Guide

Cisco public

The bridge to possible

User Defined Network Plus

Deployment Guide

Contents

About this guide

This guide is intended to provide technical guidance to design, deploy, and operate the Cisco® User Defined Network Plus solution leveraging Cisco technology partner Splash Access. It focuses on the steps to enable device-level segmentation for end user devices such as smartphones, tablets, and media streaming devices by first restricting mDNS discovery to a user's personal network or "room" and then optionally restricting unicast traffic between other personal networks or user defined networks (UDNs).

The User Defined Network Plus solution

Streaming content using technologies such as Google Chromecast or Apple AirPlay is easy for users on a home network. In a shared network environment, such as in higher education dormitories, it can be much harder for a user to find their TV among all the other residents' devices. This can cause confusion and annoyance, as students can accidentally stream to a device owned by a different student. This problem is not limited to just streaming to a TV but can affect any device using Link Local Multicast protocols.

Cisco's User Defined Network Plus solution solves this problem by providing each user with their own personal, homelike network on the building's shared network resources. Users can register and manage their own private network, where only their registered devices can communicate with each other, just as if they were on a home network.

For wireless networks managed by Cisco Meraki™, a solution similar to User Defined Network Plus is known as Wi-Fi Personal Network (WPN), and it works in conjunction with Identity Pre-Shared Key (iPSK). For large-scale deployments, user onboarding is typically done using a self-service portal from Splash Access that allows users to authenticate and create unique PSKs that are pushed to the Meraki dashboard via APIs.

Note: WPN is not part of this document. If you would like to explore the WPN functionality for Meraki-managed wireless networks, check out the following link: https://documentation.meraki.com/MR/Encryption_and_Authentication/Wi-Fi_Personal_Network_(WPN).

Splash Access is a Cisco Meraki technology partner and has been integrated with Cisco Meraki for the past seven years. Splash Access provides a secure onboarding system and management portal for end users connecting to a WPN-based SSID.

Previously, to deploy the User Defined Network solution it was necessary to have Cisco Catalyst Center, UDN cloud, and the UDN app in addition to the Cisco Catalyst™ 9800 Series Wireless Controller, Cisco access points (Wave 2 or Catalyst 9100), and Cisco Identity Services Engine (ISE).

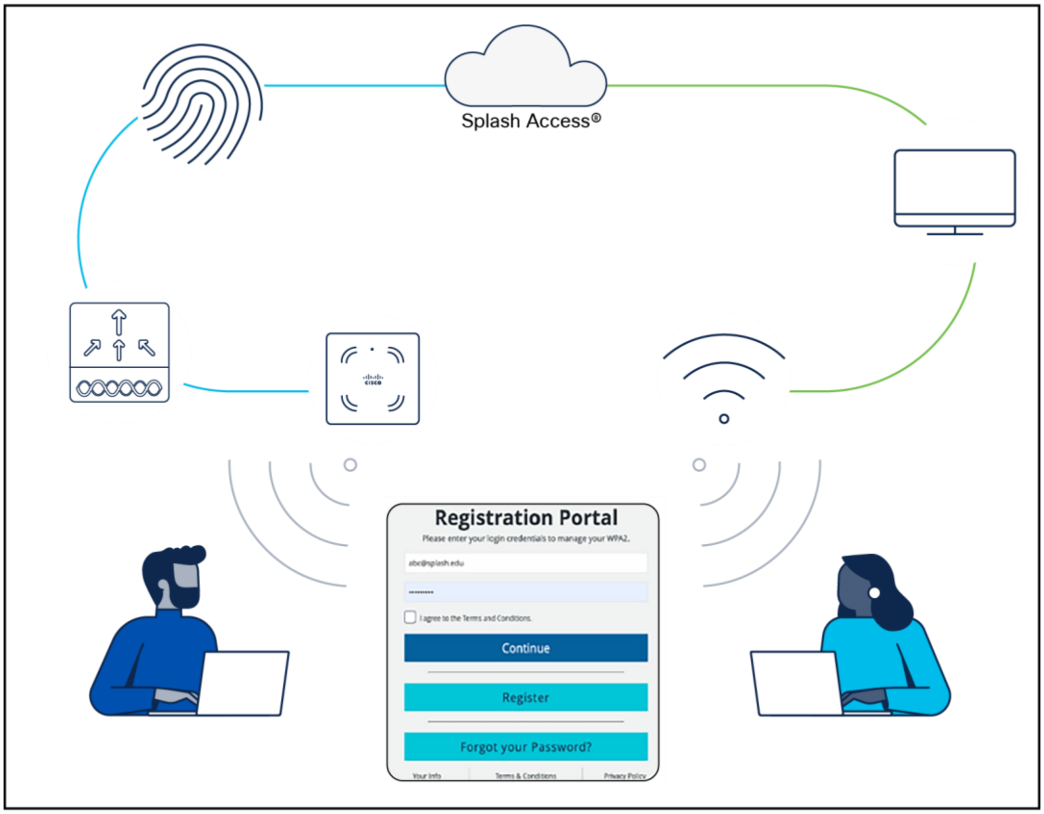


Figure 1.
Splash Access unified user experience

With the Cisco User Defined Network Plus solution, Cisco is simplifying and optimizing the user experience for both Meraki and Catalyst wireless-based deployments. User Defined Network Plus still requires the Catalyst 9800 Series controller, Cisco access points (Wave 2 or Catalyst 9100), and ISE, but the only other requirement is Splash Access. Splash Access integrates with Cisco ISE via APIs.

Tech tip

When deploying Cisco User Defined Network Plus, discovery and streaming are limited to registered devices within the user's defined network for wireless devices such as MacBooks, iPhones, and iPads. For Apple TV, if the AirPlay settings are in their default state, devices with Bluetooth enabled and within approximately 30 feet of the Apple TV – or within the signal distance for Bluetooth Low Energy (BLE) – will still be able to discover and stream to an Apple TV registered within a user defined network. Please refer to Appendix C for the procedure to disable AirPlay over Bluetooth if you would like to change this behavior.

Components

Splash Access

Splash Access communicates with Cisco ISE and is used to create the UDNs. It also registers mobile and other wireless devices as part of the user's private network.

Identity provider

The identity provider (IdP) is your organization's single sign-on (SSO) service, which is used for authentication. Microsoft Azure AD and SAML are the supported IdPs for the User Defined Network Plus solution. SAML is compatible with Shibboleth or Microsoft Active Directory Federated Services (ADFS). When a user authenticates using Splash Access and their credentials, the SSO service is queried and results returned. Upon successful authentication, the user can create their UDN "room" and add their devices.

Cisco Identity Service Engine (ISE)

Cisco ISE, a critical component of the User Defined Network Plus solution, allows you to provide highly secure network access to users and devices. It helps you gain visibility into what is happening in your network, such as who is connected, which applications are installed and running, and much more. It also shares vital contextual data, such as user and device identities, threats, and vulnerabilities with integrated solutions from Cisco technology partners, so you can identify, contain, and remediate threats faster.

In addition to serving as an organization's RADIUS server for authentication, authorization, and accounting (AAA), Cisco ISE inspects authentication attributes from the wireless controller to determine if the authenticating device is attempting to join a UDN-enabled SSID. Once confirmed, ISE communicates the information required for UDN segmentation back to the wireless controller.

Catalyst 9800 Series Wireless Controller

Cisco Catalyst 9800 Series Wireless Controllers are based on Cisco IOS® XE and integrate the RF excellence of Cisco Aironet® access points, creating a best-in-class wireless experience. The 9800 Series is built on an open and programmable architecture with built-in security, streaming telemetry, and rich analytics.

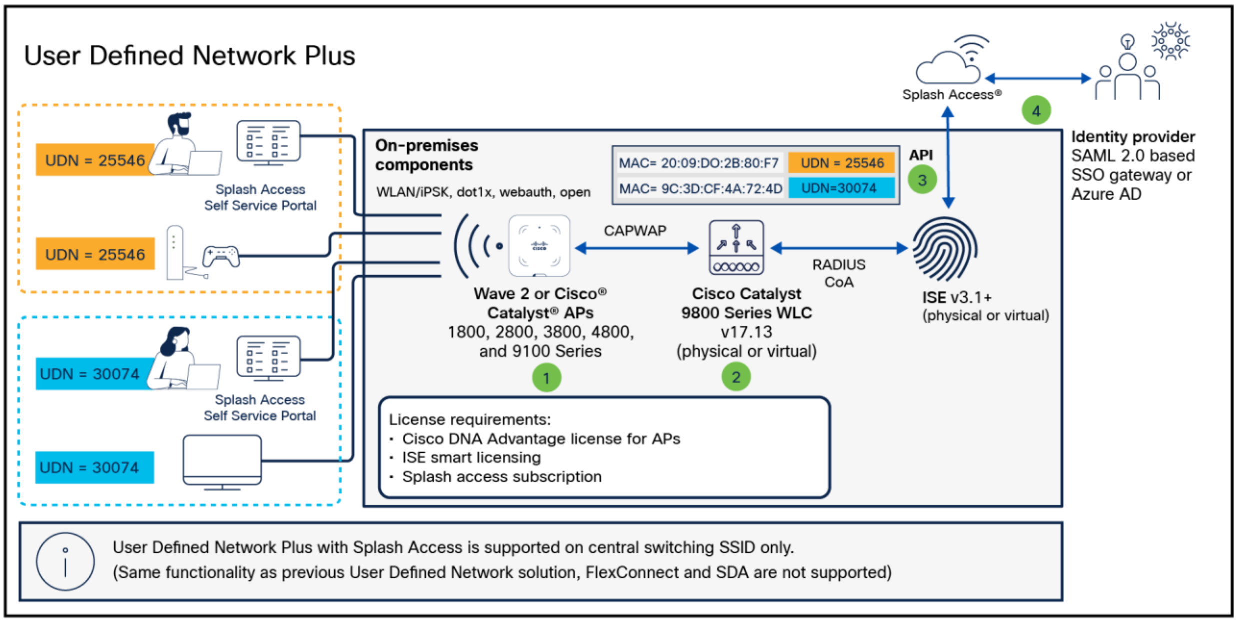
Tech tip
The Cisco User Defined Network Plus solution supports the Catalyst 9800 Series only when it is running in Local mode. Cisco Software-Defined Access (SD-Access) is not supported if fabric-enabled wireless has been deployed. Cisco User Defined Network Plus is supported if the wireless in an SD-Access fabric has been deployed as over the top using Local mode, with both control and data plane encapsulated in a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel between the access point and Catalyst 9800 Series Wireless Controller.

Cisco access points

The Cisco User Defined Network Plus solution supports all Cisco Wave 2 access points, most notably the Cisco Aironet 1800, 2800, 3800, and 4800 Series, as well as Cisco Catalyst 9100 Wi-Fi 6/6E access points.

Solution overview

The Cisco User Defined Network Plus solution incorporates the Catalyst 9800 Series controllers, Splash Access, and ISE components to provide segmented, personal networks in which users' mobile devices and streaming entertainment devices are isolated from one another by limiting multicast advertisement of services and optionally providing unicast blocking of communications between those segmented, personal networks (referred to as UDNs). Splash Access is used for device registration and de-registration. The Cisco User Defined Network Plus solution's on-premises components include Catalyst 9800 Series controllers, Wave 2 or Catalyst 9100 access points, and Cisco ISE for network access control through RADIUS AAA.



License requirements:
- Cisco DNA Advantage license for APs
- ISE smart licensing
- Splash access subscription

User Defined Network Plus with Splash Access is supported on central switching SSID only.
(Same functionality as previous User Defined Network solution, FlexConnect and SDA are not supported)

Figure 2.
Device registration and onboarding in the User Defined Network Plus solution

Cisco Identity Services Engine

In addition to providing RADIUS AAA services for user/device authentication, Cisco ISE is responsible for three other functions in the User Defined Network Plus solution:

1. ISE processes device registration and room assignment/change requests from information forwarded from Splash Access across all ISE policy service nodes in the deployment.

2. ISE interacts with the Catalyst 9800 Series controller in RADIUS authentication requests by retrieving UDN assignments for onboarding end user devices from its local database.

3. Upon successful authentication, ISE sends a RADIUS response to the wireless controller containing three UDN vendor-specific attributes (VSAs) used for UDN segmentation at the wireless controller and access point.

    - cisco-av-pair = UDN:Private-group-id (UDN ID used to separate multicast/broadcast domains)
    - cisco-av-pair = UDN:Private-group-name (The UDN “name” of the room created by a user)
    - cisco-av-pair = UDN:Private-group-owner (Identifies if the device is the owner of the UDN)

There are some manual, UDN-specific configurations required for ISE and Splash Access. All User Defined Network Plus and device registration configuration is performed via the Splash Access service. A new User Defined Network Plus pxGrid service is added that allows both ISE and Splash Access to communicate with ISE via REST APIs. ISE makes use of a new pxGrid “status” topic whenever User Defined Network Plus assignments are created, updated, or deleted.

Upon Splash Access integration with ISE, two new database tables are created. The first is for Device -UDN assignment records based on MAC addresses; this is used for device authentication. The second table is for UDN properties for which UDN is enabled and, if so, the wireless controller and SSIDs it is enabled on; this is used to check whether the authentication request received has originated from a UDN-enabled WLC or SSID requiring the extra UDN device lookup. Both database tables are replicated across a distributed ISE deployment.

Catalyst 9800 Series wireless controller

The Cisco User Defined Network Plus solution requires Cisco IOS XE-based Catalyst 9800 Series wireless controllers, either physical or virtual; AireOS-based controllers and Catalyst 9800 embedded (switch or access point) controllers are not supported. With the introduction of User Defined Network Plus, SSIDs can be defined and dedicated to UDNs in addition to those SSIDs dedicated to normal enterprise and guest wireless access. The UDN SSIDs can be configured for 802.1X, MAC Authentication Bypass (MAB), or PSK or iPSK. Prior to UDN+, only a single Catalyst 9800 Series controller or High Availability (HA) pair was supported. As a result, all devices and their UDNs are local to the WLC and the specific SSIDs associated with the UDNs, so roaming between controllers is not supported.

The mDNS Gateway functionality of the Catalyst 9800 Series WLC is completely interoperable with the User Defined Network Plus functionality. The gateway functionality must be configured separately. The mDNS Gateway functionality is required for advertisement of Bonjour services across Layer 3 networks. If your UDN+ deployment is deployed across multiple VLANs, mDNS Gateway will be required if devices in a UDN will need to discover devices in another VLAN.

Tech tip

For more information regarding mDNS, please refer to the mDNS Deployment Guide for Cisco Catalyst 9800 Series WLCs.

If a user registered their device offsite using the Splash Access portal, that device can access the User Defined Network Plus SSID upon connecting to the wireless network. If, however, due to MAC randomization they were unable to pre-register their device, the user can connect their device to any SSID providing internet access and register the device once attached to the wireless network. The SSID joined for registration while onsite could be the UDN SSID or any other, as long as the user has the credentials necessary to access the organization's wireless network based on the security implemented.

Once a device successfully registers and connects to the UDN SSID, the wireless controller sends a RADIUS authentication request to Cisco ISE. In addition to the authentication method (802.1X, MAB, or PSK) based on the wireless security configured for the UDN SSID, ISE performs a lookup for that device's MAC address and returns the authentication results as well as the RADIUS UDN-ID to the wireless controller if the MAC address is found in the ISE database. Splash Access populates the MAC addresses in the ISE identity database at the time of device registration. If no UDN information is associated with a device from Splash Access, ISE will not relay any specific UDN information back to the wireless controller and the device will be granted access upon successful authentication.

When joining the UDN SSID, if authentication is successful but the device is not registered to a user's network, the device will still gain access to the network and will be assigned a UDN-ID of zero. With a UDN-ID of zero, the device will be able to communicate in north/south fashion to the internet and wired enterprise resources. It will not be able to communicate with any other wireless devices within that UDN SSID.

When devices associated with a specific UDN attach to the UDN SSID, the controller will segment the various discovery protocol traffic, such as mDNS, to only that UDN. This will work across all Wave 2 and Catalyst 9100 access points. As a result, only those devices within a specific UDN will see the services broadcasted by any device within that UDN. Segmentation of multicast and broadcast advertisements is performed directly on the Cisco access points. Unicast controls are implemented at the wireless controller.

By default, unicast traffic is permitted between UDNs, while multicast traffic, such as mDNS, is always contained within the UDN. This default behavior of allowing unicast communications between UDNs can be changed during configuration of the UDN at the WLAN policy profile in the wireless security policy associated with the UDN WLAN. With unicast blocking enabled, mobile devices can communicate only with other devices in the same UDN or anything northbound, external to the wireless network.

Device registration and onboarding

This section provides an overview of the communications during device registration and subsequent attachment to the wireless network.

Device registration flow

1. Using the Splash Access device registration portal, the device registers with Splash Access.
2. Splash Access authenticates the user either against Azure AD or an IDP via SAML 2.0.
3. The user's network is created, and all devices' MAC address information for that UDN are collected. This can be performed offsite, before any device attaches to that user's network, if MAC randomization is disabled on the device, or onsite where MAC randomization can be enabled.
4. Upon device registration, Splash Access communicates with Cisco ISE, which in turn relays registration information for the device, including the UDN-ID, UDN name, and MAC addresses entered or if iPSK is used.
5. Registration information is then passed to Cisco ISE and stored in a database for later use when devices join the SSID and gain access to the wireless network.

Device network access

1. When the device is onsite, the UDN SSID will be selected at the device. The SSID can be configured with either a PSK, 802.1X, or MAB flow to authenticate the device.
2. A RADIUS authentication request is sent from the wireless controller to ISE.
3. ISE checks its database to perform a lookup of the MAC address in its endpoint database.
4. Upon a successful lookup, ISE passes the RADIUS response back to the wireless controller along with vendor-specific attributes identifying the
   - private-group-id: Used by the wireless controller to identify the user's network and isolate multicast and broadcast traffic between UDNs
   - private-group-name: Name of the "room" or UDN
   - private-group-owner: If the UDN is owned by that device
5. The wireless controller programs the access point with the appropriate UDN information to block multicast and broadcast traffic between UDNs.

Product requirements

The following table provides the software versions validated within this deployment guide.

Table 1. Supported software versions

Device or component	Version
Cisco Catalyst Center	2.3.5.5 or later
ISE	3.1 Patch 4 or later
Catalyst 9800 Series Wireless Controller	Cisco IOS XE 17.13.X or later with Cisco DNA Advantage licenses for access points
Cisco wireless access point	Cisco IOS XE 17.13.3 or later
Splash Access subscription	Cloud-based
Identity provider	Azure AD or SAML 2.0-enabled service

Scale

The following table provides scale numbers for the solution.

Table 2. Scale capability per device

Device	Scale
Cisco Catalyst 9800-80	Up to 64,000 unique UDNs per controller
Cisco Catalyst 9800-40	Up to 32,000 unique UDNs per controller
Cisco Catalyst 9800-L	Up to 5,000 unique UDNs per controller
Cisco Catalyst 9800-CL (private cloud)	10,000, 32,000, or 64,000 unique UDNs per controller
Cisco ISE	Up to 2 million endpoints
Splash Access	Subscription per access point

Process: Prerequisites

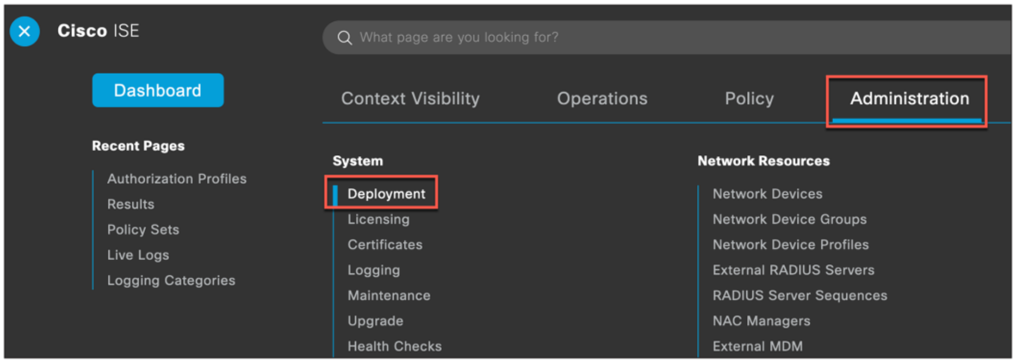
This process details the necessary steps to set up network components for the User Defined Network Plus solution. These include configuring the Catalyst 9800 Series Wireless Controller and ISE and creating a Splash Access administrator account.

- Customers need to request a Splash Access administrator account from Splash Access: https://www.splashaccess.com/request-demo/
- The Catalyst 9800 Series controller should be added to ISE and vice versa. https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214490-configure-radius-and-tacacs-for-gui-and.html
- ISE requires a **public IP address** to communicate with Splash Access, and the firewall should allow Splash Access source IP address 209.94.60.109. This Splash Access IP address can be different for different customer tenants. Also, the following ISE ports should be opened or accessible:

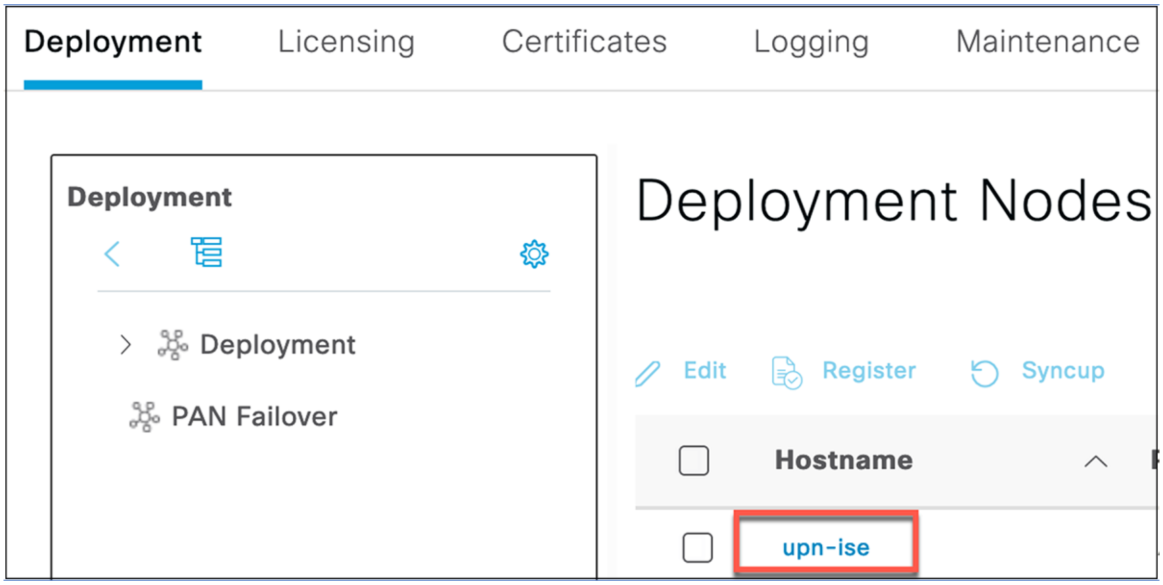
- HTTPS: TCP/443
- ISE pxGrid: TCP/8910
- ERS REST API: TCP/9060

ISE ERS/pxGrid configuration

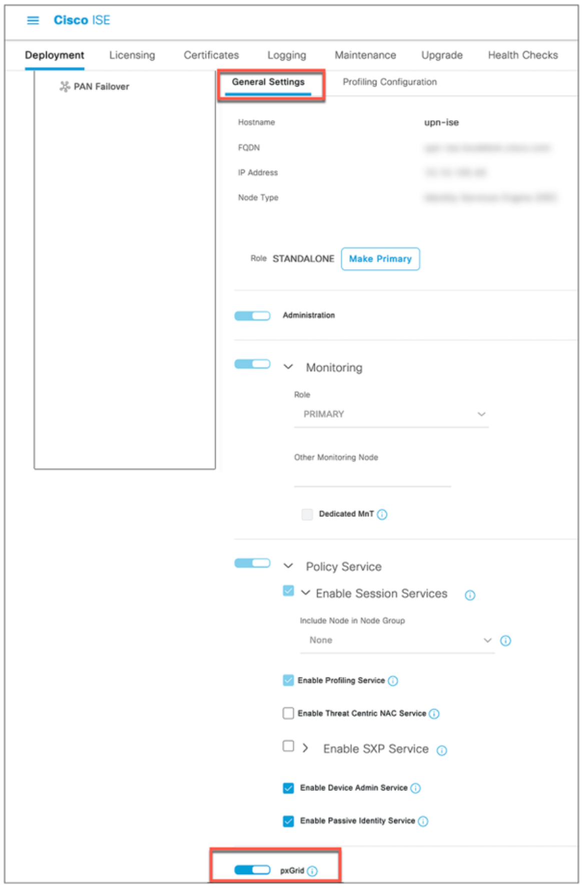
Step 1. Log in to the Cisco ISE Primary Admin Node (PAN) and navigate to **Administration > Deployment**.



Step 2. Select the hostname of the ISE node.



Step 3. Under General Settings, confirm that the **pxGrid** checkbox is selected or the toggle button is blue, and click **Save**.



