Guide Cisco public IIIIII CISCO The bridge to possible

# **User Defined Network Plus**

Deployment Guide

## Contents

About this guide	3
The User Defined Network Plus solution	3
Components	4
Solution overview	5
Cisco Identity Services Engine	6
Catalyst 9800 Series wireless controller	7
Device registration and onboarding	8
Device registration flow	8
Device network access	8
Product requirements	9
Scale	9
Process: Prerequisites	9
ISE ERS/pxGrid configuration	10
Process: Splash Access and ISE integration	12
ISE policy created for UDN	15
Splash Access workflow with ISE pxGrid (reference)	16
Splash Access Azure/SAML setup	17
Enable the User Defined Network Plus solution on the Catalyst 9800 Series	25
Process: Configuring an RLAN on the WLC (optional step)	27
End user device registration with the Splash Access portal	31
Catalyst 9800 Series wireless controller	34
Cisco Identity Services Engine (ISE)	35
Appendix A: Configuring mDNS Gateway	39
Appendix B: Randomized MAC address	41
Appendix C: Disabling AirPlay discovery and streaming via Bluetooth	42

## About this guide

This guide is intended to provide technical guidance to design, deploy, and operate the Cisco<sup>®</sup> 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<sup>™</sup>, 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 <u>Splash Access</u> 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 Merakimanaged 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<sup>™</sup> 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 <u>Appendix C</u> 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<sup>®</sup> XE and integrate the RF excellence of Cisco Aironet<sup>®</sup> 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.



#### 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.
- 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.
- 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.
- 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 17.12.3 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: <u>https://www.splashaccess.com/request-demo/</u>
- The Catalyst 9800 Series controller should be added to ISE and vice versa.
   <u>https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-</u>
   <u>controllers/214490-configure-radius-and-tacacs-for-gui-and.html</u>
- 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.

🗙 Cise	co ISE	Q What page are you looking				
Dashboard		Context Visibility	Operations	Policy	Administration	
Recent Pages		System		Network Resources		
	Authorization Profiles Results Policy Sets	Deployment		Network Devices		
		Licensing		Network Device G	Groups	
		Certificates		Network Device P	Profiles	
	Logging Categories	Logging		External RADIUS Servers		
1		Maintenance		RADIUS Server Sequences		
		Upgrade		NAC Managers		
		Health Checks		External MDM		

Step 2. Select the hostname of the ISE node.

Deployment Licensing Ce		Certific	cates	Logging	Maintenance
Deployment		ŵ	Dep	oloymer	nt Nodes
> 🎉 Dep	bloyment		🧷 Edit	Register	Syncup
₀ç₀ PAN F	anover			Hostname	~
				upn-ise	

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

ployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks
🔆 PAN	Failover	Gene	eral Settings	Profiling Config	uration	
		Hos	Iname		upn-ise	
		FQC	N			
		IP A	ddress			
		Nod	ie Type			
			Role STANDALC	DNE Make Primar	Y	
		-	Administra	ation		
			🗆 🗸 Ma	onitoring		
			Role	MADY		
			Other 1	Monitoring Node		
				Dedicated MnT (j)		
		-	— ~ Po	licy Service		
			✓	Enable Session S	ervices 🕕	
			Inclus	de Node in Node Group one		~ ()
			Enable	e Profiling Service 🕕		
			Enabl	e Threat Centric NAC Se	rvice 🕕	
			$\Box$ >	Enable SXP Ser	vice 🕧	
			🔽 Enab	le Device Admin Service	0	
			🔽 Enab	le Passive Identity Servi	ce 🕕	

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**.



