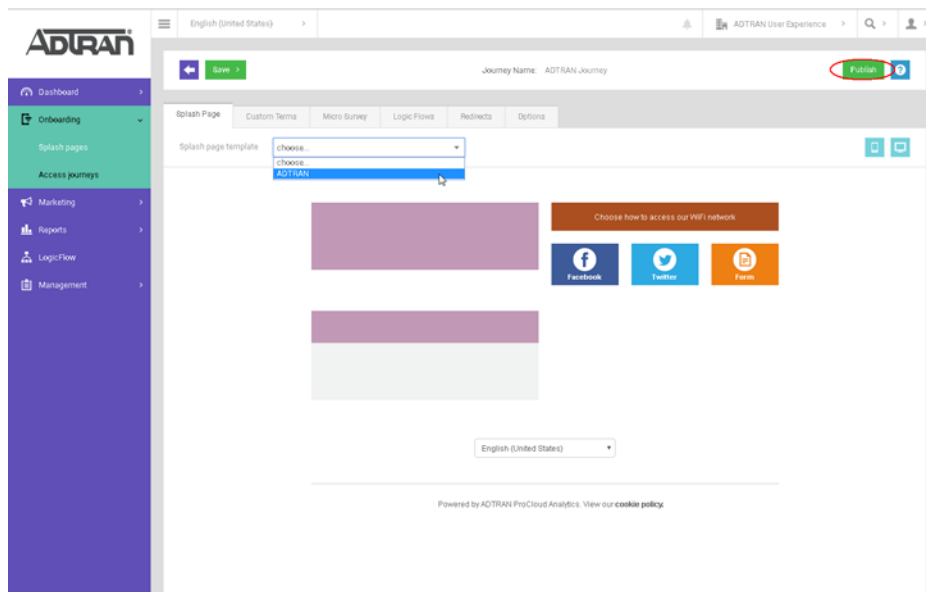
Name

Ownership scope ?

Owned by ?

- You are now editing the newly created access journey. From the **Splash Page** tab, select the name of the offline template you created in Step 2 on [page 27](#). The page will display the template. Select **Publish**.

NOTE *The online splash page will automatically be displayed after users authenticate using the offline splash page. There is no need to specify the online splash page within an access journey.*



- Complete the dialog box with the publishing parameters for this access journey. You can apply the template to a customer, group, location, or hardware. Available options will depend on the design of your network, typically pre-configured based on how you plan to use ProCloud Analytics. Select **Publish**.

Publish Settings

What would you like to apply this template to?

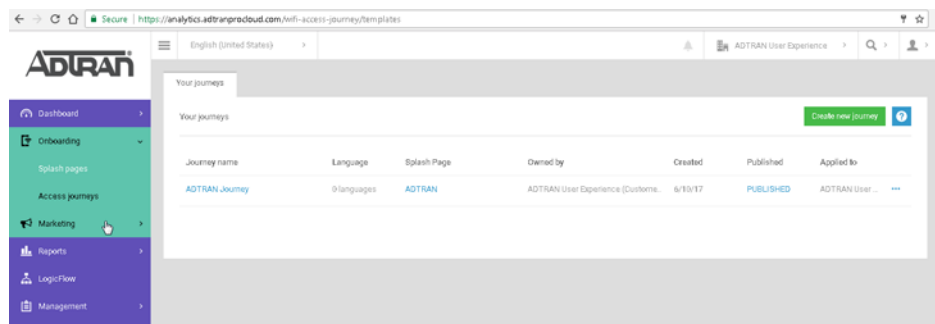
Customer

Group

Location

Hardware

- The page will now display the access journey and relevant settings.



Step 5: Review

Congratulations on successfully setting up ADTRAN ProCloud analytics! The following is a review of the steps you have completed:

- Specified social media preferences for authentication access methods.
- Created an offline splash page.
- Created an online splash page.
- Created an access journey using the offline splash page.