Hostname upn-ise

FQDN [redacted]

IP Address [redacted]

Node Type [redacted]

Role STANDALONE

Administration

Monitoring

Role PRIMARY

Other Monitoring Node

□ Dedicated MnT

Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

□ Enable SXP Service

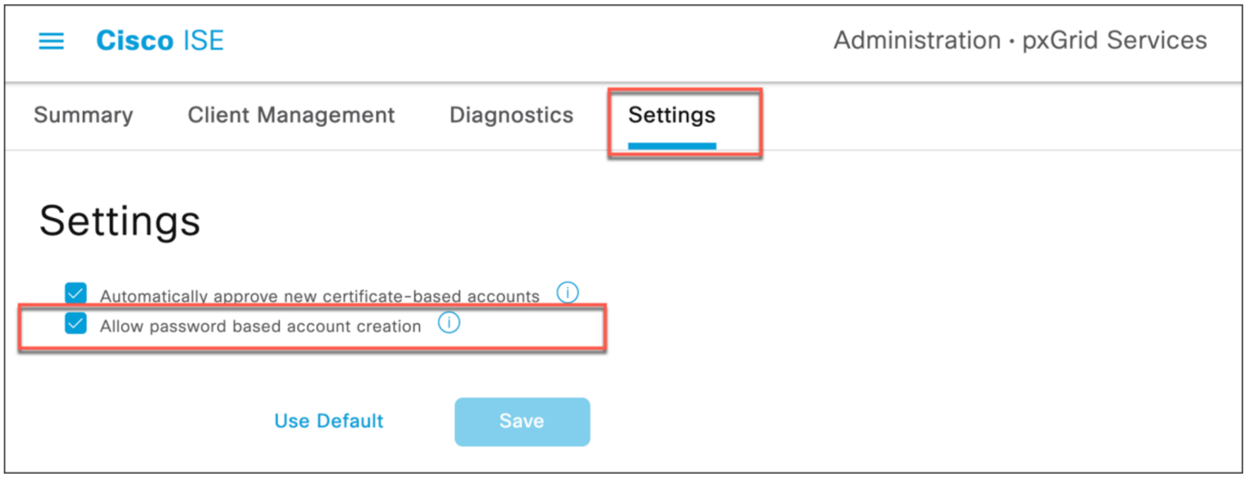
☑ Enable Device Admin Service

☑ Enable Passive Identity Service

pxGrid

Step 4. Navigate to **Administration > pxGrid Services > Settings.**

Step 5. Check that **Automatically approve new certificate-based accounts** and **Allow password based account creation** are enabled, and click **Save**.



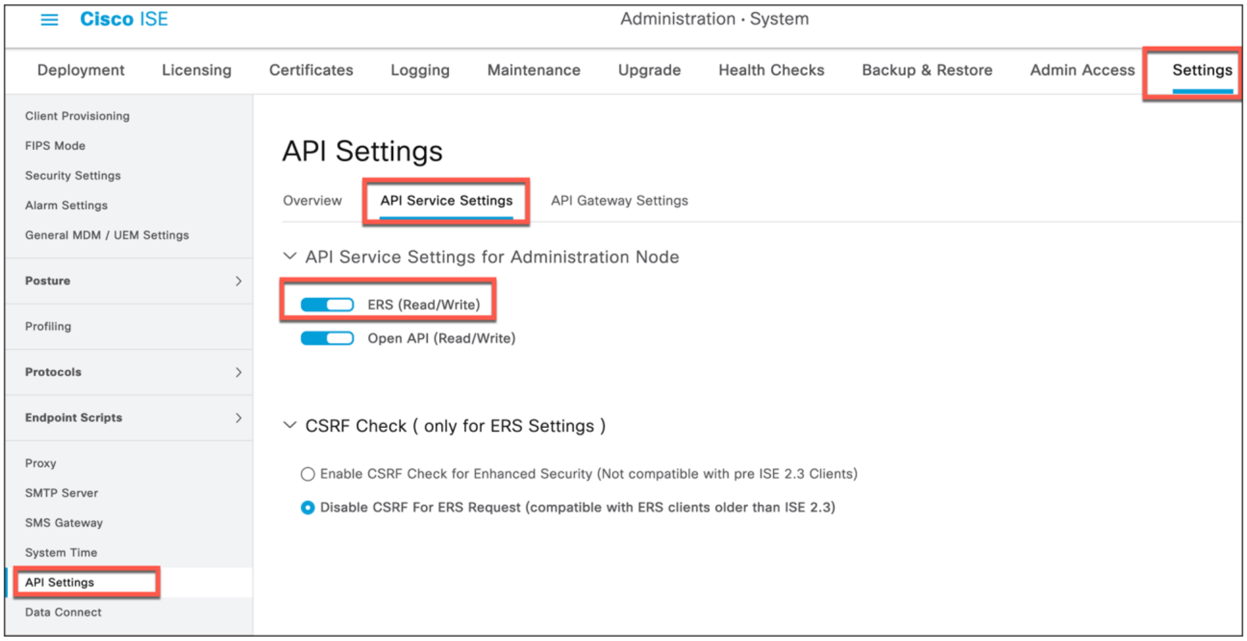
Settings

☑ Automatically approve new certificate-based accounts

☑ Allow password based account creation

Step 6. Navigate to **Administration > System > Settings > API Settings**.

Step 7. Enable **ERS (Read/Write) and** click **Save**.



API Settings

API Service Settings for Administration Node

- ERS (Read/Write)
- Open API (Read/Write)

CSRF Check (only for ERS Settings)

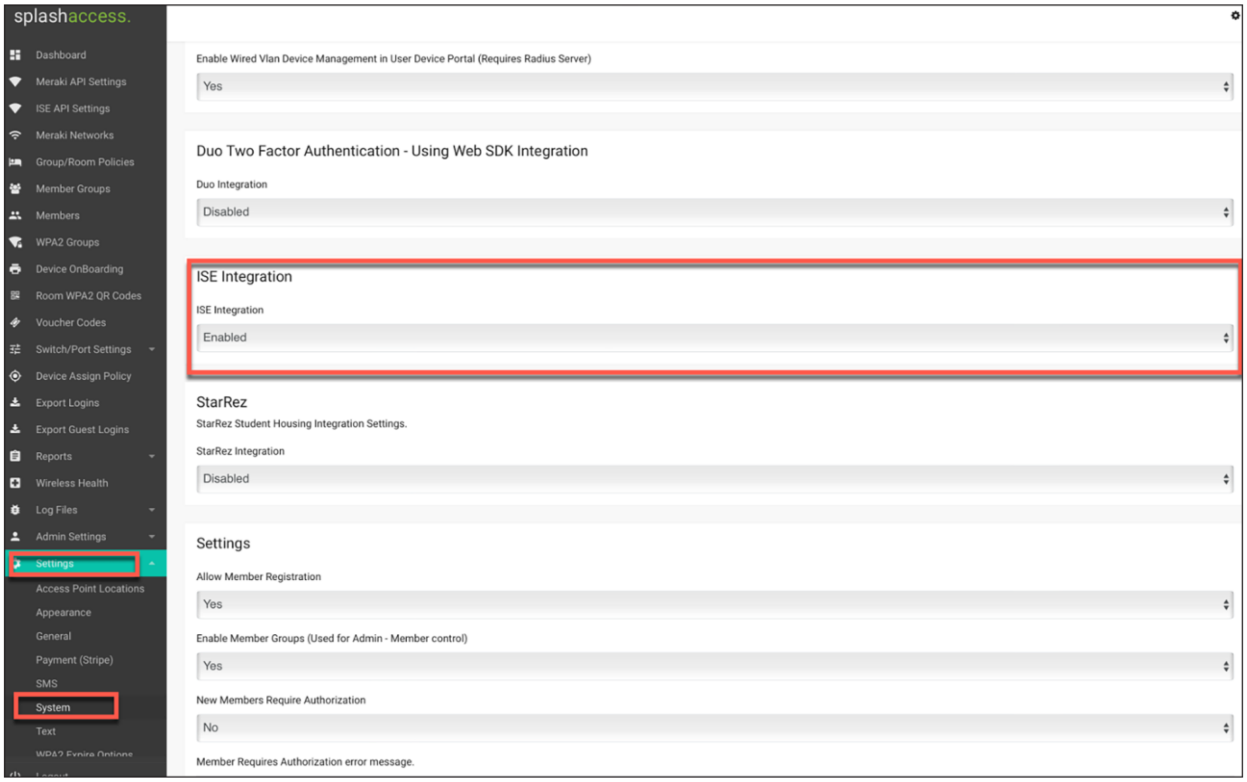
○ Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)

● Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)

Process: Splash Access and ISE integration

A Splash Access admin management account and subscription is required for the User Defined Network Plus solution. Once acquired, proceed by accessing the Splash Access admin portal as described below.
https://<customer-account-name>splashudn.com/accounts/<customer-account-name>/management/

Step 1. Enable ISE in the Splash Access portal. From the main menu, go to **Settings > System > ISE Integration** and, from the drop-down, select **Enabled**.



Enable Wired Vlan Device Management in User Device Portal (Requires Radius Server): Yes

Duo Two Factor Authentication - Using Web SDK Integration

Duo Integration: Disabled

ISE Integration

ISE Integration: Enabled

StarRez

StarRez Student Housing Integration Settings.

StarRez Integration: Disabled

Settings

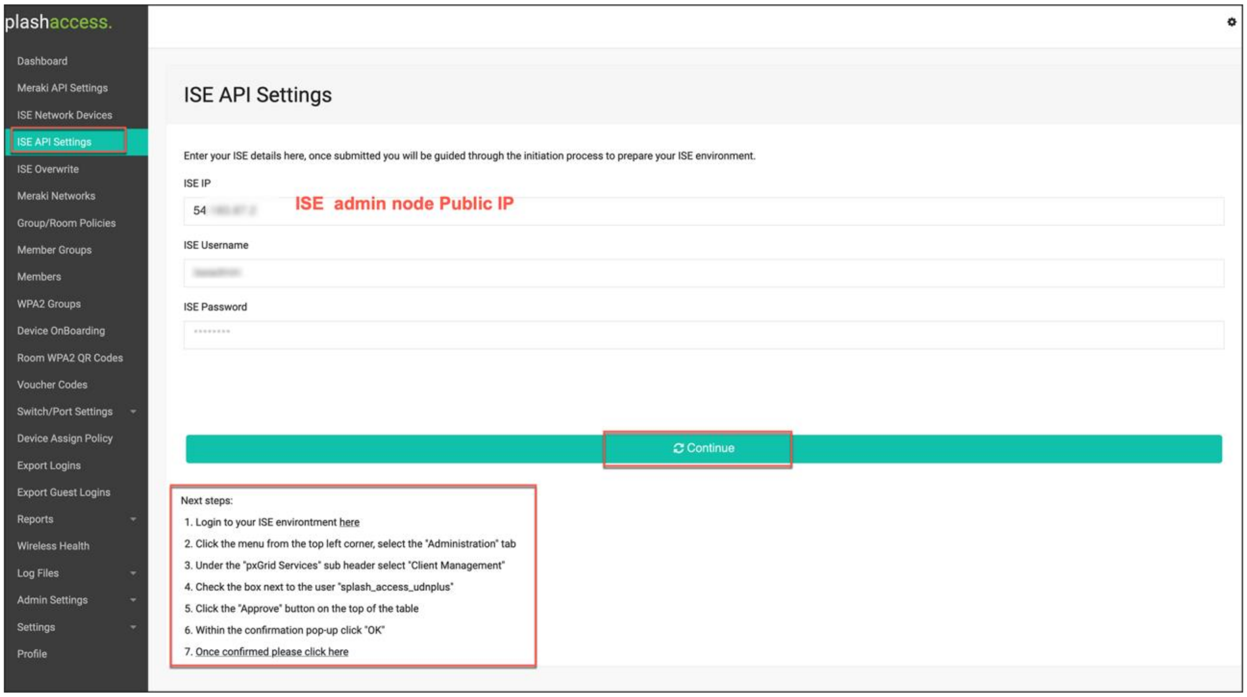
Allow Member Registration: Yes

Enable Member Groups (Used for Admin - Member control): Yes

New Members Require Authorization: No

Member Requires Authorization error message.

Step 2. Navigate to **ISE API Settings** in the menu, enter the public IP of ISE, and enter the ISE user credentials for API access. Click **Continue**.



ISE API Settings

Enter your ISE details here, once submitted you will be guided through the initiation process to prepare your ISE environment.

ISE IP: 54 [redacted]

ISE admin node Public IP

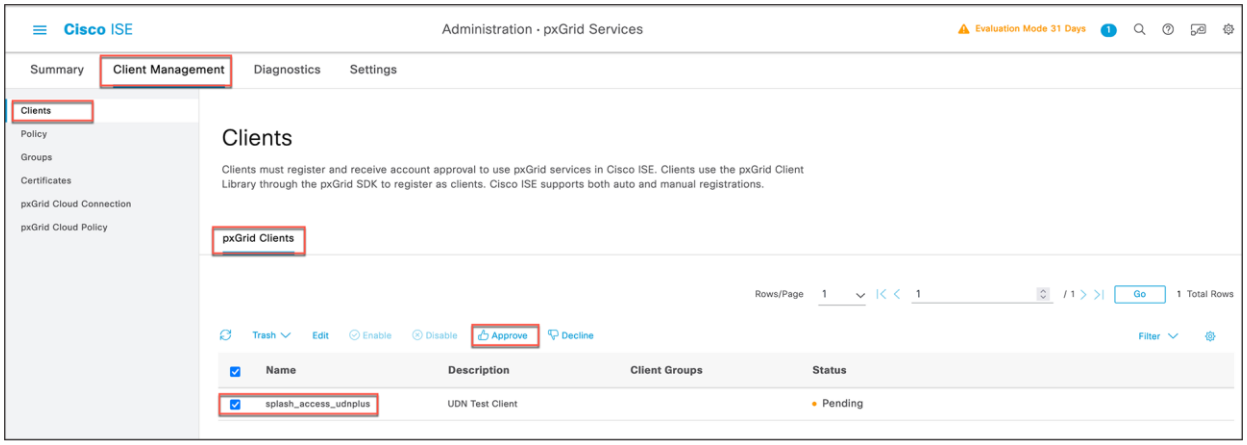
ISE Username: [redacted]

ISE Password: ········

Next steps:

1. Login to your ISE environment here
2. Click the menu from the top left corner, select the "Administration" tab
3. Under the "pxGrid Services" sub header select "Client Management"
4. Check the box next to the user "splash_access_udnplus"
5. Click the "Approve" button on the top of the table
6. Within the confirmation pop-up click "OK"
7. Once confirmed please click here

Step 3. Log in to the ISE portal and navigate to **Administration > pxGrid Services > Client Management**. Check the box next to the "splash_access_udnplus" user. Click **Approve**.

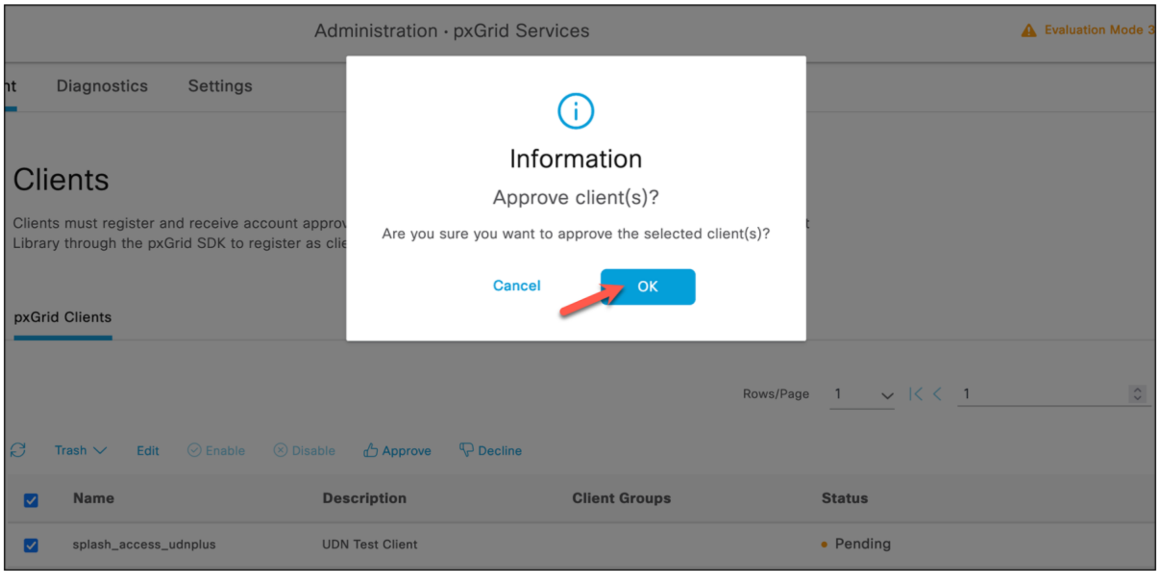


Clients

Clients must register and receive account approval to use pxGrid services in Cisco ISE. Clients use the pxGrid Client Library through the pxGrid SDK to register as clients. Cisco ISE supports both auto and manual registrations.

☑	Name	Description	Client Groups	Status
☑	splash_access_udnplus	UDN Test Client		● Pending

When the confirmation dialog box appears, click **OK**.



Clients

Clients must register and receive account approv... Library through the pxGrid SDK to register as clie...

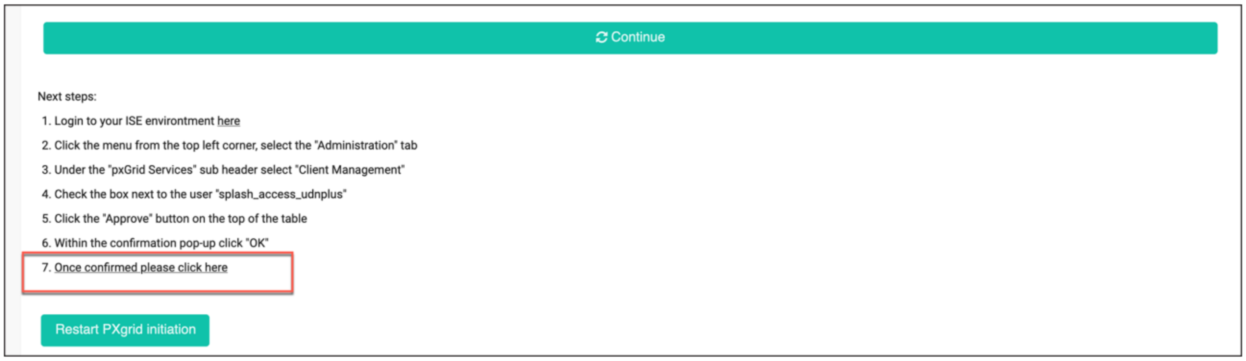
Information

Approve client(s)?

Are you sure you want to approve the selected client(s)?

☑	Name	Description	Client Groups	Status
☑	splash_access_udnplus	UDN Test Client		● Pending

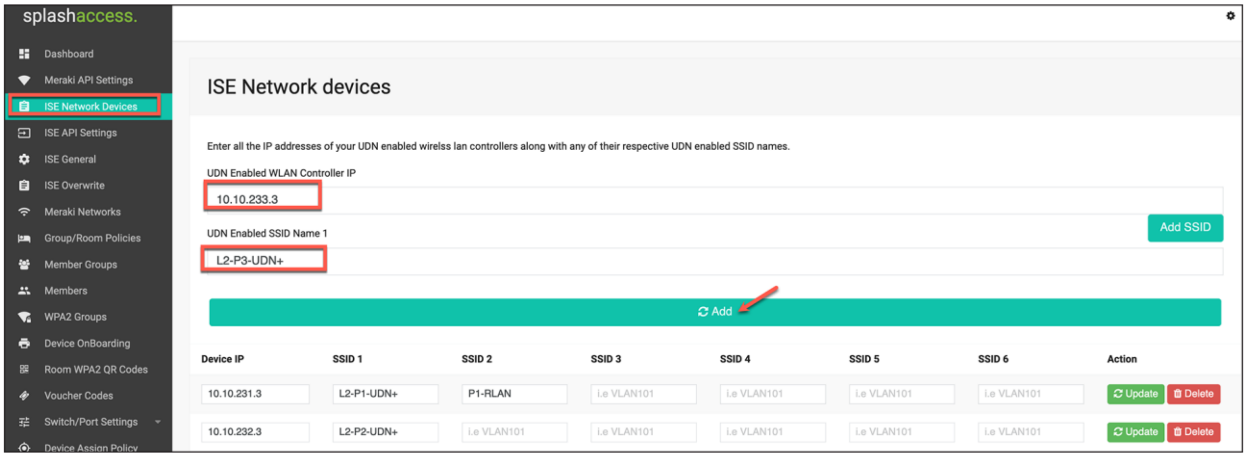
Step 4. When approved from ISE, go to the Splash Access admin portal to confirm the settings by clicking step 7, **Once confirmed please click here**.



Next steps:

1. Login to your ISE environment here
2. Click the menu from the top left corner, select the "Administration" tab
3. Under the "pxGrid Services" sub header select "Client Management"
4. Check the box next to the user "splash_access_udnplus"
5. Click the "Approve" button on the top of the table
6. Within the confirmation pop-up click "OK"
7. Once confirmed please click here

Step 5. Now go to **ISE Network Devices** and enter the IP addresses of your UDN-enabled WLC, along with any of its respective UDN-enabled WLANs (SSIDs) and remote LAN (RLAN) names.



ISE Network devices

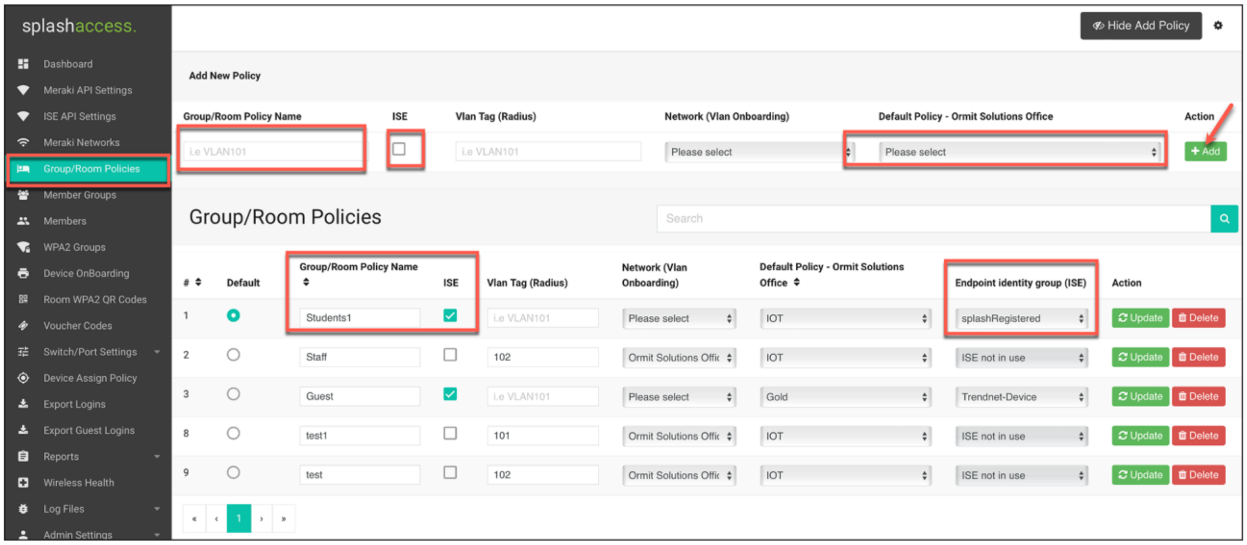
Enter all the IP addresses of your UDN enabled wirelss lan controllers along with any of their respective UDN enabled SSID names.

UDN Enabled WLAN Controller IP: 10.10.233.3

UDN Enabled SSID Name 1: L2-P3-UDN+

Device IP	SSID 1	SSID 2	SSID 3	SSID 4	SSID 5	SSID 6	Action
10.10.231.3	L2-P1-UDN+	P1-RLAN	i.e VLAN101	i.e VLAN101	i.e VLAN101	i.e VLAN101	Update Delete
10.10.232.3	L2-P2-UDN+	i.e VLAN101	i.e VLAN101	i.e VLAN101	i.e VLAN101	i.e VLAN101	Update Delete

Step 6. Navigate to **Group/Room Polices**. Create a policy name and match it to the AD group name if required. (This group/room policy name should be the same as configured on your Azure AD.) In the endpoint identity group drop-down, choose the group from which you want to insert devices.