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

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

<b>≡ Cisco</b> ISE					Administr	ation · System			
Deployment Li	censing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Client Provisioning FIPS Mode Security Settings Alarm Settings General MDM / UEM Settin	ıgs	API Set	ttings API Service S	ettings API Ga	teway Settings				
Posture Profiling	>	V API Serv	vice Setting RS (Read/Writ Open API (Read	s for Administra e) I/Write)	tion Node				
Protocols Endpoint Scripts	>	imes CSRF Cr	neck ( only f	or ERS Settings	)				
Proxy SMTP Server SMS Gateway System Time API Settings Data Connect		○ Enable C O Disable	SRF Check for	Enhanced Security Request (compatible	(Not compatible a with ERS clien	with pre ISE 2.3 Clien	ts)		

#### **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**.

sp	lashaccess.		٥
	Dashboard	Enable Wired Vlan Device Management in User Device Portal (Requires Radius Server)	
•	Meraki API Settings	Yes	\$
•	ISE API Settings		-
	Meraki Networks	Due Two Factor Anthenia Hales Web 2014 Antennaise	
) <b>I</b>	Group/Room Policies	Duo Two Factor Autinentication - Using web SDK integration	
*	Member Groups	Duo Integration	_
*	Members	Disabled	\$
<b>V</b> i	WPA2 Groups		
÷	Device OnBoarding	ISE Integration	
	Room WPA2 QR Codes	15 Internition	
Ŷ	Voucher Codes	is insymmetry	
	Switch/Port Settings 👻	Enabled	•
٢	Device Assign Policy		_
*	Export Logins	StarRez	
Ŧ	Export Guest Logins	StarRez Student Housing Integration Settings.	
Ê	Reports 👻	StarRez Integration	_
Ð	Wireless Health	Disabled	\$
Ŭ	Log Files 👻		
÷	Admin Settings 👻	Settings	
2	Settings	Allow Member Registration	
	Access Point Locations	Yas	4
	Appearance		2
	Bayment (Strine)	Enable Member Groups (Used for Admin - Member control)	
	SMS	Yas	\$
	System	New Members Require Authorization	
	Text	No	\$
	WDA? Evnire Ontione	Member Requires Authorization error message.	
715	Logout		

**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**.

lashaccess.									
Dashboard Meraki API Settings SE Network Devices	ISE API Settings								
SE API Settings SE Overwrite Aeraki Networks Group/Room Policies	Enter your ISE details here, once submitted you will be guided through the initiation process to prepare your ISE environment. ISE IP 54 ISE admin node Public IP								
lember Groups Aembers VPA2 Groups	ISE Username								
evice OnBoarding toom WPA2 QR Codes									
oucher Codes witch/Port Settings 🗢 evice Assign Policy	Continua								
kport Logins xport Guest Logins	Next steps:								
eports - Vireless Health og Files -	1. Login to your ISE environtment 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 how prove to the user "Manhaines" can be administration of the top of the top of table and the product in t								
dmin Settings - ettings - rofile	Contex rule dox instruction on the top of the table     S. Click the "Approve" button on the top of the table     Within the confirmation pop-up click 'OK'     Tonce 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**.

≡ Cisco ISE	Administration • pxGrid Services	🔺 Evaluation Mode 31 Days 🌒 🔍 ⊘ 🔎 🏟
Summary Client Manager	nent Diagnostics Settings	
Clients Policy Groups Certificates pxRrid Cloud Connection pxRrid Cloud Policy	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.	
	Rows/Page $1 \longrightarrow  \zeta   \leq 1$	
	Name Description Client Groups Status	
	Splash_access_udnplus UDN Test Client • Pending	

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

Adr	ministration · pxGrid Servic	es	<b>A</b> Evaluation Mode 3
nt Diagnostics Settings		D nation client(s)? pprove the selected client(s)?	
😂 Trash 🗸 Edit 📀 Enable 🛞 Disable	🖒 Approve 🛛 🖓 Decline	Rows/Page	<u>1 </u>
Name De	scription	Client Groups	Status
splash_access_udnplus UDI	N 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**.