Add New Policy

Group/Room Policy Name	ISE	Vlan Tag (Radius)	Network (Vlan Onboarding)	Default Policy - Ormit Solutions Office	Action
i.e VLAN101	□	i.e VLAN101	Please select	Please select	+ Add

Group/Room Policies

#	Default	Group/Room Policy Name	ISE	Vlan Tag (Radius)	Network (Vlan Onboarding)	Default Policy - Ormit Solutions Office	Endpoint identity group (ISE)	Action
1	●	Students1	☑	i.e VLAN101	Please select	IOT	splashRegistered	Update Delete
2	○	Staff	□	102	Ormit Solutions Offic	IOT	ISE not in use	Update Delete
3	○	Guest	☑	i.e VLAN101	Please select	Gold	Trendnet-Device	Update Delete
8	○	test1	□	101	Ormit Solutions Offic	IOT	ISE not in use	Update Delete
9	○	test	□	102	Ormit Solutions Offic	IOT	ISE not in use	Update Delete

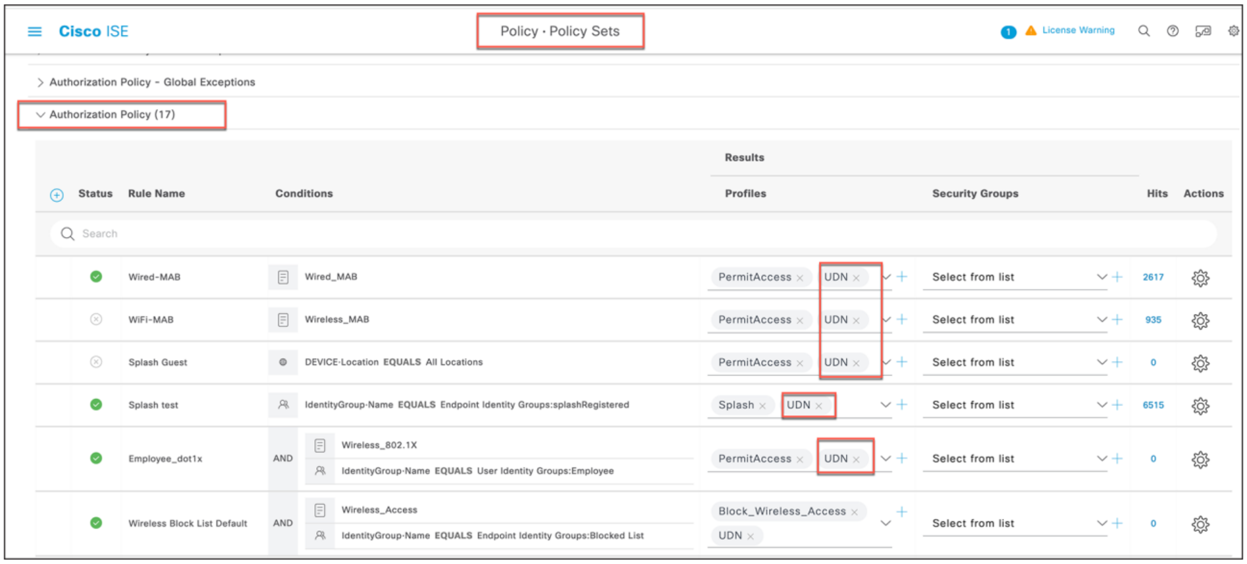
ISE policy created for UDN

Once the Splash Access and ISE authentication are approved, this process will verify that the UDN authorization profile has been pushed to ISE.

Step 1. Log in to ISE and navigate to **Policy > Policy Sets**.

Step 2. Click the > next to your Policy Sets and click to expand the authorization policy.

Step 3. Check to see that the UDN authorization profile has been pushed to every policy rule.


Cisco ISE
Policy · Policy Sets
License Warning
> Authorization Policy - Global Exceptions
∨ Authorization Policy (17)
Search

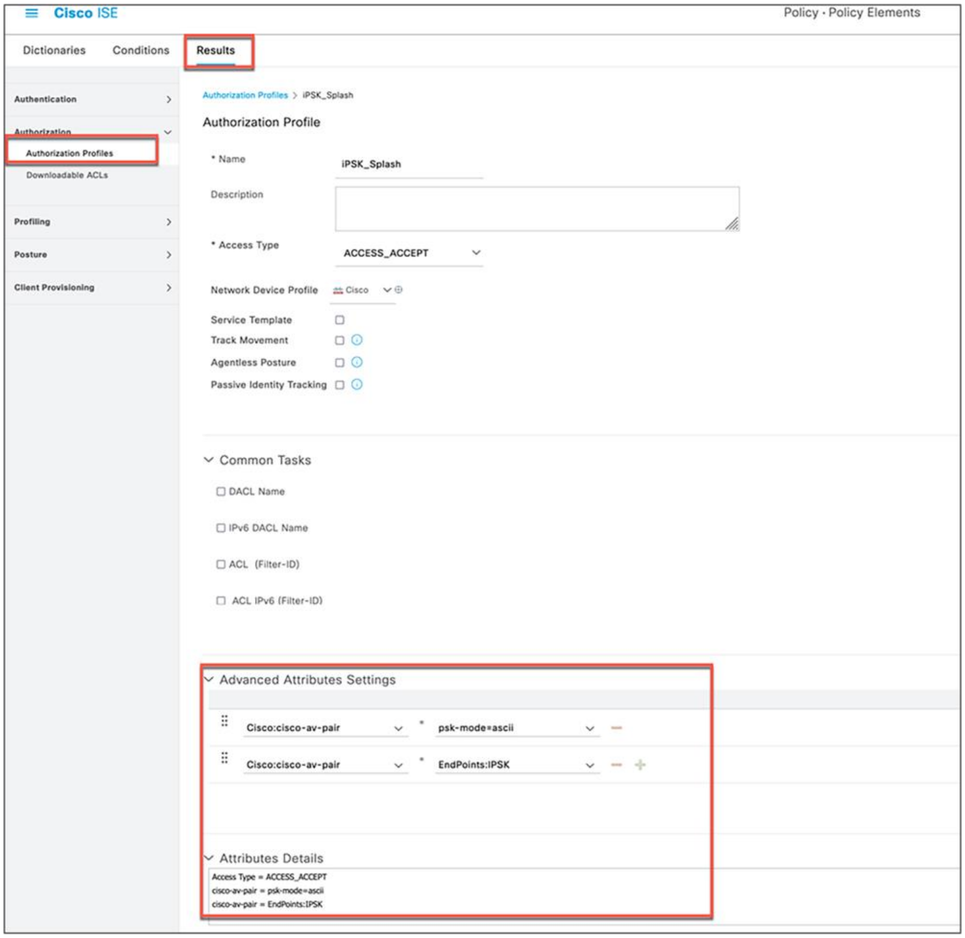
Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	Wired-MAB	Wired_MAB	PermitAccess × UDN ×	Select from list	2617	⚙
⊗	WiFi-MAB	Wireless_MAB	PermitAccess × UDN ×	Select from list	935	⚙
⊗	Splash Guest	DEVICE·Location EQUALS All Locations	PermitAccess × UDN ×	Select from list	0	⚙
✓	Splash test	IdentityGroup·Name EQUALS Endpoint Identity Groups:splashRegistered	Splash × UDN ×	Select from list	6515	⚙
✓	Employee_dot1x	AND Wireless_802.1X IdentityGroup·Name EQUALS User Identity Groups:Employee	PermitAccess × UDN ×	Select from list	0	⚙
✓	Wireless Block List Default	AND Wireless_Access IdentityGroup·Name EQUALS Endpoint Identity Groups:Blocked List	Block_Wireless_Access × UDN ×	Select from list	0	⚙

Step 4. **(Optional if using iPSK):** If iPSK is required or implemented, you will need to create another authorization profile on ISE. Navigate to **ISE > Policy > Results > Authorization Profiles**, then create an authorization profile for iPSK as follows:

Under Advanced Attributes Settings, create the following:

Cisco:cisco-av-pair = psk-mode=ascii

Cisco:cisco-av-pair = EndPoints:IPSK



Authorization Profile

* Name: iPSK_Splash

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Common Tasks

□ DACL Name

□ IPv6 DACL Name

□ ACL (Filter-ID)

□ ACL IPv6 (Filter-ID)

Advanced Attributes Settings

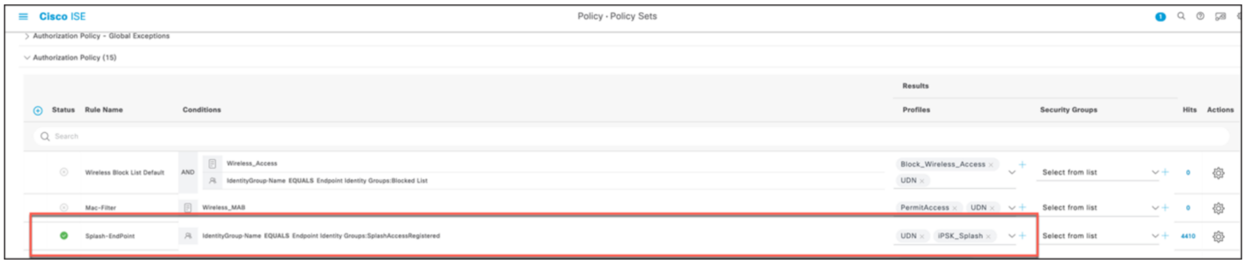
Cisco:cisco-av-pair = psk-mode=ascii

Cisco:cisco-av-pair = EndPoints:IPSK

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = EndPoints:IPSK

Now, in **ISE > Policy > Policy Sets**, configure an authorization rule that has the UDN and iPSK policy.


Cisco ISE
Policy · Policy Sets
> Authorization Policy - Global Exceptions
Authorization Policy (15)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
	Wireless Block List Default	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blocked List	Block_Wireless_Access UDN	Select from list	0	
	Mac-Filter	Wireless_MAB	PermitAccess, UDN	Select from list	0	
●	Splash-EndPoint	IdentityGroup-Name EQUALS Endpoint Identity Groups:SplashAccessRegistered	UDN, iPSK_Splash	Select from list	4410	

Splash Access workflow with ISE pxGrid (reference)

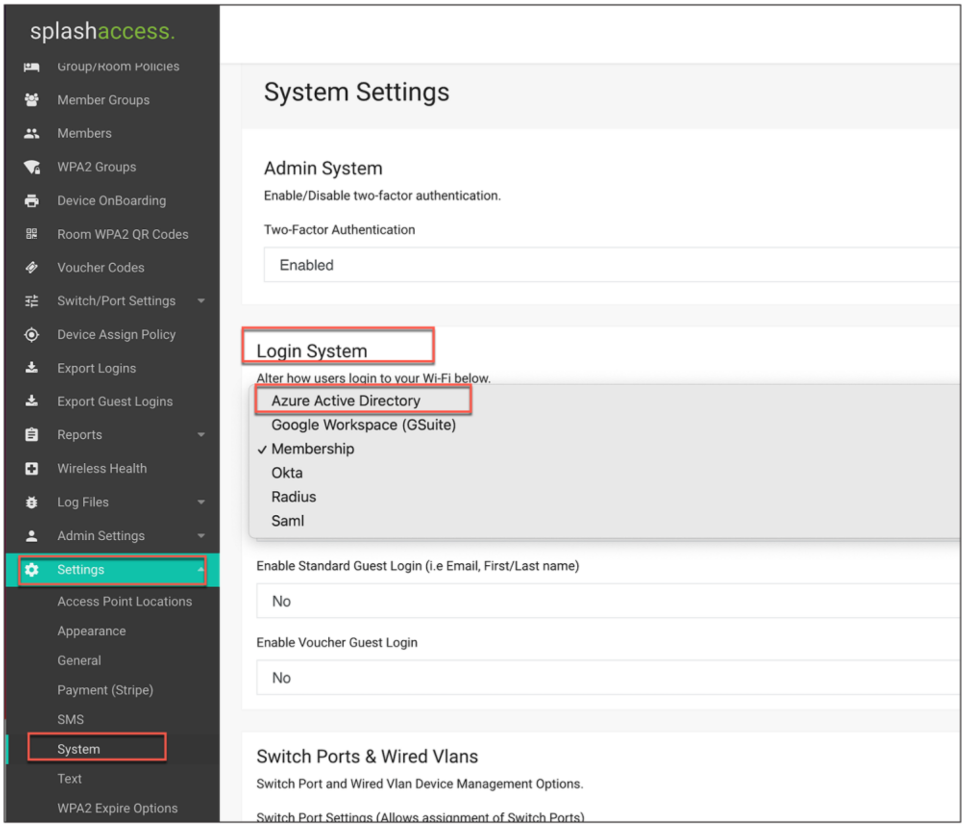
1. User logs in to the Splash Access admin portal and navigates to ISE API Settings
2. User inputs the ISE IP, Port, Username, and Password for the ISE ERS environment
3. Splash system sends POST to https://[ISE IP]:8910/pxgrid/control/AccountCreate for "userName" and "password"
4. Splash system creates a basic auth token by base64 encoding "[userName]:[password]"
5. Splash system sends POST to https://[ISE IP]:8910/pxgrid/control/AccountActivate with basic auth and with "description":"pxGrid REST User" to check for "accountState":"PENDING"
6. User logs in to ISE portal and navigates to Administration > pxGrid Services > Client Management
7. User checks box next to "splash_access_pxgrid" user and clicks "Approve"

8. Splash system sends POST to https://[ISE IP]:8910/pxgrid/control/AccountActivate with basic auth and with "description":"pxGrid REST User" to check for "accountState":"ENABLED"
9. Splash system sends POST to https://[ISE IP]:8910/pxgrid/control/ServiceLookup with basic auth and with "name":"com.cisco.ise.config.upn" to check for "services"[0]"nodeName" value
10. Splash system sends POST to https://[ISE IP]:8910/pxgrid/control/AccessSecret with basic auth and with "peerNodeName":"[nodeName]" to fetch "secret" value
11. Splash system creates new basic auth token by base64 encoding "[userName]:[secret]"
12. Splash system sends POST to https://[ISE IP]:8910/pxgrid/control/AccessSecret with new basic auth and with "upnEnabled":"true"

Splash Access Azure/SAML setup

Administrators can enable and integrate iDPs such as Azure or SAML 2.0-based SSO from Splash Access.

Step 1. From the Splash Access admin dashboard, navigate to **Settings > System > Login Systems > System Type** and choose the system type from the drop-down. Select Azure or SAML.



System Settings

Admin System

Enable/Disable two-factor authentication.

Two-Factor Authentication: Enabled

Login System

Alter how users login to your Wi-Fi below.

- Azure Active Directory
- Google Workspace (GSuite)
- ✓ Membership
- Okta
- Radius
- Saml

Enable Standard Guest Login (i.e Email, First/Last name): No

Enable Voucher Guest Login: No

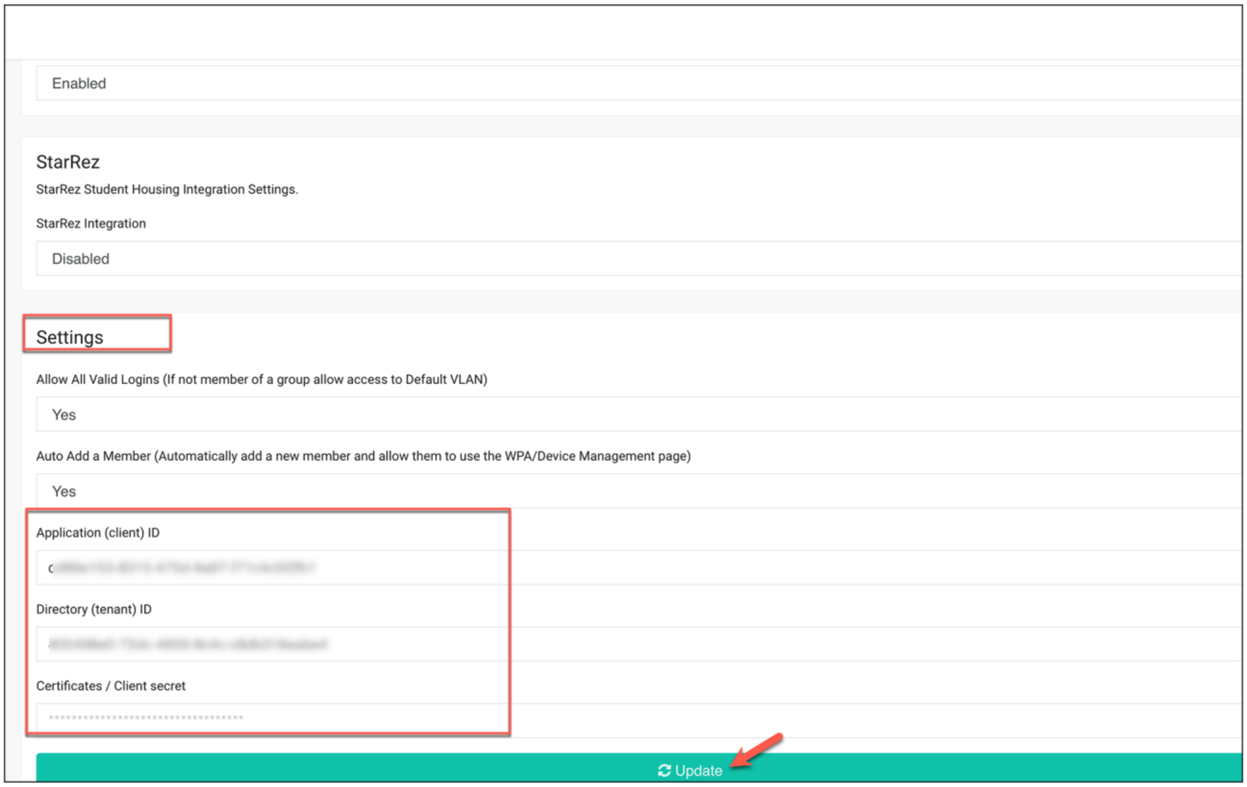
Switch Ports & Wired Vlans

Switch Port and Wired Vlan Device Management Options.

Switch Port Settings (Allows assignment of Switch Ports)

Step 2. Scroll to the bottom of the page and fill in the Azure tenant information or SAML metadata.

The administrator may need to add the Application ID, Tenant ID, and Client secret for Azure.



Enabled

StarRez

StarRez Student Housing Integration Settings.

StarRez Integration

Disabled

Settings

Allow All Valid Logins (If not member of a group allow access to Default VLAN)

Yes

Auto Add a Member (Automatically add a new member and allow them to use the WPA/Device Management page)

Yes

Application (client) ID

[redacted]

Directory (tenant) ID

[redacted]

Certificates / Client secret

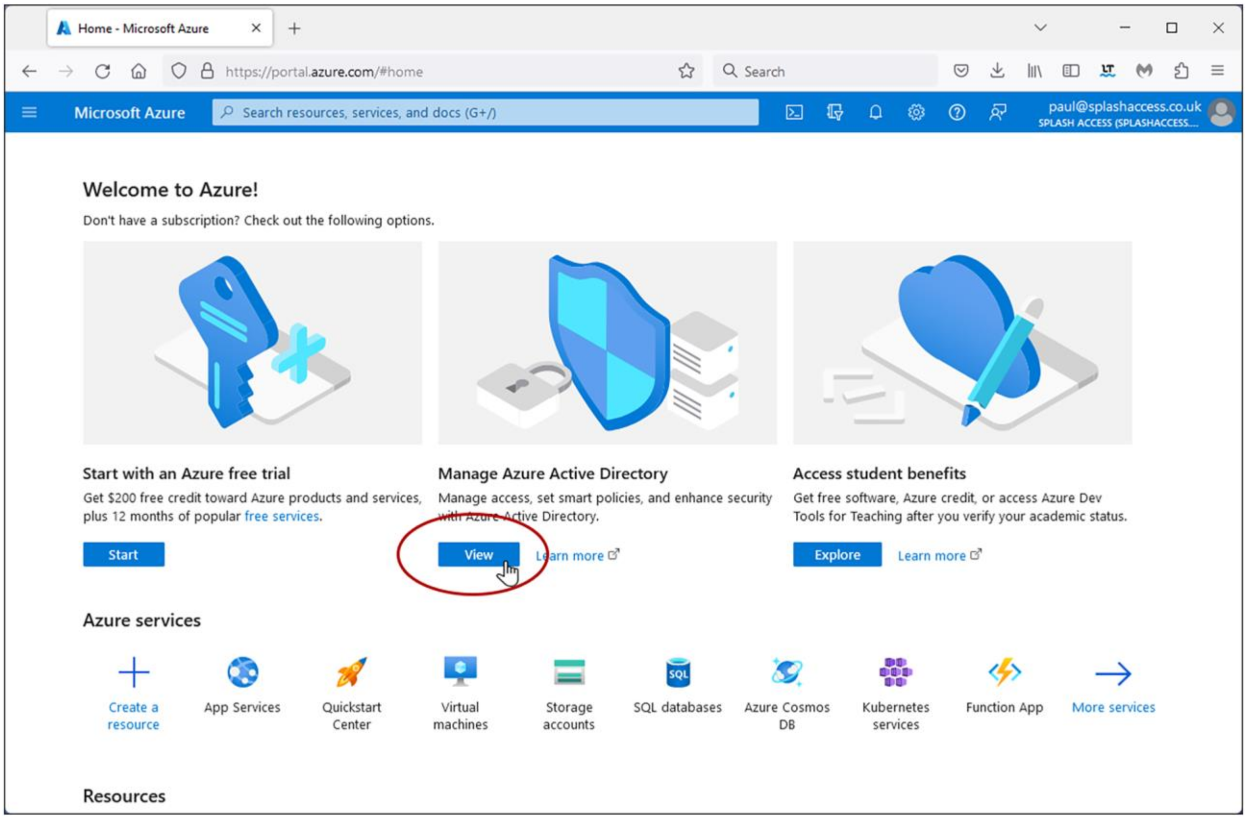
••••••••••••••••••••••••••••••••••••

Splash Access Azure setup

To set up Azure AD with Splash Access, follow the instructions below:

If you wish to use Microsoft 365, you will need to select or create an app under https://portal.azure.com. The system will then redirect users to log in using their Microsoft 365 information.

1. Access the Microsoft Azure portal: https://portal.azure.com
2. Navigate to Manage Azure Active Directory and click View.



Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

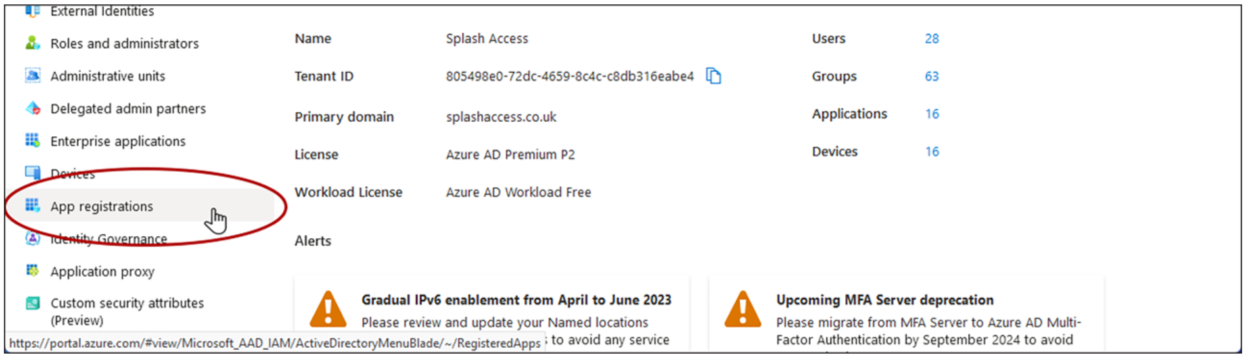
Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

Azure services

Resources

3. Click **App registrations** in the left column.



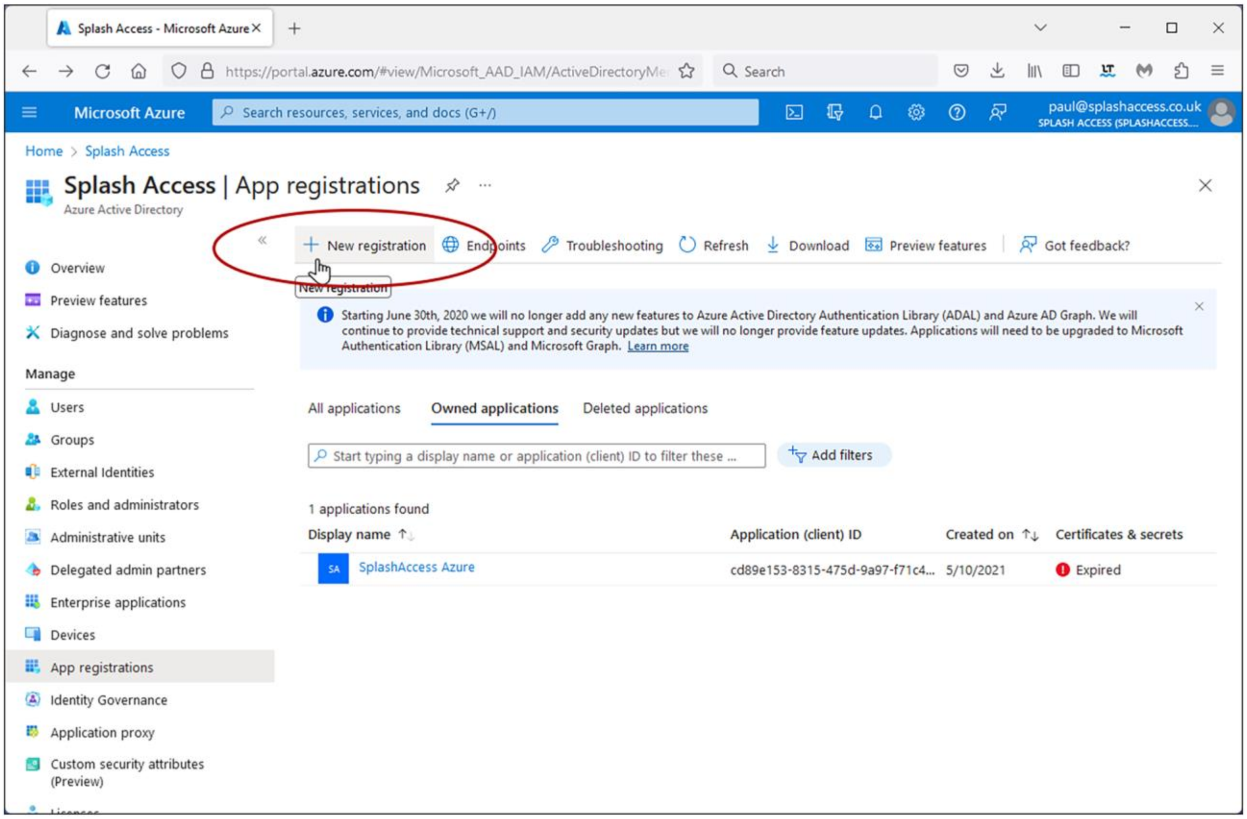
Name	Splash Access	Users	28
Tenant ID	805498e0-72dc-4659-8c4c-c8db316eabe4	Groups	63
Primary domain	splashaccess.co.uk	Applications	16
License	Azure AD Premium P2	Devices	16
Workload License	Azure AD Workload Free		

Alerts

Gradual IPv6 enablement from April to June 2023
Please review and update your Named locations ... to avoid any service

Upcoming MFA Server deprecation
Please migrate from MFA Server to Azure AD Multi-Factor Authentication by September 2024 to avoid

4. Click on the app name, for example, Splash Access, or create a web app or API type application and register it.

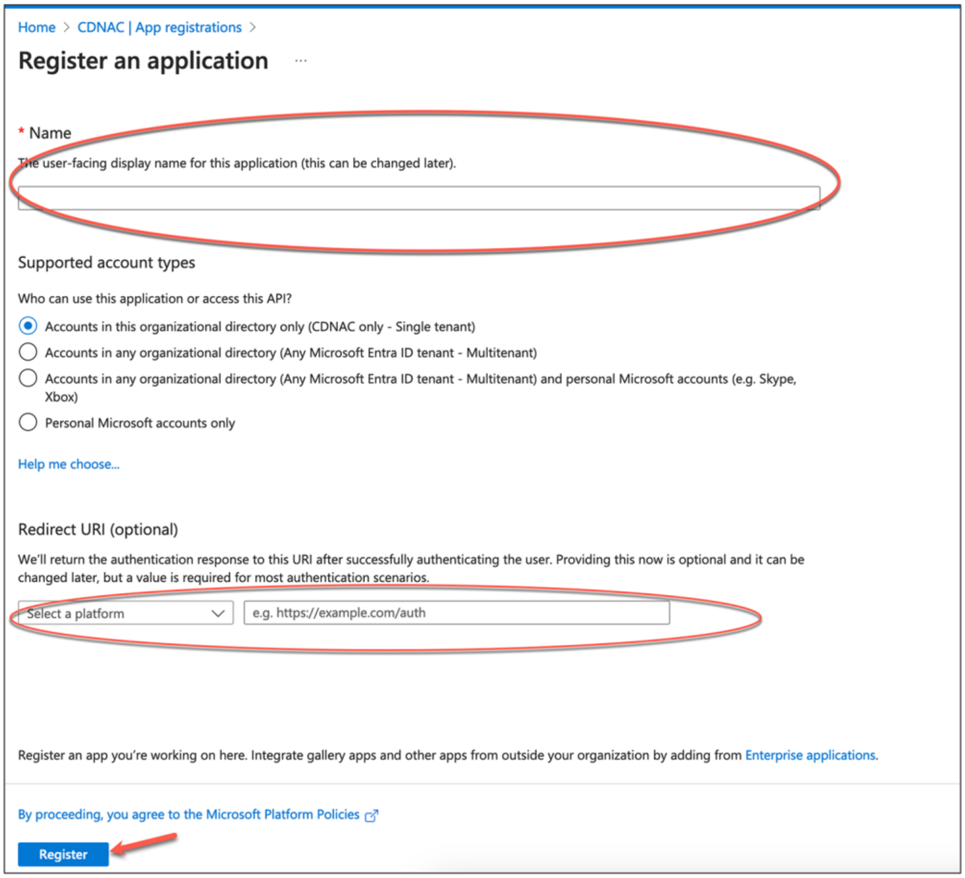


Splash Access | App registrations

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

1 applications found

Display name ↑↓	Application (client) ID	Created on ↑↓	Certificates & secrets
SA SplashAccess Azure	cd89e153-8315-475d-9a97-f71c4...	5/10/2021	Expired



Register an application

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (CDNAC only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

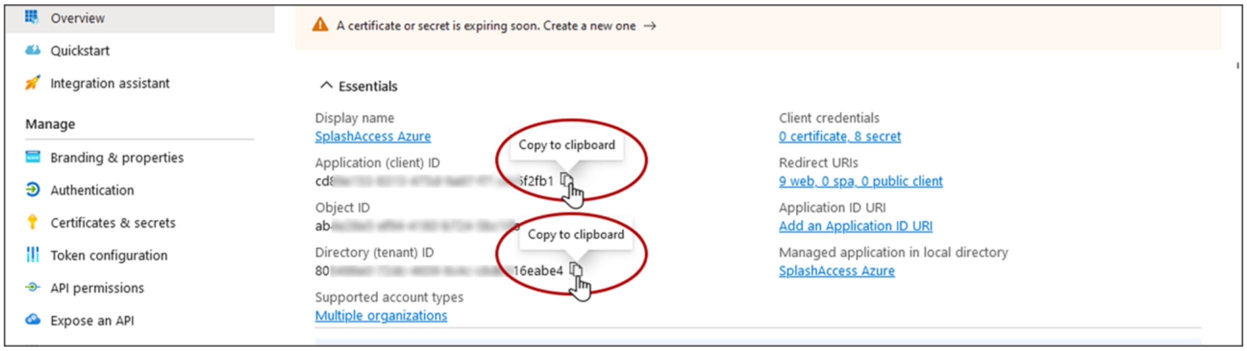
Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

5. Copy the application (client) ID and directory (tenant) ID found on this page by hovering over each and clicking to copy it to the clipboard. Paste them to your notes or paste directly into your Splash Access portal.



A certificate or secret is expiring soon. Create a new one →

Essentials

Display name: SplashAccess Azure

Application (client) ID: cd[redacted]5f2fb1 (Copy to clipboard)

Object ID: ab[redacted]

Directory (tenant) ID: 80[redacted]16eabe4 (Copy to clipboard)

Supported account types: Multiple organizations

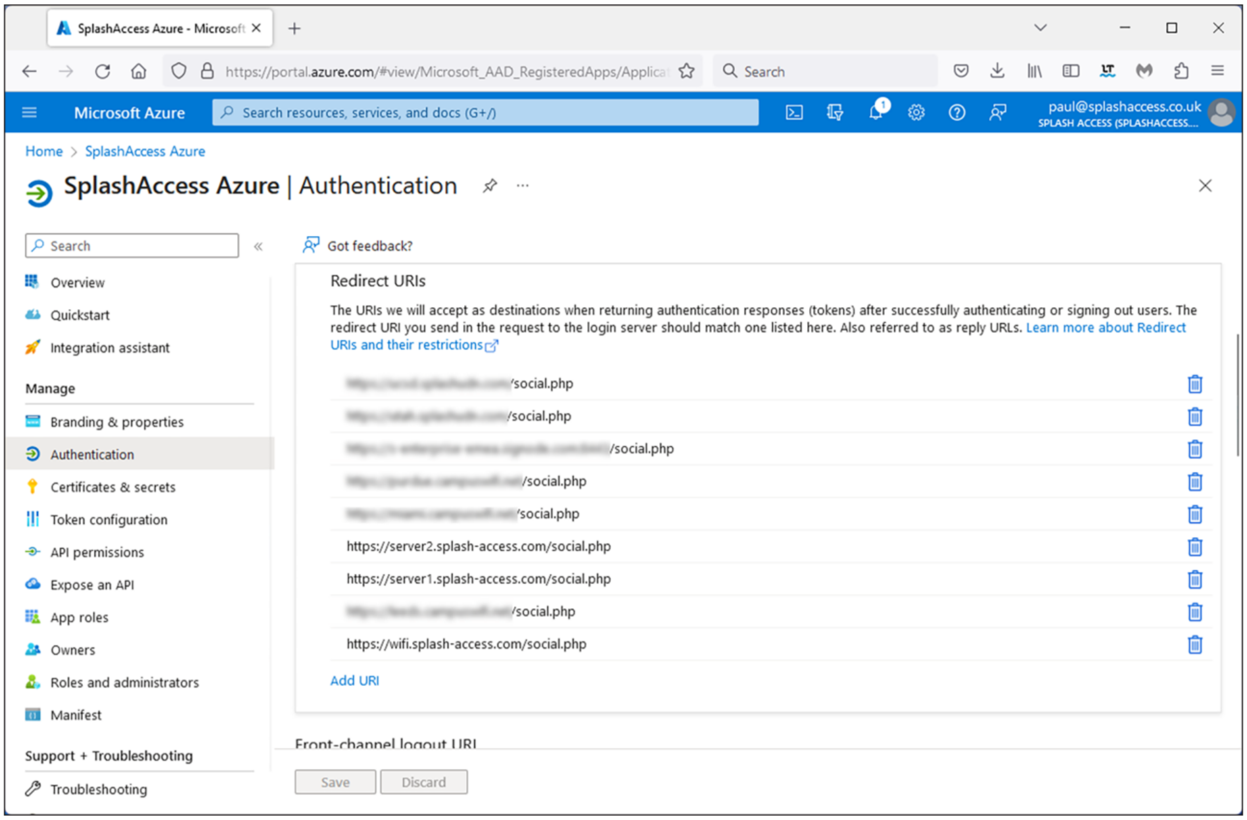
Client credentials: 0 certificate, 8 secret

Redirect URIs: 9 web, 0 spa, 0 public client

Application ID URI: Add an Application ID URI

Managed application in local directory: SplashAccess Azure

6. Navigate to **Authentication** > **Redirect URIs**.
Enter the following, replacing <YourSplashURL> with your account):
https://<YourSplashURL>/social.php



Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

[redacted]/social.php
[redacted]/social.php
[redacted]/social.php
[redacted]/social.php
[redacted]/social.php
https://server2.splash-access.com/social.php
https://server1.splash-access.com/social.php
[redacted]/social.php
https://wifi.splash-access.com/social.php

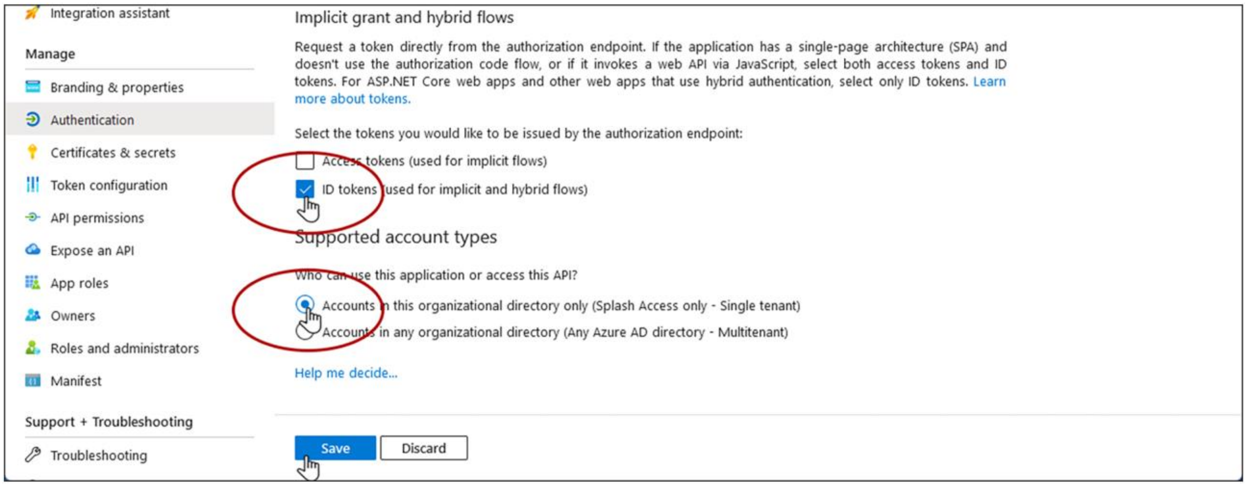
Add URI

Front-channel logout URL

7. Scroll down and enable the checkbox for **ID Tokens (used for implicit and hybrid flows)**.

8. Select **Accounts in this organizational directory only (Splash Access only – Single tenant)**.

9. Click **Save**.



Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.

Select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens (used for implicit flows)

☑ ID tokens (used for implicit and hybrid flows)

Supported account types

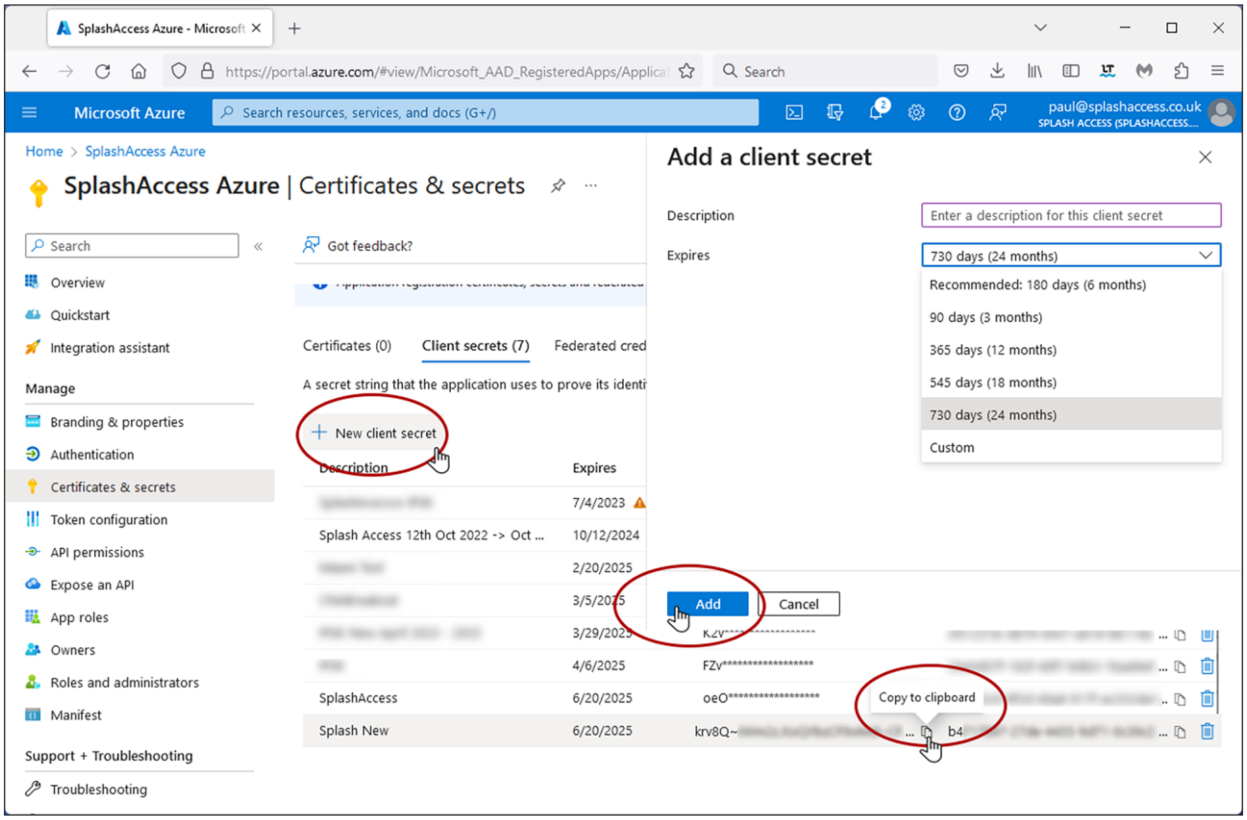
Who can use this application or access this API?

● Accounts in this organizational directory only (Splash Access only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Help me decide...

10. Navigate to **Certificates and secrets** in the menu.
    Generate a new client secret for Splash Access. Enter a name, such as Splash Access, and select the longest period for **Expires**. Make a note of this date, as you will need to update the secret before it expires.
    Click Add.
    Note: Keep this key in a safe place along with the above details.



SplashAccess Azure | Certificates & secrets

A secret string that the application uses to prove its identi

Description	Expires	
[redacted]	7/4/2023 ⚠	
Splash Access 12th Oct 2022 -> Oct ...	10/12/2024	
[redacted]	2/20/2025	
[redacted]	3/5/2025	
[redacted]	3/29/2025	K2v****************** [redacted] ...
[redacted]	4/6/2025	FZv****************** [redacted] ...
SplashAccess	6/20/2025	oeO****************** [redacted] ...
Splash New	6/20/2025	krv8Q~ [redacted] ... b4 [redacted] ...

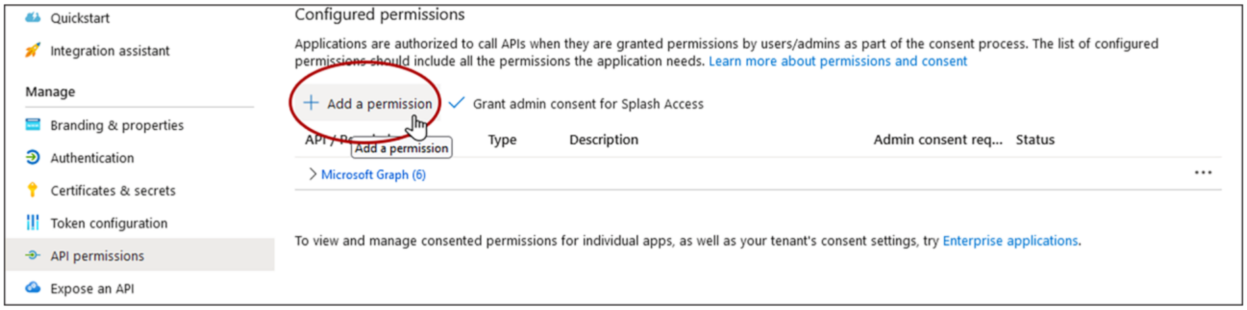
Add a client secret

Description: Enter a description for this client secret

Expires: 730 days (24 months)

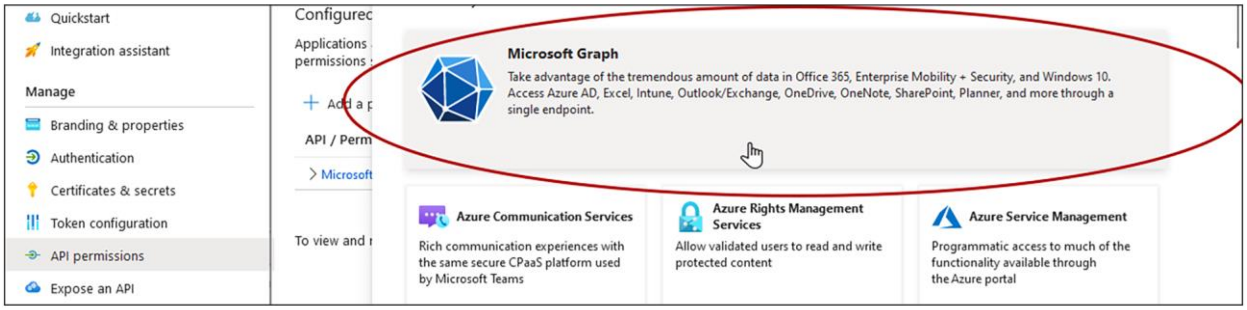
11. Copy the VALUE field into Notepad or other notes or directly into your Splash Access Azure Secret key field.

12. Navigate to **API Permissions** in the menu, click **Add a permission**, and select **Microsoft Graph – Delegated permissions**.
    Click **Grant admin consent for Splash Access**.



Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

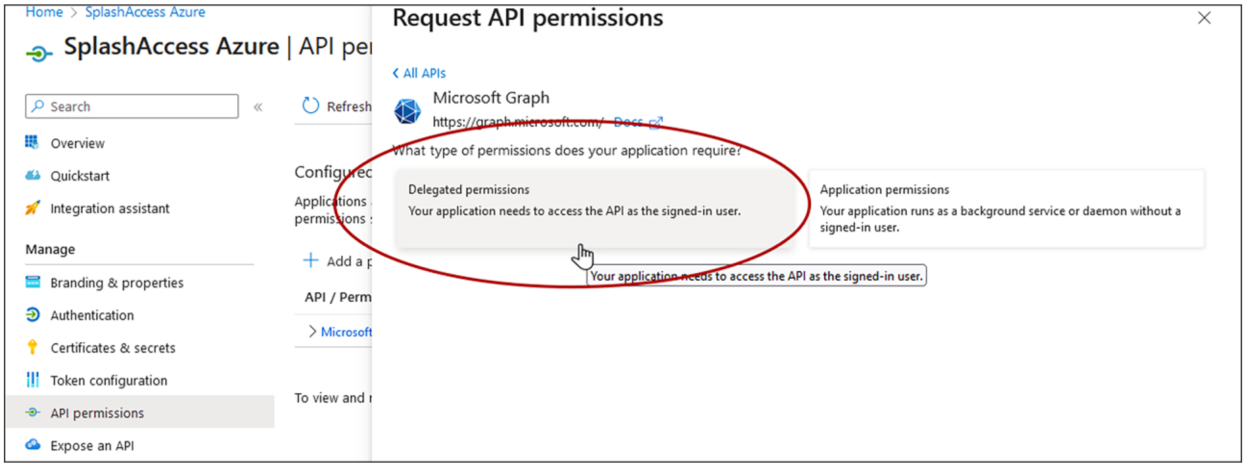


Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Allow validated users to read and write protected content

Programmatic access to much of the functionality available through the Azure portal

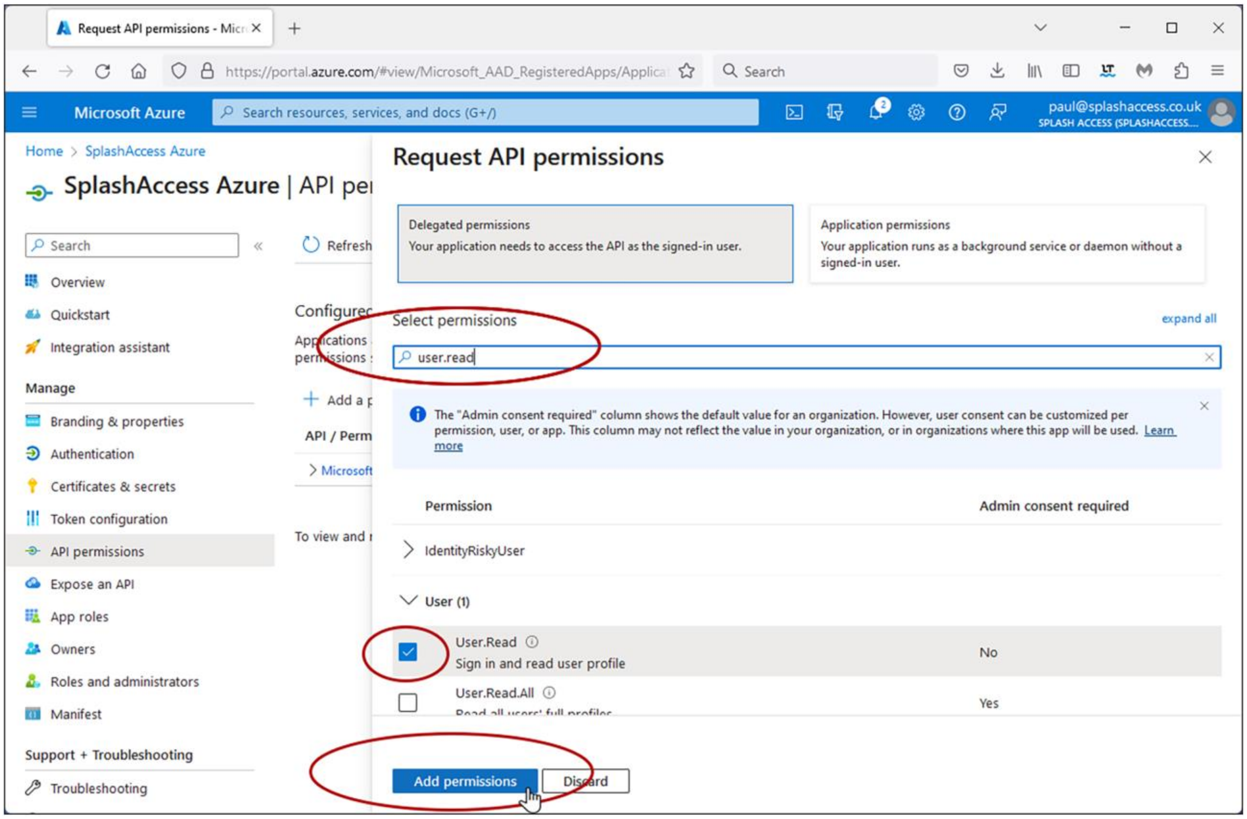


What type of permissions does your application require?

Your application needs to access the API as the signed-in user.

Your application runs as a background service or daemon without a signed-in user.

13. Search for and select the following permissions in the **Select permissions** search bar: Contacts.Read, Directory.Read.All, email, openid, profile, and User.Read. Click **Add permissions**.