Continue
Next steps:
1. Login to your ISE environtment 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
Restart PXgrid initiation

**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.

S	plashaccess.								0	
::	Dashboard Meraki API Settings									
	ISE Network Devices	ISE Network devices								
	ISE API Settings	Enter all the IP address	es of your UDN enabled wi	relss lan controllers along w	ith any of their respective	UDN enabled SSID names.				
¢	ISE General	UDN Enabled WLAN Co	ntroller IP							
Ê	ISE Overwrite	10.10.233.3								
ŝ	Meraki Networks									
) in the second s	Group/Room Policies	UDN Enabled SSID Nan	ne 1						Add SSID	
쓭	Member Groups	L2-P3-UDN+								
*	Members									
₹4	WPA2 Groups					C Add				
÷	Device OnBoarding									
88	Room WPA2 QR Codes	Device IP	SSID 1	SSID 2	SSID 3	SSID 4	SSID 5	SSID 6	Action	
ų	Voucher Codes	10.10.231.3	L2-P1-UDN+	P1-RLAN	i.e VLAN101	i.e VLAN101	i.e VLAN101	i.e VLAN101	C Update	
# @	Switch/Port Settings -	10.10.232.3	L2-P2-UDN+	i.e VLAN101	i.e VLAN101	i.e VLAN101	i.e VLAN101	i.e VLAN101	C 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.

splashaccess. Image: Splashaccess.													
Bachboard   Markit AP, Settings   Sist AP I Settings   Markit AP, Settings   Markit	splashaccess.										<	6 Hide Add Polic	y O
• ISE API Settings • Oroup/Room Policy Name • ISE Van Tag (Radius) Network (Vian Onboarding) Default Policy - Ormit Solutions Office Action   • Mender Groups • Ise VLANIO1 • Ise VLANIO1 • Pease select • Oroup/Room Policy Name • Keton   • Mender Groups • Val Croups • Ise VLANIO1 • Ise VLANIO1 • Pease select • Oroup/Room Policy Name • Keton   • Val Croups • Ise VLANIO1 • Ise velocit • Oroup/Room Policy Name • Ise VLANIO1 • Pease select • IoT • Ise plantRegistered • Usdate • Default   • Valcher Codes • Valcher Codes • Ise velocit • Iot VLANIO1 • Pease select • IoT • Ise not in use  • Usdate • Default   • Valcher Codes • Oroup/Room Policy Name • Ise VLANIO1 • Pease select • IoT • Ise not in use  • Usdate • Default   • Valcher Codes • Valcher Codes • O • Ise not in use  • Usdate • Default • Usdate • Default • Usdate • Default   • Valcher Codes • Staff • Iot VLANIO1 • Pease select • Iot · Ort • Ise not in use  • Usdate • Default   • Valcher Codes • Staff • Iot · Iot · Iot · Iot · Iot · Ort • Ise not in use  • Usdate • Default   • Valcher Codes • Staff • Iot ·	∷ ▼	Dashboard Meraki API Settings	Add N	lew Policy									
Merade Networks	•	ISE API Settings	Group/	Room Policy Na	me ISE	Vlan	Tag (Radius)	Network (Vlan Onb	oarding)	Default Policy	Ormit Solutions Office		Action
Image: Composition Policies	Ŷ	Meraki Networks	i.e VL	AN101		i.e \		Please select		Please select		¢	+ Add
Member Groups   Members   VPA2 Groups   Device OnBoarding   Room VPA2 OR Codes   Vouther Codes   Vouther Codes   Switch/Per Settings   2   O   Staff   102   Ormit Solutions Offic 2   In Seprits   Switch/Per Settings   2   3   O   Guest   In Seprits   9   O   Itest   102   Ormit Solutions Offic 2   In Seprits	<b>L</b>	Group/Room Policies							_				
Members       Group/Room Policies       Search       Search       Search       Control         WRA2 Groups       Policie OnBoarding       Policie OnBoarding </th <th>쓭</th> <th>Member Groups</th> <th>-</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>_</th>	쓭	Member Groups	-										_
WPA2 Groups       # * Default       Group/Room Policy Name Ist       Van Tag (Radius)       Network (Vian Onboarding)       Default Policy - Omit Solutions       Endpoint identity group (ISE)       Action         B       Room WPA2 QR Codes       1       Image: State Image:	**	Members	Gro	oup/Roo	m Policies			Search					٩
Device OnBoarding       # + Default       Office of OnBoarding       Detault Policy - Omit Solutions office of om	<b>V</b> 4	WPA2 Groups				_							
B8       Room WFA2 QR Codes       1       Image: Statement of the VLANIO1       Prease select + image:	ē	Device OnBoarding	# \$	Default	Group/Room Policy Name	ISE	Vlan Tag (Radius)	Network (Vlan Onboarding)	Default Policy - Orr Office 🗢	mit Solutions	Endpoint identity group (ISE)	Action	
Voucher Codes     Voucher		Room WPA2 QR Codes	1	•	Students1			Discos colost	IOT		anlack Deviatored	C Lindata	ft Doloto
3       O       Staff       102       Ormit Solutions Offic \$       IOT       ISE not in use \$       C Update       2 Dolete         • Device Assign Policy       3       O       Guest       Image: Comparison of the second of the	Ŵ	Voucher Codes		• I	Students I			Please select			splashRegistered	C Optiale	Delete
Oncide A Assign Policy                  Export Logins               3               O             Guest               Ise VLAN101               Please select               Gold             +               Trendmet-Device             +             CUpdate             0             Delete                 Export Guest Logins               8               Le VLAN101               Please select             +             Gold             +             Trendmet-Device             +             CUpdate             0             Delete                 Export               0             Cueles             Heat               101               Ormit Solutions             Offic             IOT             +             ISE not in use             +             CUpdate             0             Delete                 Witeless Health               102               Ormit Solutions             Offic             +             IOT             +             ISE not in use             +             CUpdate             0             Delete		Switch/Port Settings 👻	2	0	Staff		102	Ormit Solutions Offic \$	IOT	\$	ISE not in use \$	C Update	🖬 Delete
Export Guiss     Export Guiss     C     Court     C	۲	Device Assign Policy	3	0	Guest		Le VI AN101	Plages calact	Gold	*	Trendnet-Device	Clindate	ft Delete
Export Guest Logins     8	*	Export Logins		Ŭ	duon	- T-		1 16036 361601 ¥	GOIG	•		o opdate	
	*	Export Guest Logins	8	0	test1		101	Ormit Solutions Offic 💠	IOT	\$	ISE not in use \$	C Update	🖬 Delete
	8	Reports -	9	0	test		102	Ormit Solutions Offic	IOT	\$	ISE not in use	C Update	Delete
- In the second s	•	Wireless Health								•	•		
c c l j k	¢	Log Files 👻	«	< 1 → »									