Request API permissions

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

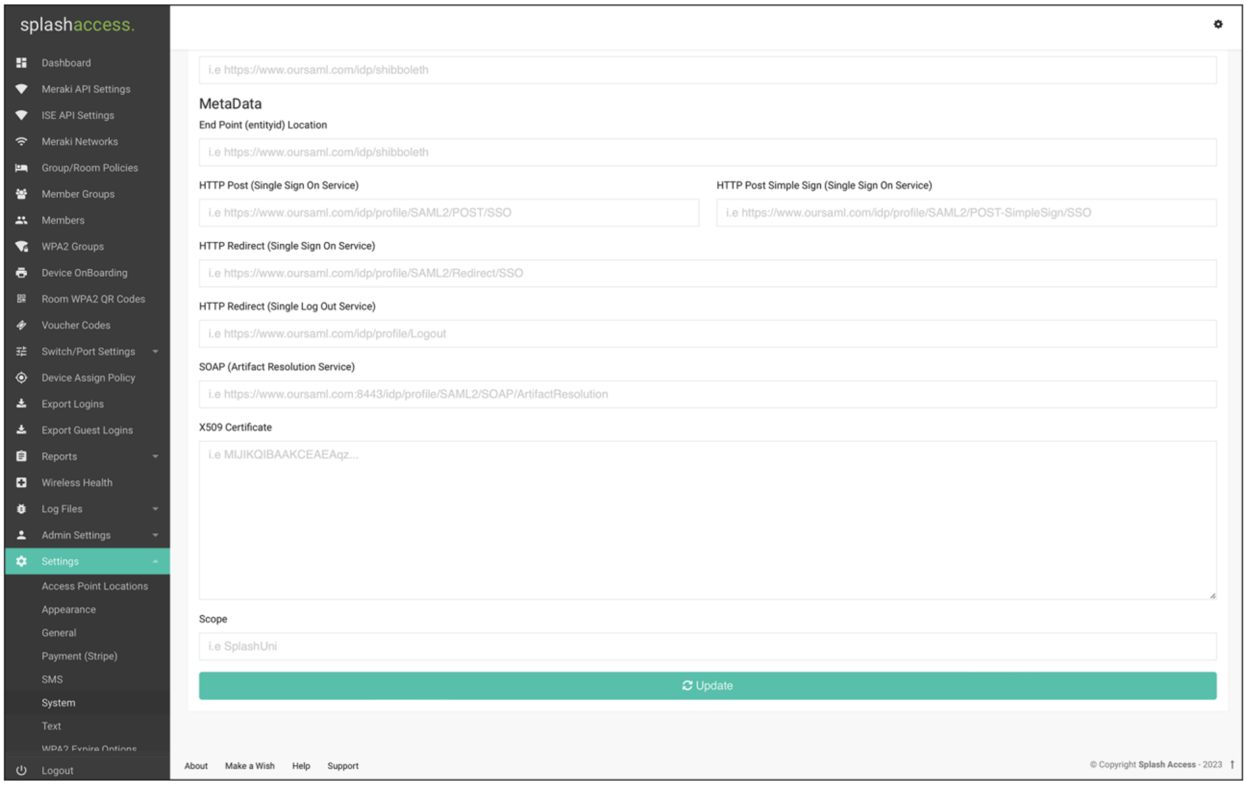
expand all

user.read

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Permission	Admin consent required
> IdentityRiskyUser	
∨ User (1)	
☑ User.Read Sign in and read user profile	No
□ User.Read.All Read all users' full profiles	Yes

Similarly, for SAML-based authentication, use the MetaData URL for additional configuration from the URL strings.



i.e https://www.oursaml.com/idp/shibboleth

MetaData

End Point (entityid) Location

i.e https://www.oursaml.com/idp/shibboleth

HTTP Post (Single Sign On Service)

i.e https://www.oursaml.com/idp/profile/SAML2/POST/SSO

HTTP Post Simple Sign (Single Sign On Service)

i.e https://www.oursaml.com/idp/profile/SAML2/POST-SimpleSign/SSO

HTTP Redirect (Single Sign On Service)

i.e https://www.oursaml.com/idp/profile/SAML2/Redirect/SSO

HTTP Redirect (Single Log Out Service)

i.e https://www.oursaml.com/idp/profile/Logout

SOAP (Artifact Resolution Service)

i.e https://www.oursaml.com:8443/idp/profile/SAML2/SOAP/ArtifactResolution

X509 Certificate

i.e MIJIKQIBAAKCEAEAqz...

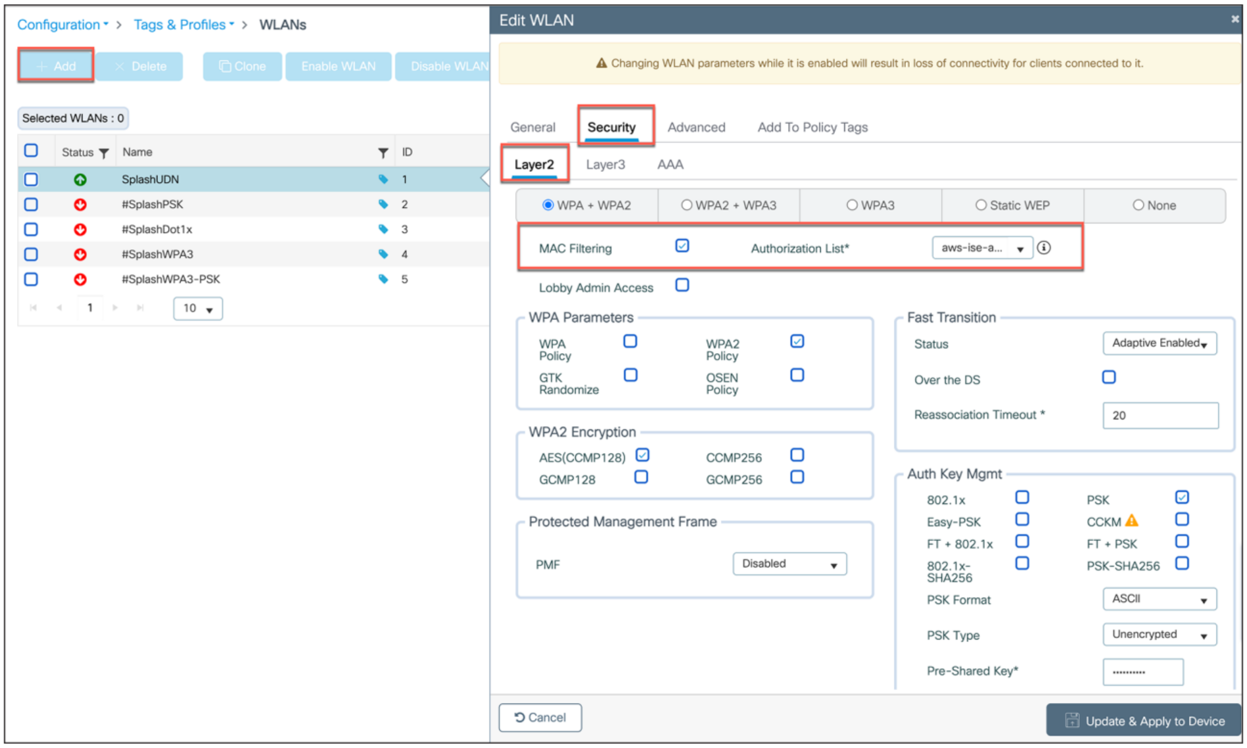
Scope

i.e SplashUni

Enable the User Defined Network Plus solution on the Catalyst 9800 Series

This process will enable the User Defined Network Plus solution configuration on the Catalyst 9800 wireless controller. User defined Network Plus is only supported in central mode deployments, that is, with the access point in Local mode.

Step 1. Log in to the Catalyst 9800 Series WLC.
Navigate to **Configuration > Tags & Profiles > WLANs.** Select the WLAN where users want to enable their UDN



Configuration ▾ > Tags & Profiles ▾ > WLANs

Selected WLANs : 0

□	Status	Name	ID
□	●	SplashUDN	1
□	●	#SplashPSK	2
□	●	#SplashDot1x	3
□	●	#SplashWPA3	4
□	●	#SplashWPA3-PSK	5

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

● WPA + WPA2 ○ WPA2 + WPA3 ○ WPA3 ○ Static WEP ○ None

MAC Filtering ☑ Authorization List* aws-ise-a...

Lobby Admin Access □

WPA Parameters
WPA Policy □ WPA2 Policy ☑
GTK Randomize □ OSEN Policy □

WPA2 Encryption
AES(CCMP128) ☑ CCMP256 □
GCMP128 □ GCMP256 □

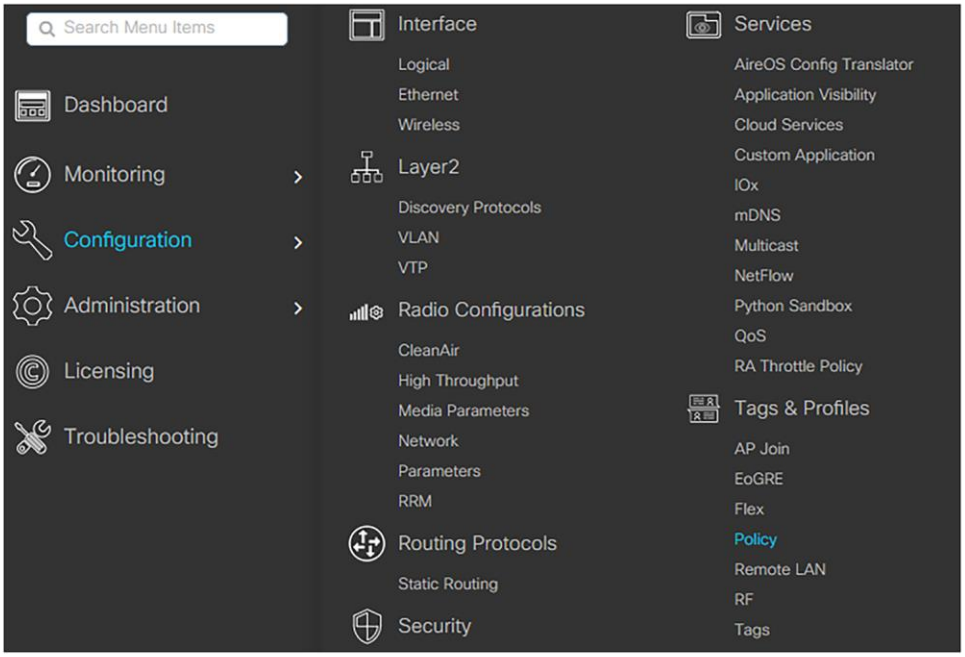
Protected Management Frame
PMF Disabled

Fast Transition
Status Adaptive Enabled
Over the DS □
Reassociation Timeout * 20

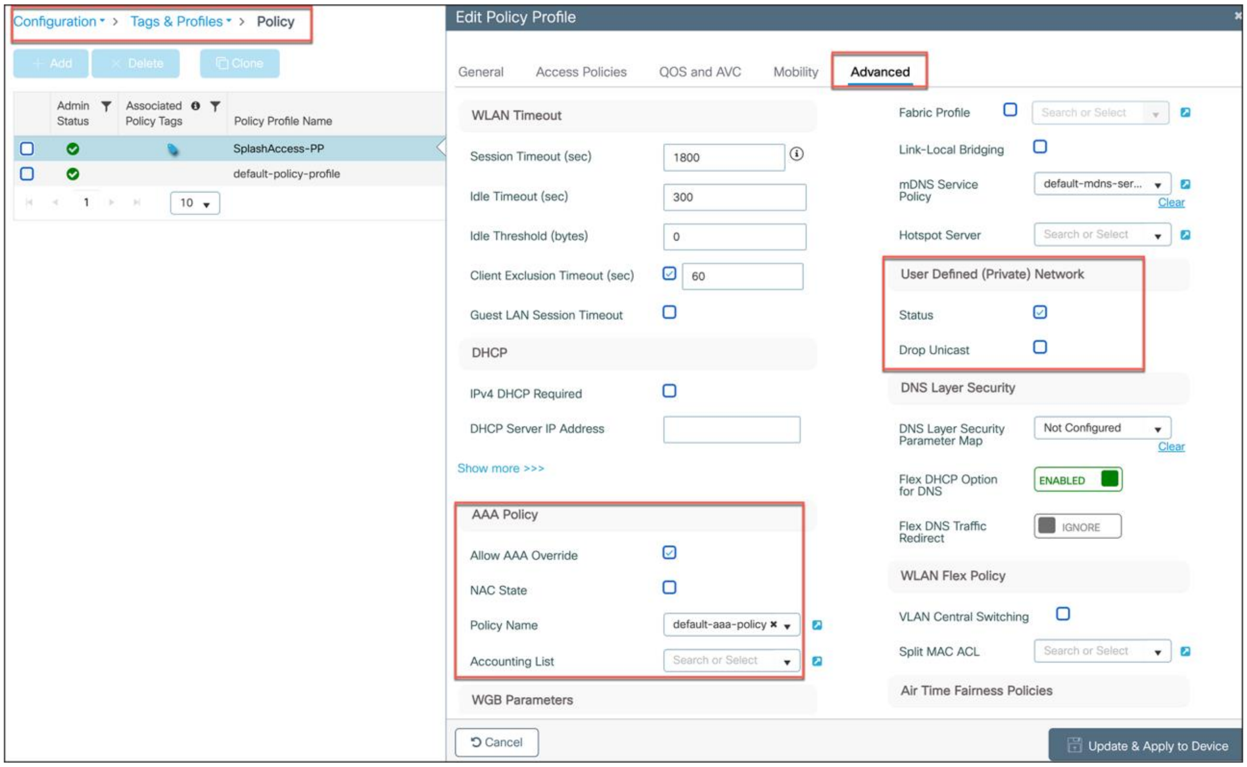
Auth Key Mgmt
802.1x □ PSK ☑
Easy-PSK □ CCKM ⚠ □
FT + 802.1x □ FT + PSK □
802.1x-SHA256 □ PSK-SHA256 □
PSK Format ASCII
PSK Type Unencrypted
Pre-Shared Key* ....

or create a new one by clicking **Add**. Then go to **Security > Layer2**. For PSK/iPSK/ Webauth/Open, make sure to select **MAC Filtering** and **Authorization List** for the ISE that is used for UDN, and click **Update and Apply to Device**. For 802.1X, MAC filtering is not required.

Step 2. Navigate to **Configuration > Tags and Profiles > Policy**. Click the policy profile that you want to configure and enable User Defined Network Plus on and that needs to be tied to the WLAN for use.



Step 3. Under the **Advanced** tab, ensure that the **User Defined (Private) Network Status** box is checked and, optionally, that **Drop Unicast** is selected. Also, ensure that in AAA Policy, **Allow AAA Override** is selected and the Policy Name is set to **default-aaa-policy**. Finally, confirm that **Accounting List** is set to **default**.



Admin Status	Associated Policy Tags	Policy Profile Name
✓	●	SplashAccess-PP
✓		default-policy-profile

WLAN Timeout

Session Timeout (sec): 1800

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 60

Guest LAN Session Timeout: □

DHCP

IPv4 DHCP Required: □

DHCP Server IP Address:

AAA Policy

Allow AAA Override: ☑

NAC State: □

Policy Name: default-aaa-policy

Accounting List: Search or Select

WGB Parameters

Fabric Profile: □ Search or Select

Link-Local Bridging: □

mDNS Service Policy: default-mdns-ser... Clear

Hotspot Server: Search or Select

User Defined (Private) Network

Status: ☑

Drop Unicast: □

DNS Layer Security

DNS Layer Security Parameter Map: Not Configured Clear

Flex DHCP Option for DNS: ENABLED

Flex DNS Traffic Redirect: IGNORE

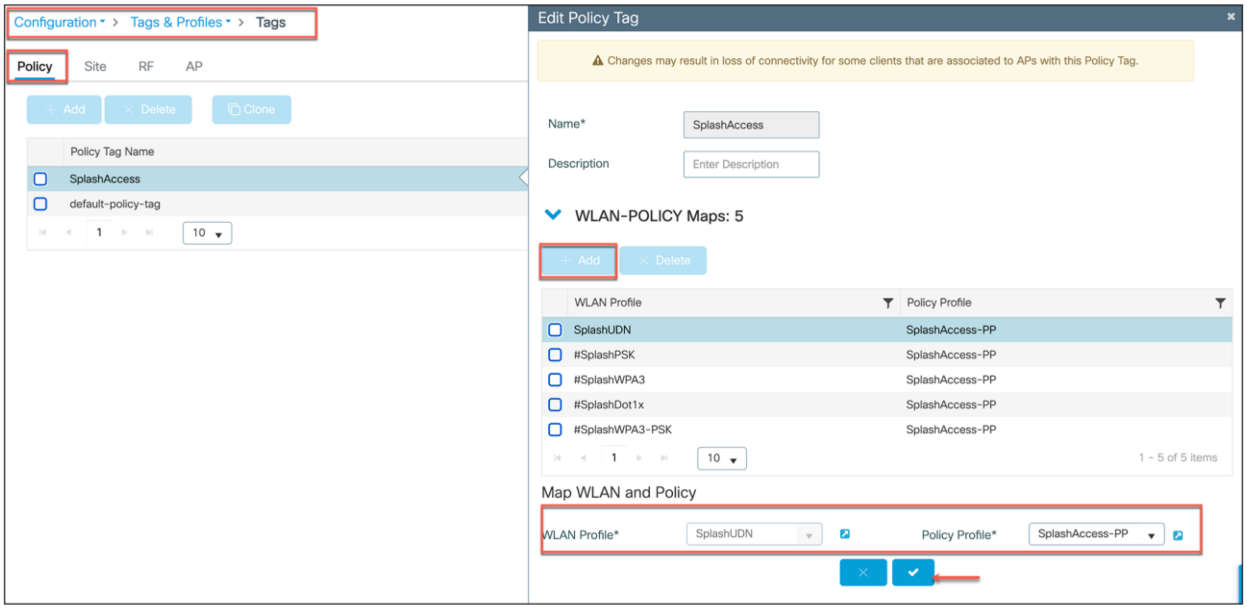
WLAN Flex Policy

VLAN Central Switching: □

Split MAC ACL: Search or Select

Air Time Fairness Policies

Step 4. Now confirm that the WLAN and policy profile are part of the policy tag where UDN-enabled SSIDs are to be broadcasted. To do this, go to **Configuration > Tags & Profiles > Tags**.



Policy Tag Name
SplashAccess
default-policy-tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name* SplashAccess

Description Enter Description

WLAN-POLICY Maps: 5

WLAN Profile	Policy Profile
SplashUDN	SplashAccess-PP
#SplashPSK	SplashAccess-PP
#SplashWPA3	SplashAccess-PP
#SplashDot1x	SplashAccess-PP
#SplashWPA3-PSK	SplashAccess-PP

1 - 5 of 5 items

Map WLAN and Policy

WLAN Profile* SplashUDN   Policy Profile* SplashAccess-PP

Process: Configuring an RLAN on the WLC (optional step)

This section is optional and is required only if the customer wants to enable and configure the User Defined Network Plus solution on an RLAN.

A few things to note:

- RLAN workflow is supported in Cisco Catalyst Center Release 2.2.3.
- ISE will not be configured with an RLAN name.

When can we configure an RLAN on the WLC for User Defined Network Plus?

- An RLAN can be configured on the WLC after the access point is provisioned with SSIDs and UDNs.

How do I do this?

Step 1. Configure the RLAN profile and RLAN policy:

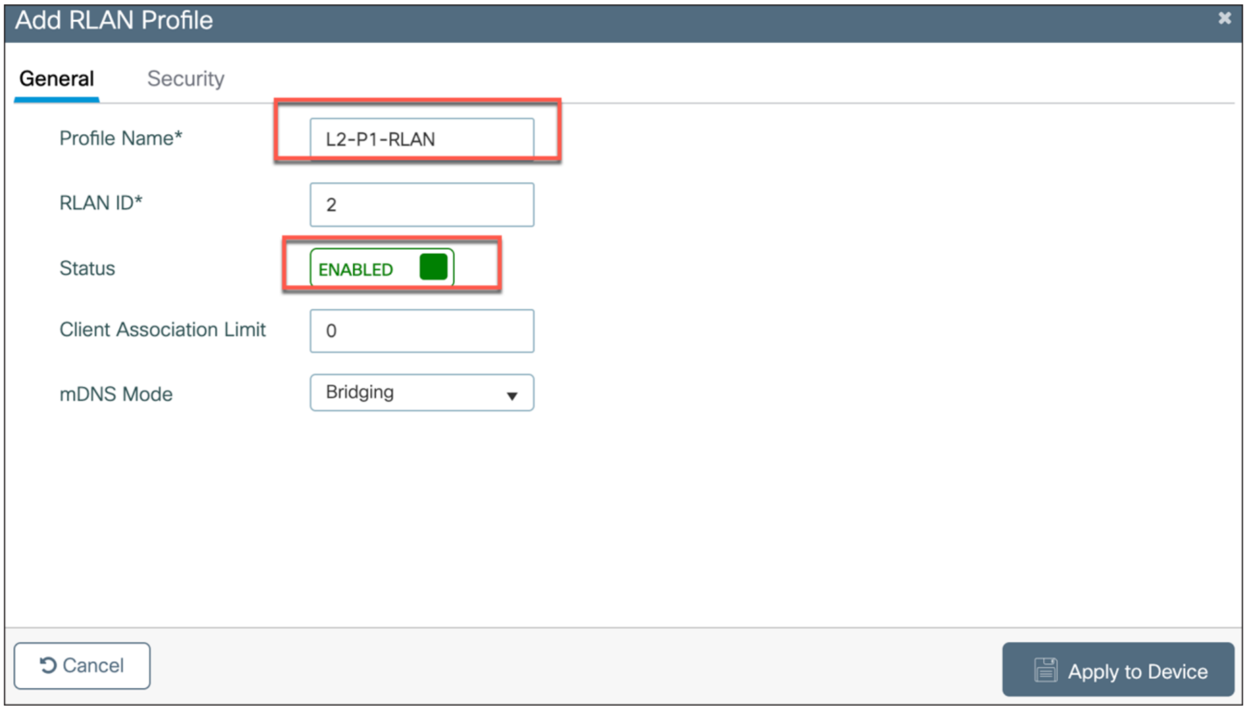
1. Log in to the WLC via the GUI.
2. Navigate to **Configuration > Tags and Profiles > Remote LAN**.
3. On the **RLAN Profile** tab, click **+ ADD** to create a new RLAN profile.

Create the profiles based on the following configuration. Leave the defaults not mentioned as is.

Tab	Setting	Value
General tab		
	Profile Name	Configure name any intuitive to the user
	Status	Enabled
Security tab > Layer 2		
	802.1X (optional)	Enable if you want to enable 802.1X on wired clients

Tab	Setting	Value
	Mac Filtering (mandatory if 802.1X is not enabled)	Choose from the configured authorization list
	Authentication List (required if 802.1X is enabled)	Choose the configured authentication list

Click **Apply to Device**.



Add RLAN Profile

General | Security

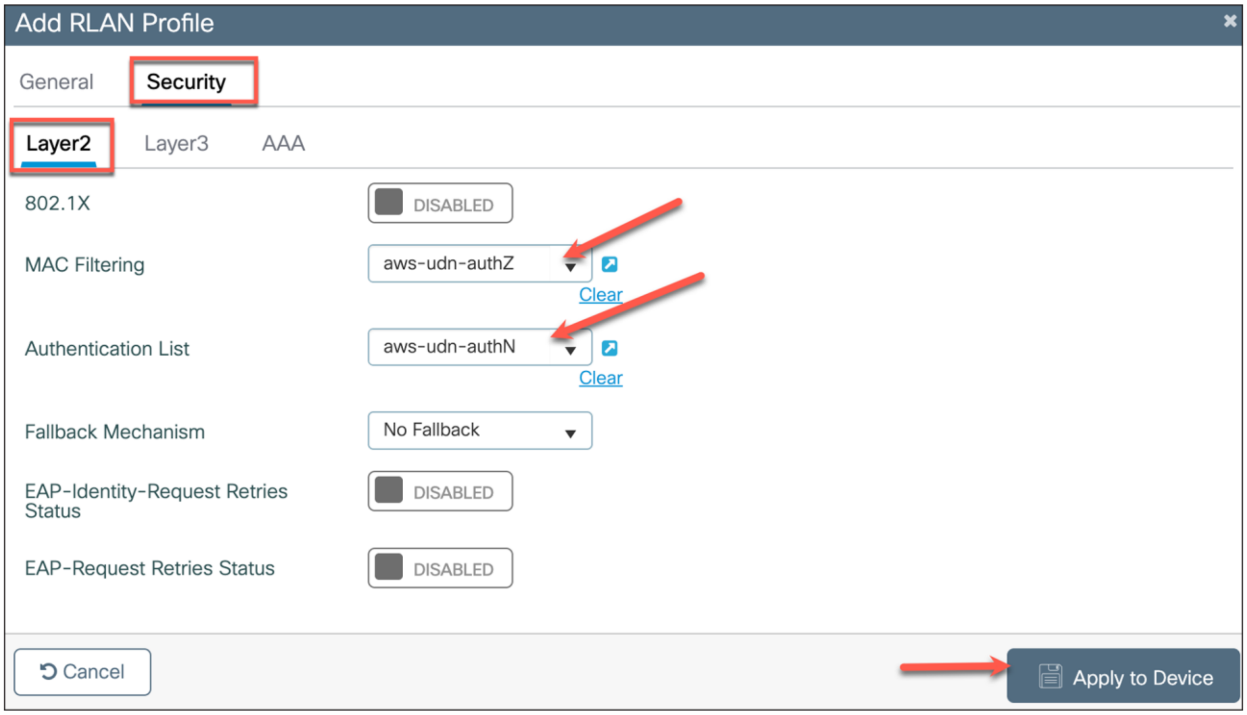
Profile Name*: L2-P1-RLAN

RLAN ID*: 2

Status: ENABLED

Client Association Limit: 0

mDNS Mode: Bridging



Add RLAN Profile

General | Security

Layer2 | Layer3 | AAA

802.1X: DISABLED

MAC Filtering: aws-udn-authZ

Authentication List: aws-udn-authN

Fallback Mechanism: No Fallback

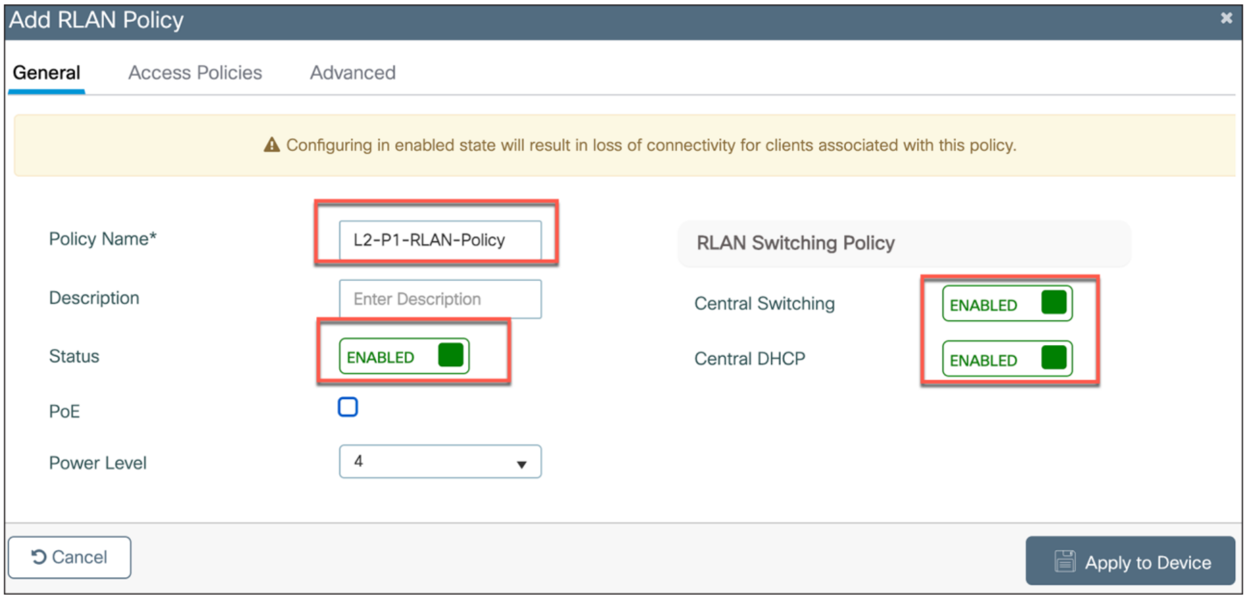
EAP-Identity-Request Retries Status: DISABLED

EAP-Request Retries Status: DISABLED

1. On the **RLAN Policy** tab, click **+ ADD** to create a new RLAN policy.
   Create the policy based on the following configuration. Leave the defaults not mentioned as is.