#### **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.

=	≡ C	isco IS	E		Policy	Policy Sets				•	License Warning	Q (	) ,a ¢
-	> Auth	norization	Policy - Global Exceptions										
	∨ Auth	norization	Policy (17)										
								Results					
	Ð	Status	Rule Name	Con	ditions			Profiles		Security Group	05	Hits	Actions
	C	CSearch											
		0	Wired-MAB	Ξ	Wired_MAB		_	${\sf PermitAccess} \times$	UDN × V +	Select from lis	t ~+	2617	Ś
			WIFI-MAB	Ξ	Wireless_MAB		_	${\sf PermitAccess} \times$		Select from lis	•t ~ +	935	<u>کې</u>
		$\otimes$	Splash Guest	۲	DEVICE-Location EQUALS All Locations		_	${\sf PermitAccess} \times$	UDN × Y	Select from lis	t	0	ŝ
		0	Splash test	8	IdentityGroup-Name EQUALS Endpoint Identity Grou	ips:splashRegistered	_	Splash × UDN	×	Select from lis	t ~+	6515	ŝ
		0	Employee_dot1x	AND	Wireless_802.1X           R           IdentityGroup-Name EQUALS User Identity	Groups:Employee		${\sf PermitAccess} \times$		Select from lis	.t ~+	0	ŝ
		0	Wireless Block List Default	AND	Wireless_Access           R           IdentityGroup-Name           EQUALS           Endpoint	tity Groups:Blocked List		Block_Wireless_A	×	Select from lis	<u>.t ~</u> +	0	錼