Tab	Setting	Value
General tab		
	Policy Name	Configure policy name
	Status	Enabled
	Central Switching	Enabled
	Central DHCP	Enabled
Access Policies tab		
	VLAN	<VLAN ID> or name
	Host Mode	Singlehost: One device per port Multihost: Multiple devices per port (hub)
Advanced tab		
	User Defined (Private) Network Status	**Enable** to enable UDN
	Drop Unicast (optional)	Enable to enable UDN unicast
	AAA Override	Enable
	Accounting List	Set if required

Click **Apply to Device**.



⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this policy.

Policy Name* L2-P1-RLAN-Policy

Description Enter Description

Status ENABLED

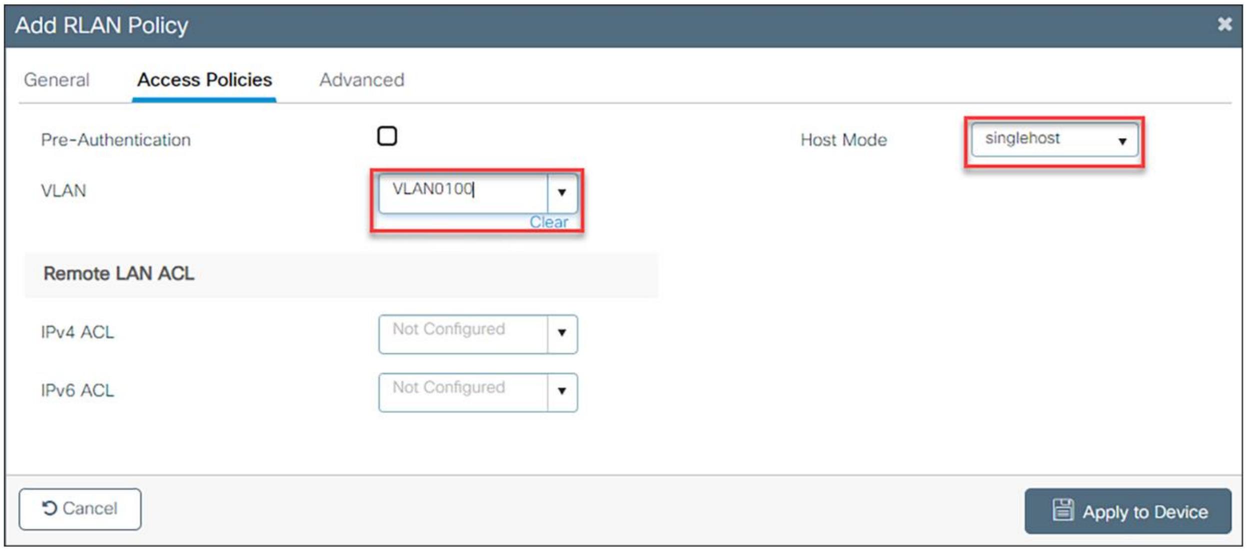
PoE □

Power Level 4

RLAN Switching Policy

Central Switching ENABLED

Central DHCP ENABLED



Add RLAN Policy

Pre-Authentication ☐

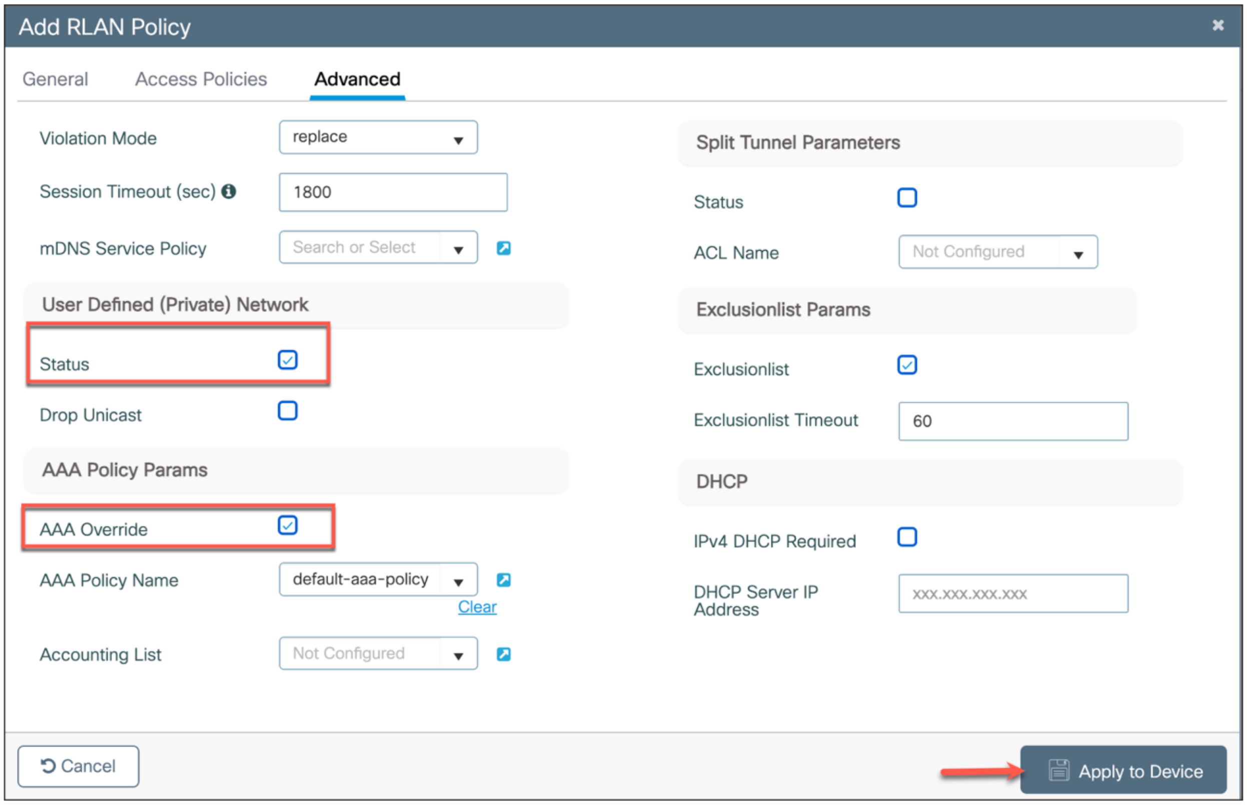
VLAN: VLAN0100

Host Mode: singlehost

Remote LAN ACL

IPv4 ACL: Not Configured

IPv6 ACL: Not Configured



Add RLAN Policy

Violation Mode: replace

Session Timeout (sec): 1800

mDNS Service Policy: Search or Select

User Defined (Private) Network

Status ☑

Drop Unicast ☐

AAA Policy Params

AAA Override ☑

AAA Policy Name: default-aaa-policy

Accounting List: Not Configured

Split Tunnel Parameters

Status ☐

ACL Name: Not Configured

Exclusionlist Params

Exclusionlist ☑

Exclusionlist Timeout: 60

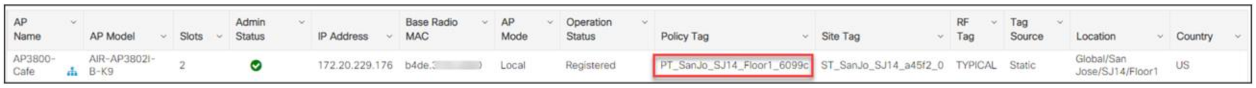
DHCP

IPv4 DHCP Required ☐

DHCP Server IP Address: xxx.xxx.xxx.xxx

Step 2. Apply the RLAN to the policy profile.

1. Navigate to **Configuration > Wireless > Access Points**.
   Note the policy profile assigned to the access point.



AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Policy Tag	Site Tag	RF Tag	Tag Source	Location	Country
AP3800-Cafe	AIR-AP3802I-B-K9	2	✓	172.20.229.176	b4de.[redacted]	Local	Registered	PT_SanJo_SJ14_Floor1_6099c	ST_SanJo_SJ14_a45f2_0	TYPICAL	Static	Global/San Jose/SJ14/Floor1	US

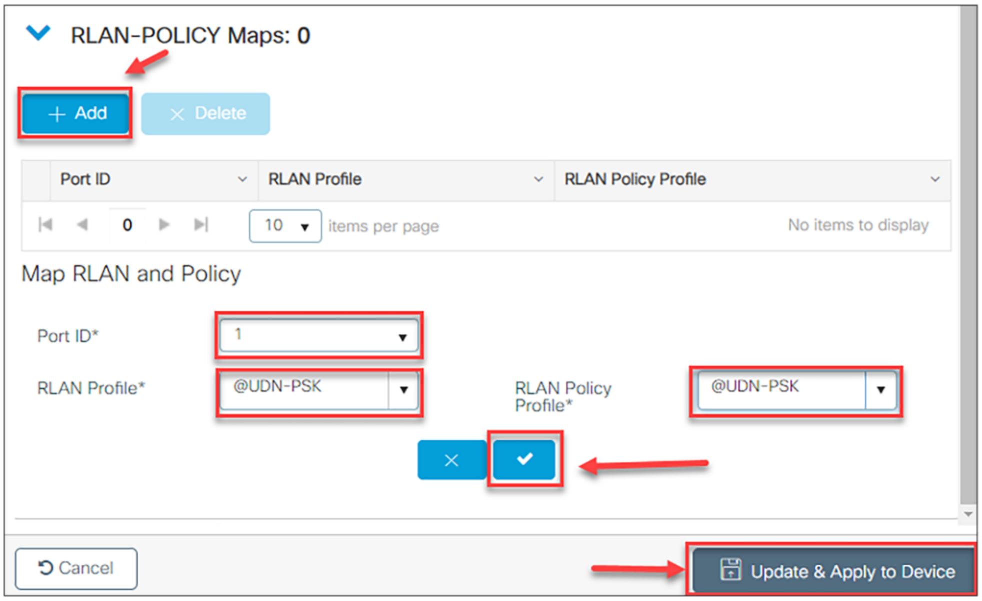
2. Navigate to **Configuration > Tags and Profiles > Tags**, then click on the policy tag assigned to the access point.

3. Under **RLAN-POLICY Maps**, click **+ Add** to add a new policy map and configure it with the required port.

Port ID	**Port number to enable**
RLAN Profile	RLAN Profile created in the previous step
RLAN Policy Profile	RLAN Policy created in the previous step

Click ✓ to add the port configuration.

4. Repeat step 3 if you need to add multiple ports.
5. Click **Update and Apply to Device** to update the RLAN configuration.



RLAN-POLICY Maps: 0

Port ID	RLAN Profile	RLAN Policy Profile

0 · 10 items per page · No items to display

Map RLAN and Policy

Port ID*: 1

RLAN Profile*: @UDN-PSK

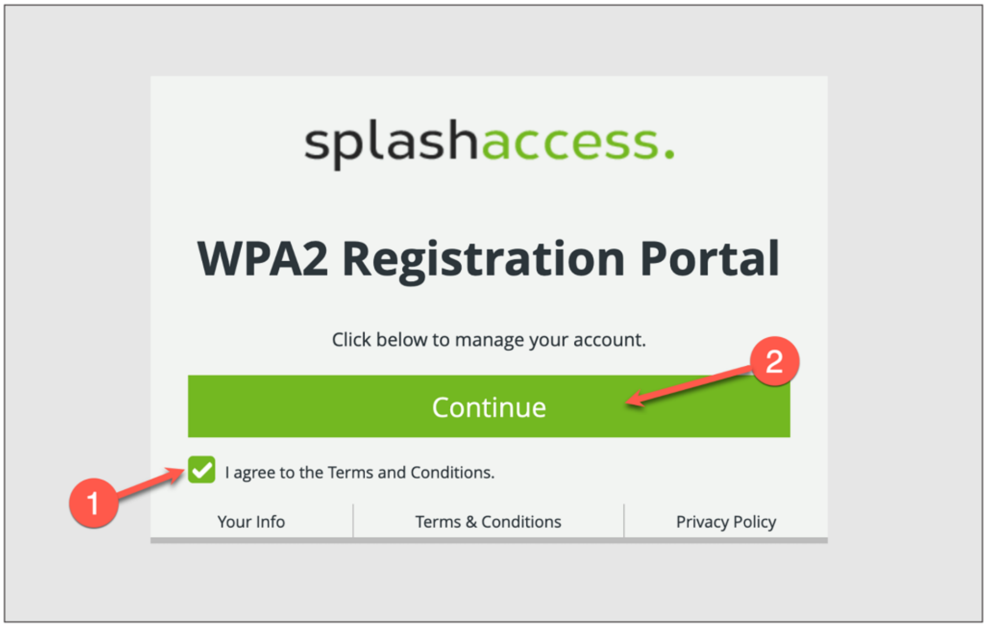
RLAN Policy Profile*: @UDN-PSK

End user device registration with the Splash Access portal

The Splash Access user device registration link/portal is provided to the end user as part of the Splash Access subscription. It mimics the following URL: https://<customer-account>splashudn.com/accounts/<customer-account>/device/

When an end user clicks the link, they will be presented with a web page requiring them to enter their credentials, which can be defined as part of AD.

From the user device portal, read the terms and conditions and accept by checking the **I agree to the Terms and Conditions** box, then click **Continue**.



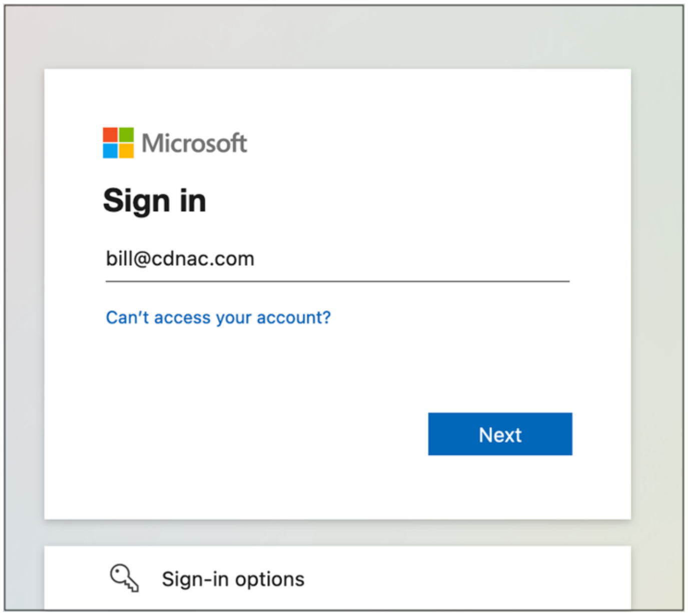
splashaccess.

WPA2 Registration Portal

Click below to manage your account.

☑ I agree to the Terms and Conditions.

The user will be sent to their AD credentials page, where they can enter their provided username and password.



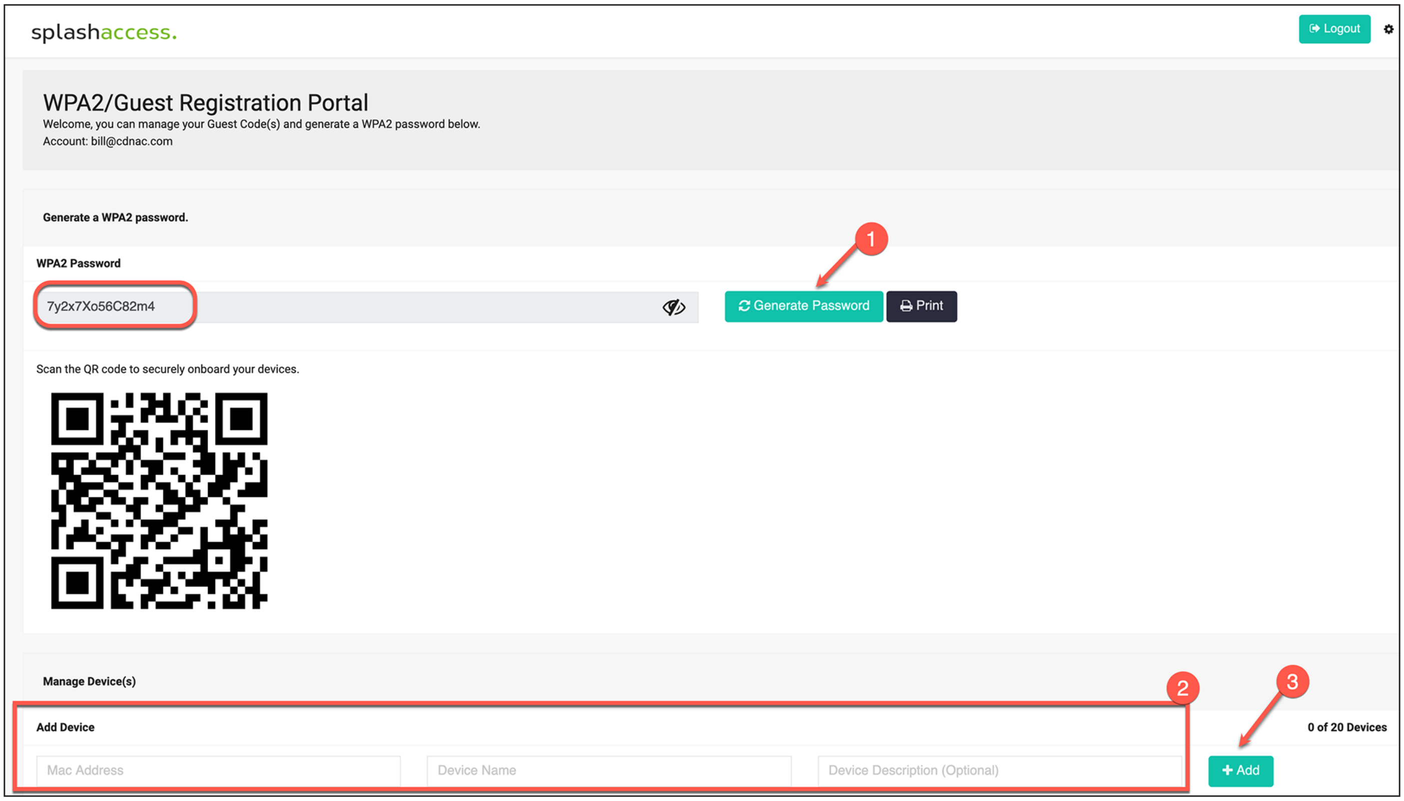
Microsoft

Sign in

bill@cdnac.com

Once an end user is logged in, the Splash Access device registration portal will be displayed.

1. To add the devices, first generate a WPA2 password (iPSK), which is mostly for IoT devices. If the QR code for the SSID was enabled from the Splash Access admin portal, that will also be displayed.
2. The end user can now add their devices by entering their MAC addresses.



WPA2/Guest Registration Portal

Welcome, you can manage your Guest Code(s) and generate a WPA2 password below.

Account: bill@cdnac.com

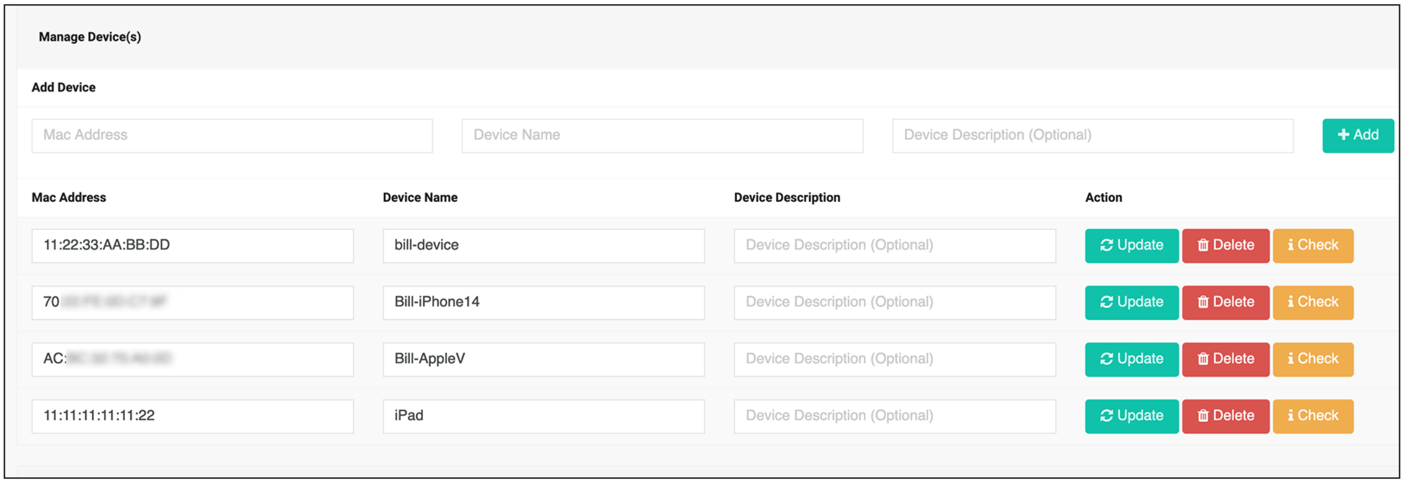
Generate a WPA2 password.

WPA2 Password: 7y2x7Xo56C82m4

Scan the QR code to securely onboard your devices.

Manage Device(s)

Add Device

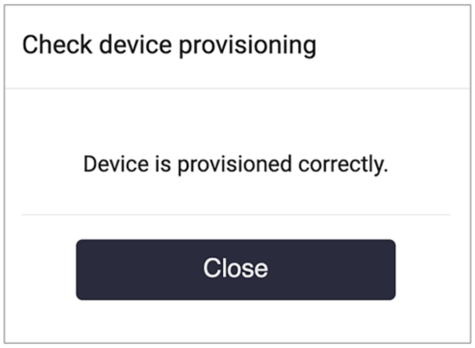


Manage Device(s)

Add Device

Mac Address	Device Name	Device Description	Action
11:22:33:AA:BB:DD	bill-device	Device Description (Optional)	Update Delete i Check
70[redacted]	Bill-iPhone14	Device Description (Optional)	Update Delete i Check
AC:[redacted]	Bill-AppleV	Device Description (Optional)	Update Delete i Check
11:11:11:11:11:22	iPad	Device Description (Optional)	Update Delete i Check

The user can check the device status by clicking the i **Check** button.



Check device provisioning

Device is provisioned correctly.

Now when the end user connects to the UDN-enabled SSID, their registered devices will be part of that user's network or "room," and only they can access and cast to their own devices.

Troubleshooting User Defined Network Plus

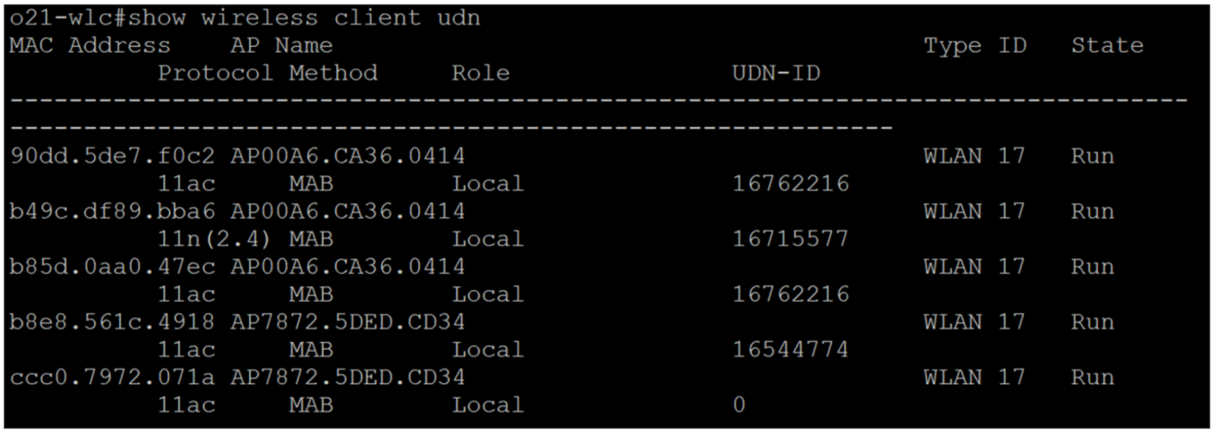
This section will go over commands that are useful when troubleshooting the User Defined Network Plus solution.

Catalyst 9800 Series wireless controller

These commands are run on the Catalyst 9800 controller.

show wireless client udn

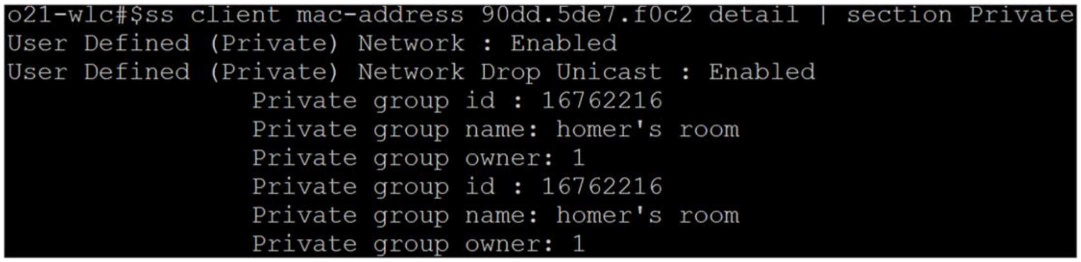
This command shows all the clients that are currently connected and the UDNs to which they are connected.



```
o21-wlc#show wireless client udn
MAC Address    AP Name                                        Type ID   State
          Protocol Method     Role               UDN-ID
--------------------------------------------------------------------------------
------------------------------------------------------------
90dd.5de7.f0c2 AP00A6.CA36.0414                               WLAN 17   Run
          11ac     MAB        Local              16762216
b49c.df89.bba6 AP00A6.CA36.0414                               WLAN 17   Run
          11n(2.4) MAB        Local              16715577
b85d.0aa0.47ec AP00A6.CA36.0414                               WLAN 17   Run
          11ac     MAB        Local              16762216
b8e8.561c.4918 AP7872.5DED.CD34                               WLAN 17   Run
          11ac     MAB        Local              16544774
ccc0.7972.071a AP7872.5DED.CD34                               WLAN 17   Run
          11ac     MAB        Local              0
```

show wireless client mac-address <mac address> detail | section Private

This command can be used to see details on a certain MAC address.



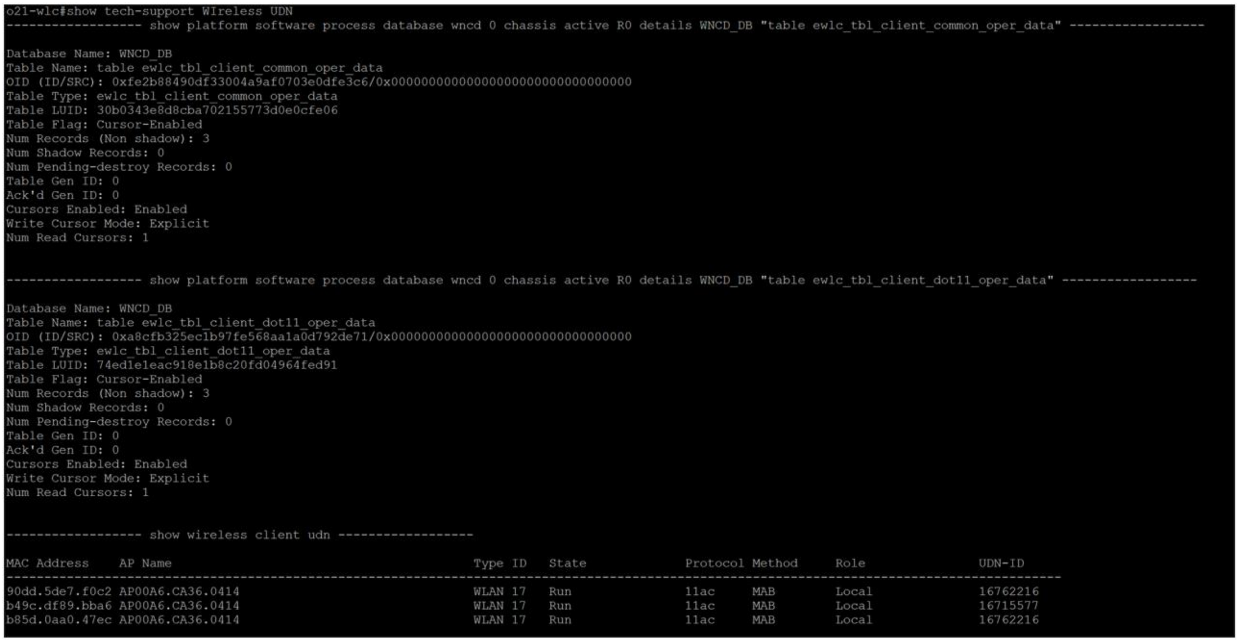
```
o21-wlc#$ss client mac-address 90dd.5de7.f0c2 detail | section Private
User Defined (Private) Network : Enabled
User Defined (Private) Network Drop Unicast : Enabled
                Private group id : 16762216
                Private group name: homer's room
                Private group owner: 1
                Private group id : 16762216
                Private group name: homer's room
                Private group owner: 1
```

show wireless profile policy detailed <profile-name> | include User

This command can be used to verify that the policy profile is pushed and UDN is enabled.

show tech-support wireless udn

This command shows a ton of information that is useful when troubleshooting.



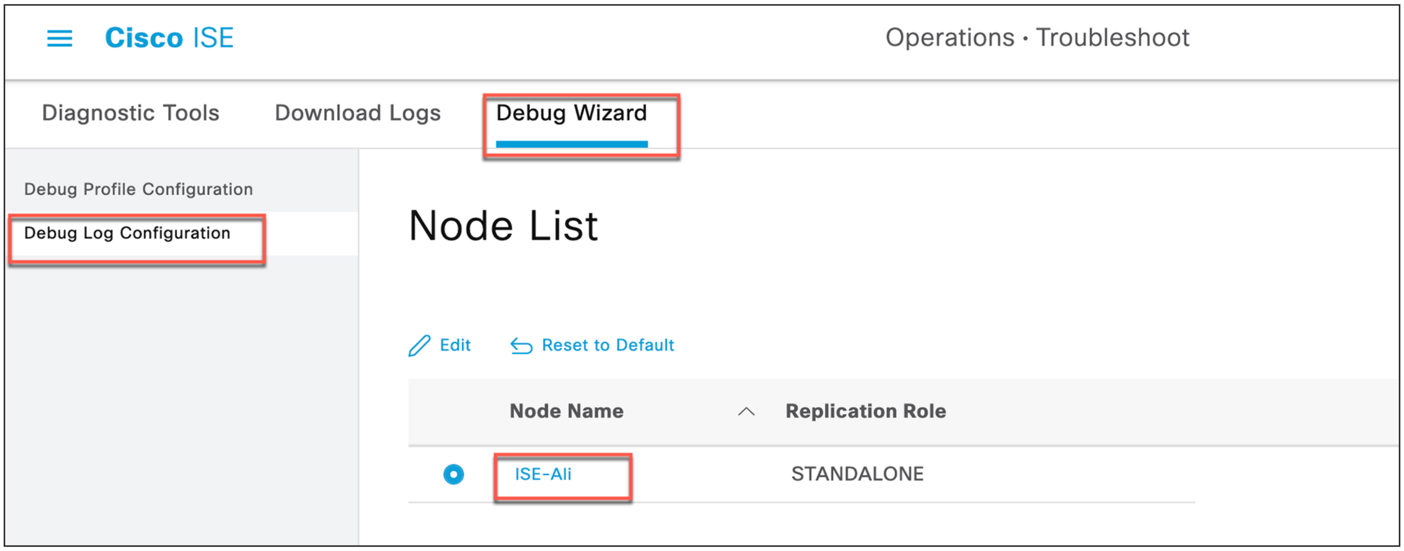
```
o21-wlc#show tech-support WIreless UDN
------------------ show platform software process database wncd 0 chassis active R0 details WNCD_DB "table ewlc_tbl_client_common_oper_data" ------------------

Database Name: WNCD_DB
Table Name: table ewlc_tbl_client_common_oper_data
OID (ID/SRC): 0xfe2b88490df33004a9af0703e0dfe3c6/0x00000000000000000000000000000000
Table Type: ewlc_tbl_client_common_oper_data
Table LUID: 30b0343e8d8cba702155773d0e0cfe06
Table Flag: Cursor-Enabled
Num Records (Non shadow): 3
Num Shadow Records: 0
Num Pending-destroy Records: 0
Table Gen ID: 0
Ack'd Gen ID: 0
Cursors Enabled: Enabled
Write Cursor Mode: Explicit
Num Read Cursors: 1


------------------ show platform software process database wncd 0 chassis active R0 details WNCD_DB "table ewlc_tbl_client_dot11_oper_data" ------------------

Database Name: WNCD_DB
Table Name: table ewlc_tbl_client_dot11_oper_data
OID (ID/SRC): 0xa8cfb325ec1b97fe568aa1a0d792de71/0x00000000000000000000000000000000
Table Type: ewlc_tbl_client_dot11_oper_data
Table LUID: 74ed1e1eac918e1b8c20fd04964fed91
Table Flag: Cursor-Enabled
Num Records (Non shadow): 3
Num Shadow Records: 0
Num Pending-destroy Records: 0
Table Gen ID: 0
Ack'd Gen ID: 0
Cursors Enabled: Enabled
Write Cursor Mode: Explicit
Num Read Cursors: 1


------------------ show wireless client udn ------------------

MAC Address    AP Name                                        Type ID   State             Protocol Method     Role               UDN-ID
--------------------------------------------------------------------------------------------------------------------------------------------
90dd.5de7.f0c2 AP00A6.CA36.0414                               WLAN 17   Run               11ac     MAB        Local              16762216
b49c.df89.bba6 AP00A6.CA36.0414                               WLAN 17   Run               11ac     MAB        Local              16715577
b85d.0aa0.47ec AP00A6.CA36.0414                               WLAN 17   Run               11ac     MAB        Local              16762216
```

Cisco Identity Services Engine (ISE)

This section will provide troubleshooting information for Cisco ISE.

Turning on User Defined Network Plus debug logs on Cisco ISE

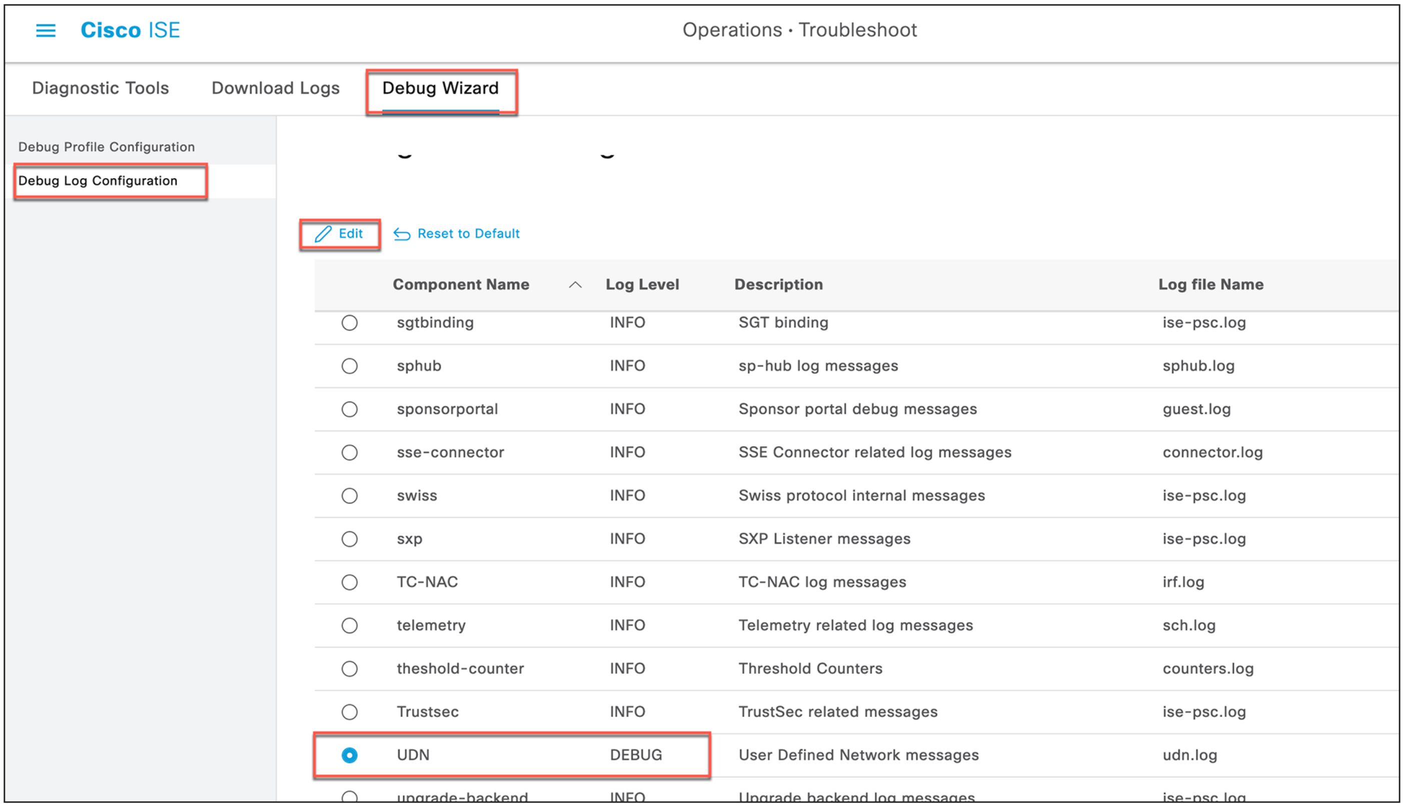
Step 1. On ISE, navigate to **Administration > Operations > Troubleshoot > Debug Wizard > Debug Log Configuration** and select the ISE node from the list.



	Node Name	Replication Role
●	ISE-Ali	STANDALONE

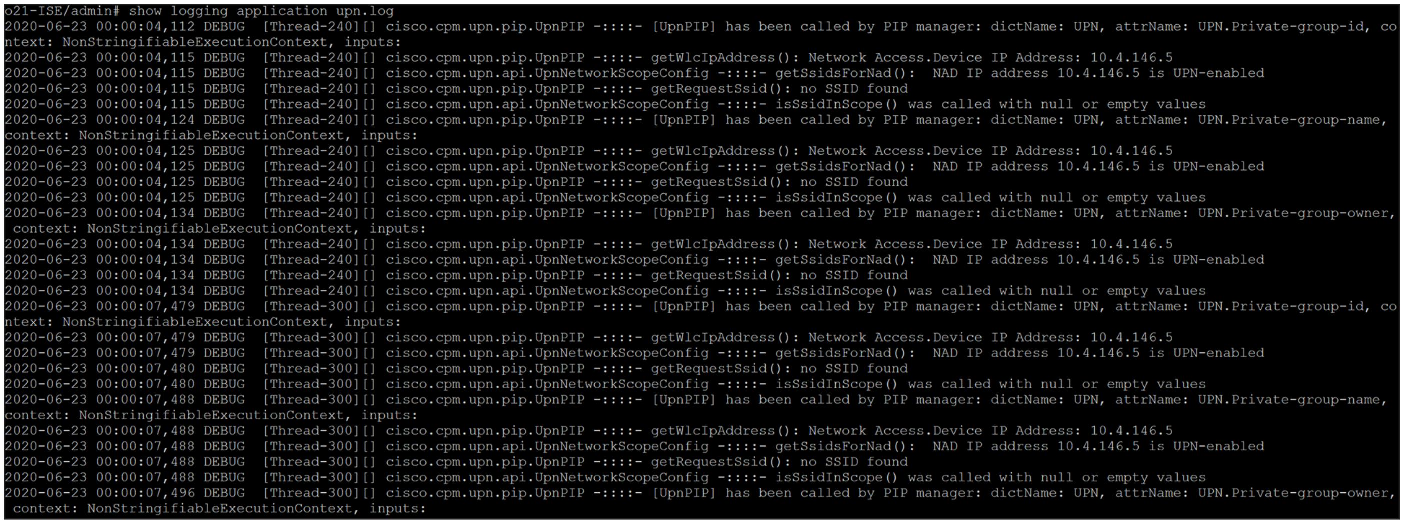
Scroll down the list until you see **UDN** under **Component Name**.

Step 2. Change the log level of UDN to **DEBUG** and click **Save**.



	Component Name	Log Level	Description	Log file Name
○	sgtbinding	INFO	SGT binding	ise-psc.log
○	sphub	INFO	sp-hub log messages	sphub.log
○	sponsorportal	INFO	Sponsor portal debug messages	guest.log
○	sse-connector	INFO	SSE Connector related log messages	connector.log
○	swiss	INFO	Swiss protocol internal messages	ise-psc.log
○	sxp	INFO	SXP Listener messages	ise-psc.log
○	TC-NAC	INFO	TC-NAC log messages	irf.log
○	telemetry	INFO	Telemetry related log messages	sch.log
○	theshold-counter	INFO	Threshold Counters	counters.log
○	Trustsec	INFO	TrustSec related messages	ise-psc.log
●	UDN	DEBUG	User Defined Network messages	udn.log
○	upgrade-backend	INFO	Upgrade backend log messages	ise-psc.log

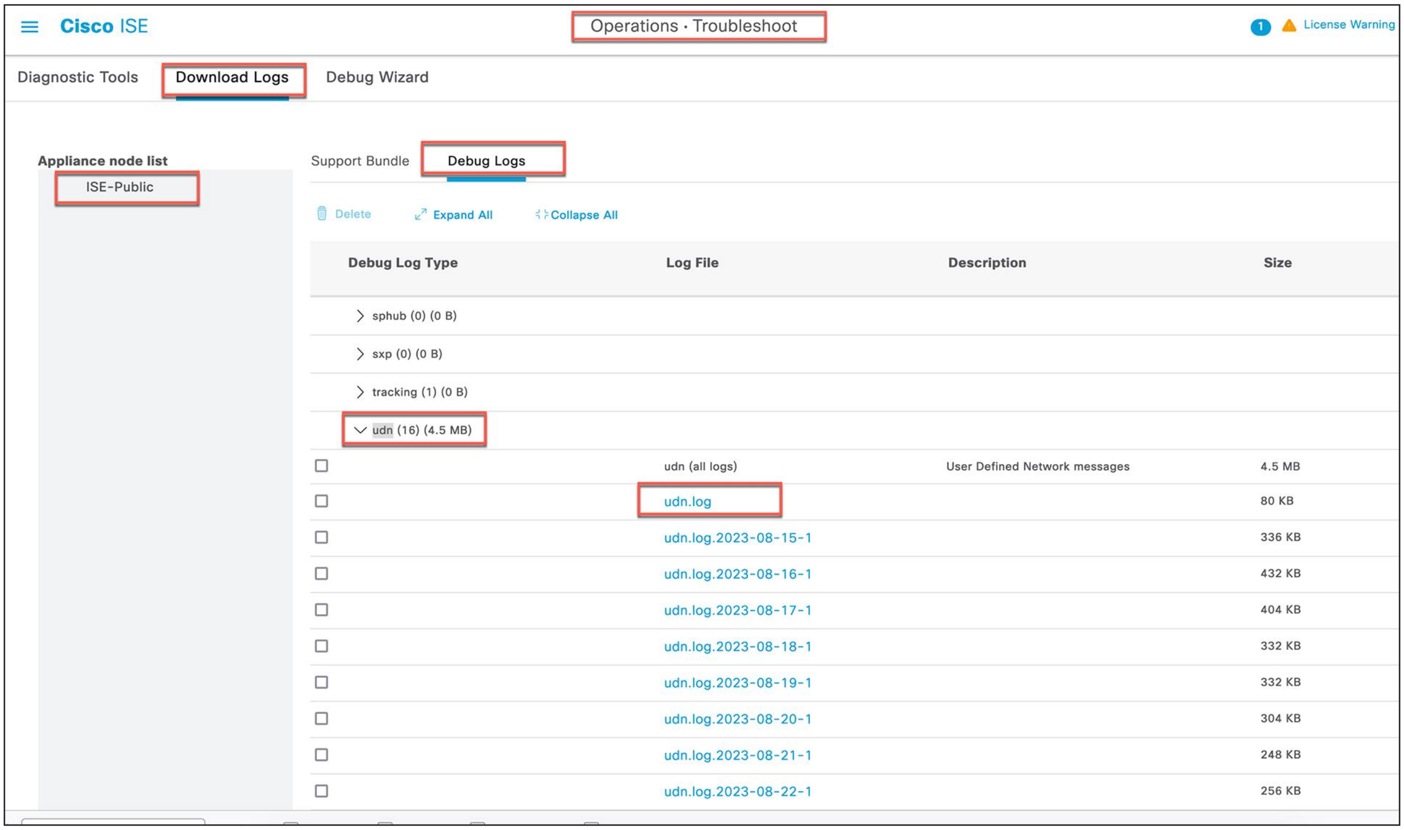
Step 3. With logging enabled, view the logs by accessing the ISE console and entering the command **show logging application upn.log**.



```
o21-ISE/admin# show logging application upn.log
2020-06-23 00:00:04,112 DEBUG  [Thread-240][] cisco.cpm.upn.pip.UpnPIP -::::- [UpnPIP] has been called by PIP manager: dictName: UPN, attrName: UPN.Private-group-id, co
ntext: NonStringifiableExecutionContext, inputs:
2020-06-23 00:00:04,115 DEBUG  [Thread-240][] cisco.cpm.upn.pip.UpnPIP -::::- getWlcIpAddress(): Network Access.Device IP Address: 10.4.146.5
2020-06-23 00:00:04,115 DEBUG  [Thread-240][] cisco.cpm.upn.api.UpnNetworkScopeConfig -::::- getSsidsForNad():  NAD IP address 10.4.146.5 is UPN-enabled
2020-06-23 00:00:04,115 DEBUG  [Thread-240][] cisco.cpm.upn.pip.UpnPIP -::::- getRequestSsid(): no SSID found
2020-06-23 00:00:04,115 DEBUG  [Thread-240][] cisco.cpm.upn.api.UpnNetworkScopeConfig -::::- isSsidInScope() was called with null or empty values
2020-06-23 00:00:04,124 DEBUG  [Thread-240][] cisco.cpm.upn.pip.UpnPIP -::::- [UpnPIP] has been called by PIP manager: dictName: UPN, attrName: UPN.Private-group-name,
context: NonStringifiableExecutionContext, inputs:
2020-06-23 00:00:04,125 DEBUG  [Thread-240][] cisco.cpm.upn.pip.UpnPIP -::::- getWlcIpAddress(): Network Access.Device IP Address: 10.4.146.5
2020-06-23 00:00:04,125 DEBUG  [Thread-240][] cisco.cpm.upn.api.UpnNetworkScopeConfig -::::- getSsidsForNad():  NAD IP address 10.4.146.5 is UPN-enabled
2020-06-23 00:00:04,125 DEBUG  [Thread-240][] cisco.cpm.upn.pip.UpnPIP -::::- getRequestSsid(): no SSID found
2020-06-23 00:00:04,125 DEBUG  [Thread-240][] cisco.cpm.upn.api.UpnNetworkScopeConfig -::::- isSsidInScope() was called with null or empty values
2020-06-23 00:00:04,134 DEBUG  [Thread-240][] cisco.cpm.upn.pip.UpnPIP -::::- [UpnPIP] has been called by PIP manager: dictName: UPN, attrName: UPN.Private-group-owner,
 context: NonStringifiableExecutionContext, inputs:
2020-06-23 00:00:04,134 DEBUG  [Thread-240][] cisco.cpm.upn.pip.UpnPIP -::::- getWlcIpAddress(): Network Access.Device IP Address: 10.4.146.5
2020-06-23 00:00:04,134 DEBUG  [Thread-240][] cisco.cpm.upn.api.UpnNetworkScopeConfig -::::- getSsidsForNad():  NAD IP address 10.4.146.5 is UPN-enabled
2020-06-23 00:00:04,134 DEBUG  [Thread-240][] cisco.cpm.upn.pip.UpnPIP -::::- getRequestSsid(): no SSID found
2020-06-23 00:00:04,134 DEBUG  [Thread-240][] cisco.cpm.upn.api.UpnNetworkScopeConfig -::::- isSsidInScope() was called with null or empty values
2020-06-23 00:00:07,479 DEBUG  [Thread-300][] cisco.cpm.upn.pip.UpnPIP -::::- [UpnPIP] has been called by PIP manager: dictName: UPN, attrName: UPN.Private-group-id, co
ntext: NonStringifiableExecutionContext, inputs:
2020-06-23 00:00:07,479 DEBUG  [Thread-300][] cisco.cpm.upn.pip.UpnPIP -::::- getWlcIpAddress(): Network Access.Device IP Address: 10.4.146.5
2020-06-23 00:00:07,479 DEBUG  [Thread-300][] cisco.cpm.upn.api.UpnNetworkScopeConfig -::::- getSsidsForNad():  NAD IP address 10.4.146.5 is UPN-enabled
2020-06-23 00:00:07,480 DEBUG  [Thread-300][] cisco.cpm.upn.pip.UpnPIP -::::- getRequestSsid(): no SSID found
2020-06-23 00:00:07,480 DEBUG  [Thread-300][] cisco.cpm.upn.api.UpnNetworkScopeConfig -::::- isSsidInScope() was called with null or empty values
2020-06-23 00:00:07,488 DEBUG  [Thread-300][] cisco.cpm.upn.pip.UpnPIP -::::- [UpnPIP] has been called by PIP manager: dictName: UPN, attrName: UPN.Private-group-name,
context: NonStringifiableExecutionContext, inputs:
2020-06-23 00:00:07,488 DEBUG  [Thread-300][] cisco.cpm.upn.pip.UpnPIP -::::- getWlcIpAddress(): Network Access.Device IP Address: 10.4.146.5
2020-06-23 00:00:07,488 DEBUG  [Thread-300][] cisco.cpm.upn.api.UpnNetworkScopeConfig -::::- getSsidsForNad():  NAD IP address 10.4.146.5 is UPN-enabled
2020-06-23 00:00:07,488 DEBUG  [Thread-300][] cisco.cpm.upn.pip.UpnPIP -::::- getRequestSsid(): no SSID found
2020-06-23 00:00:07,488 DEBUG  [Thread-300][] cisco.cpm.upn.api.UpnNetworkScopeConfig -::::- isSsidInScope() was called with null or empty values
2020-06-23 00:00:07,496 DEBUG  [Thread-300][] cisco.cpm.upn.pip.UpnPIP -::::- [UpnPIP] has been called by PIP manager: dictName: UPN, attrName: UPN.Private-group-owner,
 context: NonStringifiableExecutionContext, inputs:
```