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

Cisco ISE			Policy · Policy Elements
Dictionaries Cond	ditions	Results	
Authentication	>	Authorization Profiles > iPSK_Splash	
Authorization	×	Authorization Profile	
Authorization Profiles		Name iPSK_Splash	
Downloadable ACLs		Description	
		Description	
rofiling	>	* Access Tupe	
osture	>	ACCESS_ACCEPT V	
Client Provisioning	>	Network Device Profile 🗮 Cisco 🗸 🕀	
		Service Template	
		Track Movement 🛛 🛈	
		Agentless Posture	
		Passive Identity Tracking 🔲 🕕	
		✓ Common Tasks	
		DACL Name	
		ACL (Filter-ID)	
		ACL IPv6 (Filter-ID)	
		✓ Advanced Attributes Settings	
		🗄 Cisco:cisco-av-pair 🗸 " psk-mode=ascii 🗸 —	
		#	
		" Cisco:cisco-av-pair V EndPoints:IPSK V =	P
		✓ Attributes Details	
		Access Type = ACCESS_ACCEPT risco-analy = pdc mode=scrii	
		cisco-av-pair = EndPoints:IPSK	

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

=	Cisco I	SE		Policy · Policy Sets			0 (	2 Ø	<b>7</b>
> A	uthorization	n Policy - Global Exceptions							
~ A	uthorization	n Policy (15)							
					Results				
	Status	Rule Name	Conditions		Profiles	Security Groups		Hits	Actions
	Q Searc	'n							
		Wireless Block List Default	AND Restly Groups Name EQUALS Endpoint Identity Groups:Blocked List		Block_Wireless_Access × +	Select from list	~+	۰	¢
_		Mac-Filter	Wireless_MAB		PermitAccess $\times$ UDN $\times$ $\checkmark$ +	Select from list	$\sim +$	0	{ô}
	٥	Splash-EndPoint	A IdentityGroup-Name EQUALS Endpoint Identity Groups:SplashAccessRegistered		UDN $\times$ IPSK_Splash $\times$ $\checkmark$ +	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
- 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.

splashaccess.									
🛏 Group/Room Policies									
嶜 Member Groups	System Settings								
🐣 Members									
WPA2 Groups	Admin System								
🖶 Device OnBoarding	Enable/Disable two-factor authentication.								
器 Room WPA2 QR Codes	Two-Factor Authentication								
🛷 Voucher Codes	Enabled								
료 Switch/Port Settings 👻									
Device Assign Policy									
🛓 Export Logins	Login System								
🛓 Export Guest Logins	Azure Active Directory								
🛱 Reports 👻	Google Workspace (GSuite)								
- Wireless Health	✓ Membership								
Wileless Health	Okta								
👙 Log Files 🛛 👻	Sami								
💄 Admin Settings 🛛 👻									
🕸 Settings 🔺	Enable Standard Guest Login (i.e Email, First/Last name)								
Access Point Locations	No								
Appearance	Enable Voucher Guest Login								
General	N.								
Payment (Stripe)	INO								
SMS									
System	Switch Ports & Wired Vlans								
Text	Switch Port and Wired Vlan Device Management Options.								
WPA2 Expire 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							
C							
Directory (tenant) ID							
REAL TO ALL AND A REAL AND TAKEN							
Certificates / Client secret							
*****							
	Contraction of the second seco						

#### 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 <u>https://portal.azure.com</u>. The system will then redirect users to log in using their Microsoft 365 information.

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



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

External Identities					
and administrators	Name	Splash Access		Users	28
Administrative units	Tenant ID	805498e0-72dc-4659-8c4c-c8db316eabe4 🗋		Groups	63
🔶 Delegated admin partners	Primary domain	splashaccess.co.uk		Applications	16
Enterprise applications	License	Azure AD Premium P2		Devices	16
Devices					
👪 App registrations	Workload License	Azure AD Workload Free			
(a) Identity Governance	Alerts				
Application proxy					
Custom security attributes	Gradual IPve	enablement from April to June 2023	Upco	oming MFA Server	deprecation
(Preview)	Please reviev	and update your Named locations 🥼 🦲	Please	se migrate from MF	FA Server to Azure AD Multi-
https://portal.azure.com/#view/Microsoft_AAD_IAM	/ActiveDirectoryMenuBlade	/~/RegisteredApps : to avoid any service	Facto	or Authentication by	y 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.

A Splash Access - Microsoft Azure ×	F										$\sim$		-		$\times$
$\leftarrow \rightarrow$ C $\textcircled{a}$ $\bigcirc$ A https://port	tal.azure.com/#view/	Microsoft_AAD_IAN	M/ActiveDirectoryMe	☆ Q	Search				$\bigtriangledown$	$ \pm $	111		u (	<b>)</b> ර	≡
$\equiv$ Microsoft Azure $P$ Search re	esources, services, an	d docs (G+/)				P	Û		0	ন্স	ې SPL	baul@sj Asн Acc	olashacc ESS (SPLAS	ess.co.u HACCESS	k 🙆
Home > Splash Access															
Splash Access   App registrations       * ···       ×         Azure Active Directory       ×       ×															
Overview	+ New registration	n 🌐 Endpoints	P Troubleshooting	🖒 Refre	sh ⊻ Dov	wnload	🐼 Pre	eview	feature	s	ନ୍ <u>ନ</u> ୧	ot feed	back?		
<ul> <li>Preview features</li> <li>X Diagnose and solve problems</li> </ul>	Starting June 3 continue to pro Authentication	Oth, 2020 we will no lo ovide technical suppo Library (MSAL) and N	nger add any new featur rt and security updates b Aicrosoft Graph. <u>Learn m</u>	es to Azure A ut we will no <u>ore</u>	ctive Director longer provic	y Auther le feature	ntication l e updates	Library . Appli	(ADAL) cations	and Az will nee	ture AD ad to b	) Graph. e upgrad	We will led to Mi	crosoft	×
Manage															
🚨 Users	All applications	Owned application	ons Deleted applic	ations											
🏄 Groups	Start typing a general start typing a gene	lisplay name or app	lication (client) ID to fi	ter these	+	Add filt	ers								
📫 External Identities	,		(												
Roles and administrators	1 applications foun	d													
Administrative units	Display name $\uparrow_{\downarrow}$			A	pplication (	client) II	D		Create	ed on	$\uparrow_{\downarrow}$	Certific	ates & s	ecrets	
🚸 Delegated admin partners	sa SplashAcce	ess Azure		c	d89e153-83	15-475d	l-9a97-f7	1c4	5/10/2	2021		Exp	ired		
Enterprise applications															
Devices															
App registrations															
Identity Governance															
Application proxy															
Custom security attributes (Preview)															

Home > CDNAC   App registrations >								
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)								
O Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)								
<ul> <li>Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)</li> </ul>								
O 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.								
Select a platform V e.g. https://example.com/auth								
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 🗗								
Register								

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.

Overview	lace A certificate or secret is expiring soon. Create a new one $ ightarrow$							
📣 Quickstart								
🚀 Integration assistant	↑ Essentials							
Manage	Display name SplashAccess Azure	Client credentials <u>0 certificate, 8 secret</u>						
🔤 Branding & properties	Application (client) ID	Redirect URIs						
Authentication	cdł śf2fb1 Um	<u>9 web, 0 spa, 0 public client</u>						
📍 Certificates & secrets	Object ID ab Copy to clipboard	Application ID URI Add an Application ID URI						
Token configuration	Directory (tenant) ID	Managed application in local directory SplashAccess Azure						
→ API permissions	Supported account types							
🙆 Expose an API	Multiple organizations							

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

👗 SplashAccess Azure - Microsoft X + 🗸 –	×						
C      A https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/Applica     C     C     Search     O      L     L     L     C     L     C     L     C     L     C     L     C     L     C     L     C     L  L     L	≡						
😑 Microsoft Azure 🔎 Search resources, services, and docs (G+/) 🗵 🖟 🖓 🛞 🕐 🖗 paul@splashaccess.co.	uk 🙆						
Home > SplashAccess Azure							
SplashAccess Azure   Authentication * ···	$\times$						
Redirect URIs							
4 Quickstart The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The URIs we will accept as the user of the URIs we will accept as the user of t	ie						
1 Integration assistant URIs and their restrictions							
Manage 'social.php	Û						
Branding & properties /social.php	۱.						
Authentication /social.php							
📍 Certificates & secrets /social.php	۱.						
Token configuration 'social.php	۱.						
API permissions https://server2.splash-access.com/social.php	۵.						
Expose an API https://server1.splash-access.com/social.php	Û						
👪 App roles /social.php							
A Owners https://wifi.splash-access.com/social.php	۱.						
& Roles and administrators Add URI							
III Manifest							
Support + Troubleshooting							
7 Troubleshooting           Save         Discard							

- 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.