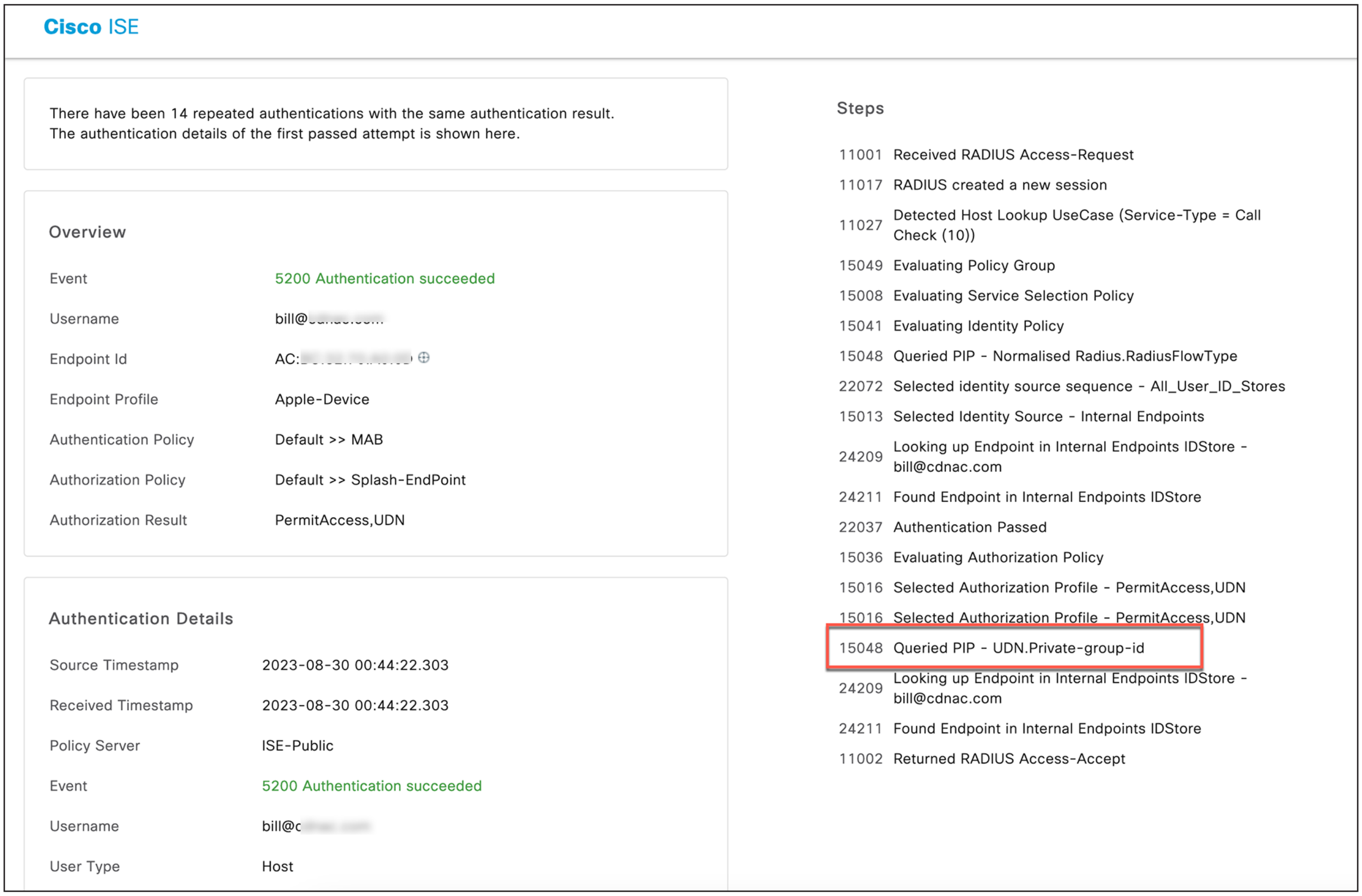
From the ISE dashboard go to **Operations > Troubleshoot > Download Logs**, select the ISE node from the list, and click **Debug Logs**.

Under **Application logs**, select **udn** and click **udn.log** to download the log file.



	Debug Log Type	Log File	Description	Size
	sphub (0) (0 B)			
	sxp (0) (0 B)			
	tracking (1) (0 B)			
	udn (16) (4.5 MB)			
□		udn (all logs)	User Defined Network messages	4.5 MB
□		udn.log		80 KB
□		udn.log.2023-08-15-1		336 KB
□		udn.log.2023-08-16-1		432 KB
□		udn.log.2023-08-17-1		404 KB
□		udn.log.2023-08-18-1		332 KB
□		udn.log.2023-08-19-1		332 KB
□		udn.log.2023-08-20-1		304 KB
□		udn.log.2023-08-21-1		248 KB
□		udn.log.2023-08-22-1		256 KB

Successful authentication of a registered device:



Cisco ISE

There have been 14 repeated authentications with the same authentication result. The authentication details of the first passed attempt is shown here.

Overview

Event	5200 Authentication succeeded
Username	bill@[redacted]
Endpoint Id	AC:[redacted] ⊕
Endpoint Profile	Apple-Device
Authentication Policy	Default >> MAB
Authorization Policy	Default >> Splash-EndPoint
Authorization Result	PermitAccess,UDN

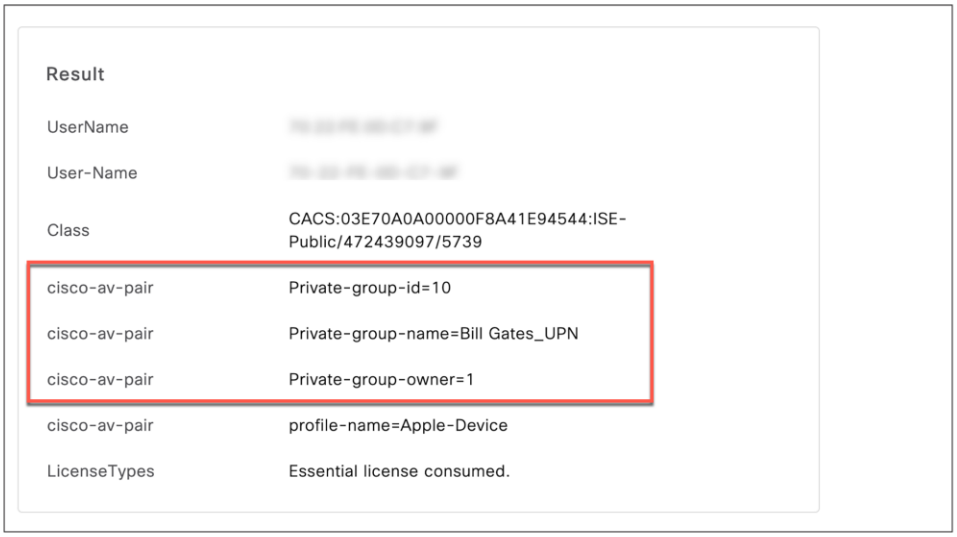
Authentication Details

Source Timestamp	2023-08-30 00:44:22.303
Received Timestamp	2023-08-30 00:44:22.303
Policy Server	ISE-Public
Event	5200 Authentication succeeded
Username	bill@c[redacted]
User Type	Host

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15041	Evaluating Identity Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Endpoints
24209	Looking up Endpoint in Internal Endpoints IDStore - bill@cdnac.com
24211	Found Endpoint in Internal Endpoints IDStore
22037	Authentication Passed
15036	Evaluating Authorization Policy
15016	Selected Authorization Profile - PermitAccess,UDN
15016	Selected Authorization Profile - PermitAccess,UDN
15048	Queried PIP - UDN.Private-group-id
24209	Looking up Endpoint in Internal Endpoints IDStore - bill@cdnac.com
24211	Found Endpoint in Internal Endpoints IDStore
11002	Returned RADIUS Access-Accept

Successful authentication of an unregistered device:



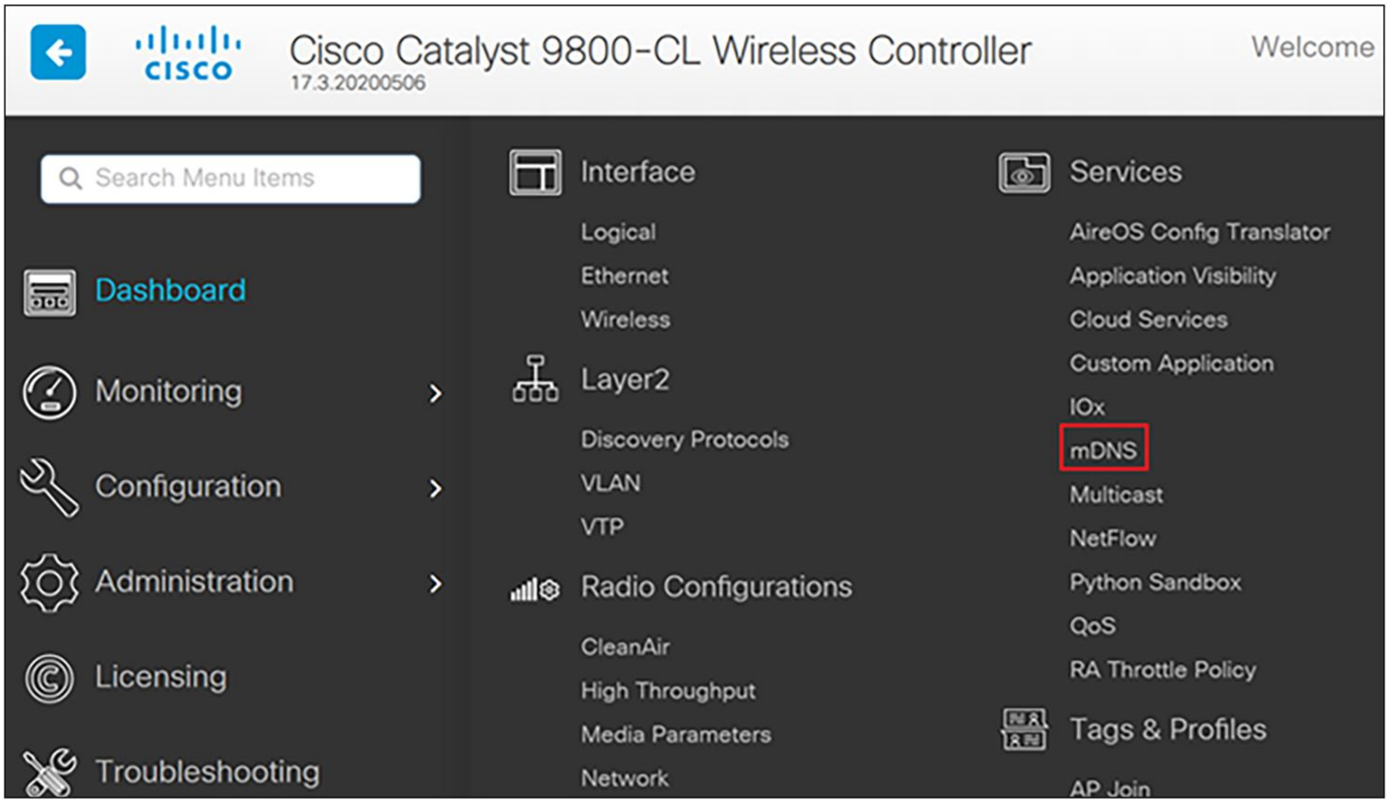
Result

UserName	[redacted]
User-Name	[redacted]
Class	CACS:03E70A0A00000F8A41E94544:ISE-Public/472439097/5739
cisco-av-pair	Private-group-id=10
cisco-av-pair	Private-group-name=Bill Gates_UPN
cisco-av-pair	Private-group-owner=1
cisco-av-pair	profile-name=Apple-Device
LicenseTypes	Essential license consumed.

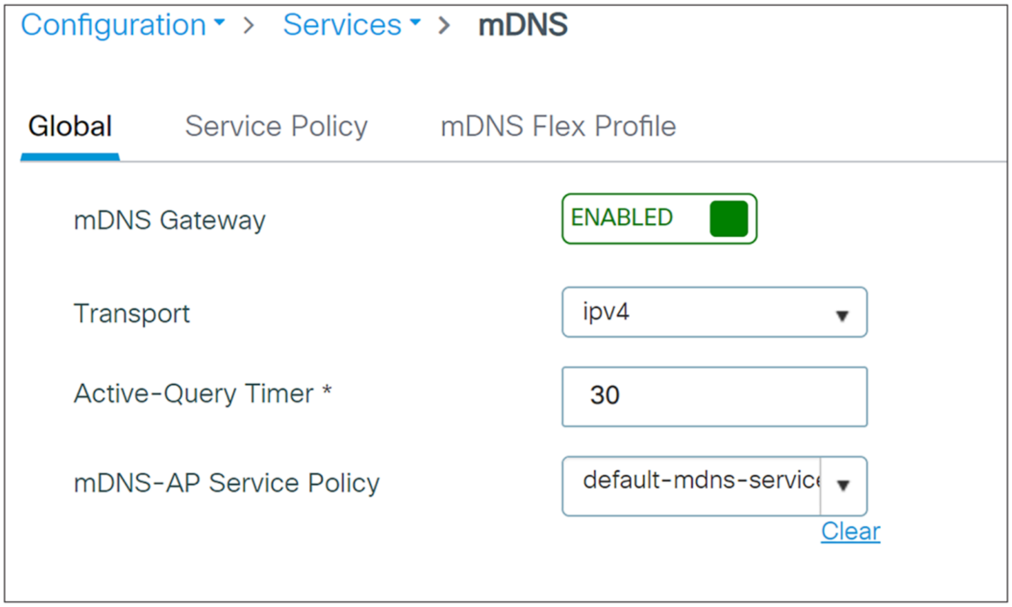
Appendix A: Configuring mDNS Gateway

Cisco's Service Discovery Gateway, or mDNS Gateway, allows for controlled and secure access to services and devices across subnets. It listens to service announcements on all configured network segments and builds a cache of services and addresses. It proxies these requests to other segments and can also apply filters based on various service attributes. These filters can limit what services will be requested or advertised.

Step 1. In the Catalyst 9800 WLC, navigate to Configuration > Services > mDNS.



Step 2. Under **Global**, click next to **mDNS Gateway** to enable it and click **Apply**. If running IPv6, change the **Transport** setting to **Both**.



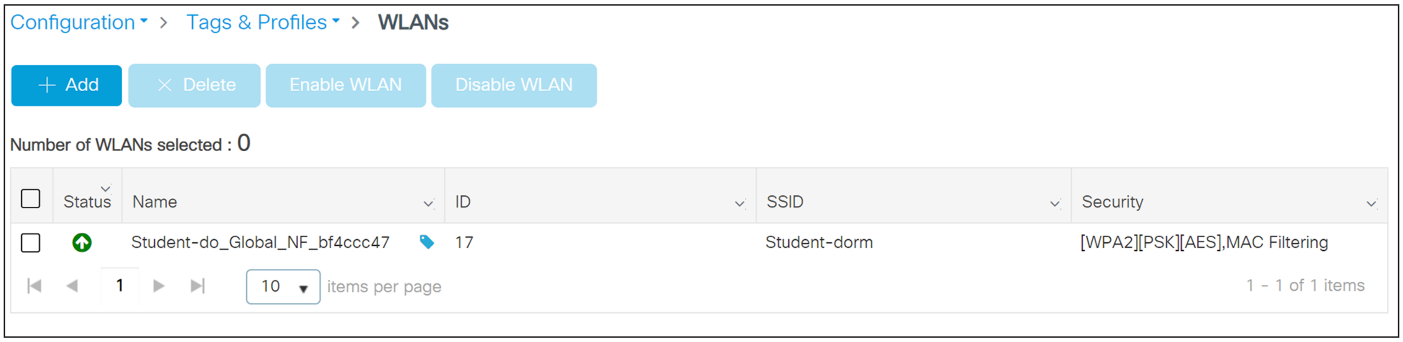
mDNS Gateway: ENABLED

Transport: ipv4

Active-Query Timer *: 30

mDNS-AP Service Policy: default-mdns-servic

Step 3. Navigate to **Configuration > Tags & Profiles > WLANs**.



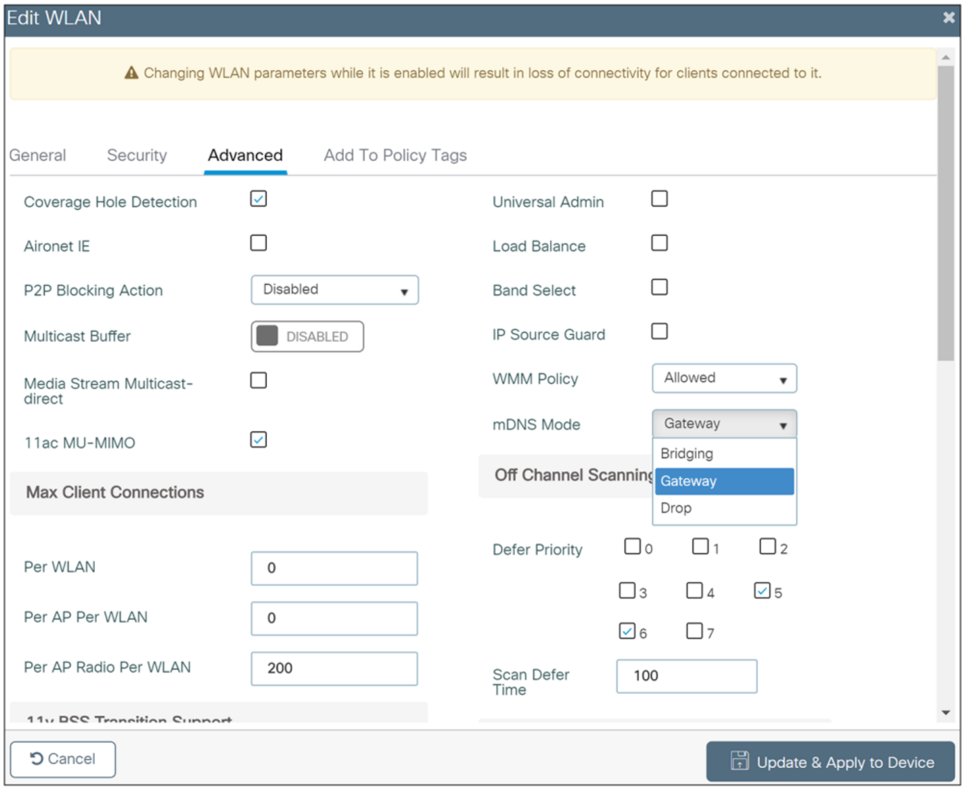
Number of WLANs selected : 0

□	Status	Name	ID	SSID	Security
□	⬆	Student-do_Global_NF_bf4ccc47	17	Student-dorm	[WPA2][PSK][AES],MAC Filtering

1 | 10 items per page | 1 - 1 of 1 items

Step 4. Select the WLAN profile on which to enable mDNS Gateway functionality.

Step 5. Select the **Advanced** tab and change the **mDNS Mode** drop-down to **Gateway**. Click **Update and Apply to Device** when finished.



⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

- Coverage Hole Detection ☑
- Aironet IE □
- P2P Blocking Action: Disabled
- Multicast Buffer: DISABLED
- Media Stream Multicast-direct □
- 11ac MU-MIMO ☑
- Universal Admin □
- Load Balance □
- Band Select □
- IP Source Guard □
- WMM Policy: Allowed
- mDNS Mode: Gateway

Max Client Connections

- Per WLAN: 0
- Per AP Per WLAN: 0
- Per AP Radio Per WLAN: 200

11v BSS Transition Support

Off Channel Scanning

- Defer Priority: □0 □1 □2 □3 □4 ☑5 ☑6 □7
- Scan Defer Time: 100

Step 6. These steps enable **the default-mdns-service-policy** on the WLAN with the following services:

airplay, airtunes, homesharing, printer-ipp, printer-lpd, printer-ipps, printer-socket, google-chromecast, itune-wireless-devicesharing

Tech tip

The Cisco User Defined Network Plus solution does not solve the problem of Universal Plug and Play (UPnP) across VLANs.

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215352-configure-and-troubleshoot-mdns-on-catal.html#toc-hId--1086275938

Appendix B: Randomized MAC address

MAC addresses are used to track and log users in public spaces, and this data can be used for marketing purposes or sold to third parties. To prevent this, device manufacturers have implemented random MAC addresses. This makes the user MAC address unique per network, preventing device tracking. The address is kept consistent per network, meaning once a device is associated with an SSID it will not have to authenticate again. This is why, when using a device with a random MAC address with the User Defined Network Plus solution, a device must be connected to the UDN SSID before it can be registered.

Appendix C: Disabling AirPlay discovery and streaming via Bluetooth

By default, Apple TV has AirPlay enabled with discovery via mDNS and streaming over Ethernet or wireless networks as well as Bluetooth. In a home, these settings are optimal for easy connectivity. However, in environments such as university dormitories, hospitals, and long-term healthcare facilities, these default settings will allow other people to not only discover, but stream to a user's Apple TV if they are on the same wired or wireless network, or within 30 feet of the device (in the case of Bluetooth).

When the Cisco User Defined Network Plus solution is deployed, discovery and streaming is limited to registered devices within the end user's UDN for wired and wireless devices such as MacBooks, iPhones, and iPads. For Apple TV, however, if the AirPlay settings are left in their default state, devices with Bluetooth enabled and within roughly 30 feet of the Apple TV, the signal distance for Bluetooth Low Energy (BLE), will still be able to discover and stream to an Apple TV registered within a UDN. The outcome, if Bluetooth is left enabled, will be that devices in adjacent rooms, both horizontally and vertically, would likely be able to communicate with the Apple TV.

As the concept of Cisco User Defined Network Plus is to optimize the user experience by displaying only those AirPlay devices within the UDN, it might be optimal for the organization deploying the User Defined Network Plus solution to recommend that Apple TV owners disable Bluetooth on their Apple TVs when installing them in their rooms. Unfortunately, there is no single button or setting to disable Bluetooth on the Apple TV, and so the following procedure details how this is accomplished.

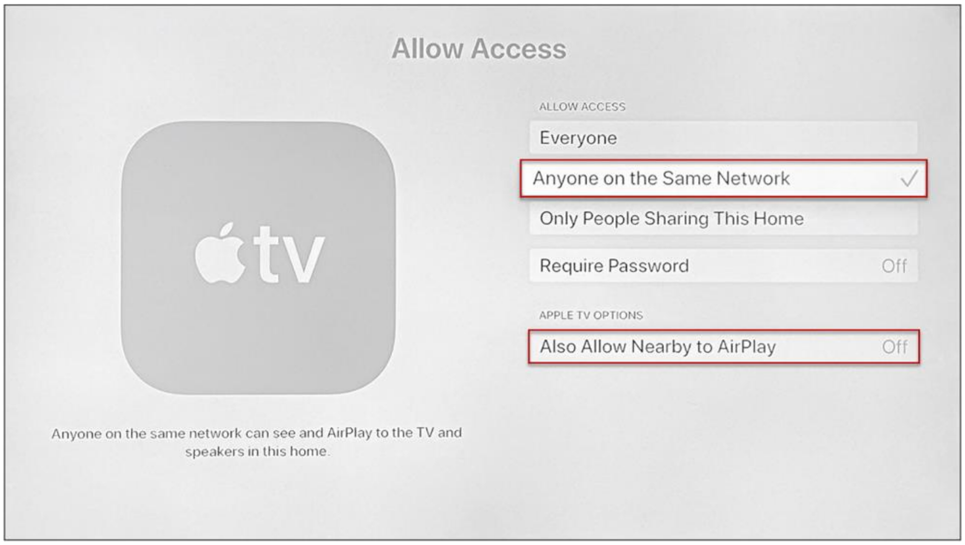
Step 1. From the Apple TV home screen, select **Settings**.

Step 2. Select **AirPlay** and **HomeKit**.

Step 3. Select **Allow Access** (the default is Everyone).

Step 4. Change from **Everyone** to **Anyone on the Same Network**.

Step 5. An Apple TV Options box appears in which you need to change **Also Allow Nearby to AirPlay** to **Off**.



Allow Access

ALLOW ACCESS

Everyone

Anyone on the Same Network ✓

Only People Sharing This Home

Require Password Off

APPLE TV OPTIONS

Also Allow Nearby to AirPlay Off

Anyone on the same network can see and AirPlay to the TV and speakers in this home.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C07-4015479-00 12/23