🚀 Integration assistant	Implicit grant and hybrid flows
Manage	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
🚍 Branding & properties	tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.
Authentication	Select the tokens you would like to be issued by the authorization endpoint:
📍 Certificates & secrets	Access tokens (used for implicit flows)
Token configuration	ID tokens used for implicit and hybrid flows)
->- API permissions	
🙆 Expose an API	Supported account types
👪 App roles	Who can use this application or access this API?
🎎 Owners	Accounts n this organizational directory only (Splash Access only - Single tenant)
A Roles and administrators	Account in any organizational directory (Any Azure AD directory - Multitenant)
0 Manifest	Help me decide
Support + Troubleshooting	
Troubleshooting	Save Discard

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 - Microsoft X + 🗸 — 🗆								×			
$\leftarrow$ $\rightarrow$ C $\textcircled{a}$ $\bigcirc$ A https://point	rtal. <b>azure.com</b> /#view/Microsoft_AAD_Regis	teredApps/Appli	cal ☆ Q Search			⊘ ⊻	hit\		u. 🕅	பி	≡
≡ Microsoft Azure 🔎 Search I	resources, services, and docs (G+/)			R 🗘	۲	ଡ ନ	SP	paul@s LASH ACC	plashacces	s.co.uk	0
Home > SplashAccess Azure	Cortificatos & socrats	A	Add a client	secret							×
	Certificates & secrets	~	Description		En	ter a desci	iption f	or this	client secre	t	
	🔗 Got feedback?		Expires		73	0 days (24	month	5)		1	$\sim$
Overview	• Appreciation registration certificates, see				Re	commend	ed: 180	days (6	months)		
🍊 Quickstart					90	days (3 m	onths)				
🚀 Integration assistant	Certificates (0) Client secrets (7)	Federated cred			36	5 days (12	months	5)			
Manage	A secret string that the application uses to	prove its identi			54	5 days (18	months	5)			
🖬 Branding & properties	+ New client secret				73	0 days (24	months	5)			
Authentication	I we chent secret	Funites			Cu	stom					
📍 Certificates & secrets		Z/4/2022									
Token configuration	Splach Accors 12th Oct 2022 -> Oct	10/12/2023									
-> API permissions		2/20/2025									
🙆 Expose an API		3/5/2015									
App roles	The law and loss and	3/29/2023	Kay Canc	er		_				ID	
A Owners		4/6/2025	FZv*********	rik.	_	_					Ê.
& Roles and administrators	SplashAccess	6/20/2025	0e0***********	*** Cor	by to clip	board				. D	Î
🔟 Manifest	Splash New	6/20/2025	krv8Q~			b4				D	ے ا ا
Support + Troubleshooting					J						_
Troubleshooting											

- 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.

🗳 Quickstart	Configured permissions						
🚀 Integration assistant	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						
Manage	+ Add a permission V Grant admin consent for Splash Access						
Branding & properties	Admin concent reg Statur						
Authentication	Add a permission type Description Add a permission						
📍 Certificates & secrets	/ Microsoft Graph (6)						
Token configuration							
- API permissions	To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.						
🙆 Expose an API							



Home > SplashAccess Azure	Request API permissions ×	
<sub> - SplashAccess Azure</sub>	API per	
	All APIs Microsoft Graph	
Search «	Refresh     Intersection of the section of the	
Overview	What type of permissions does your application require?	
🍊 Quickstart	Configured	
🚀 Integration assistant	Applications Permissions: 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.	
Manage	+ Addar	
Branding & properties	API / Perm	
Authentication		
📍 Certificates & secrets	> Microsoft	
Token configuration		
- API permissions	to view and t	
lexpose an API		

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 - Micro 🗙	-					$\sim$	1	-		×
	al.azure.com/#view/Microsoft_AAD_RegisteredApps/Applica	Q Search		$\bigtriangledown$	$_{\pm}$	lii\	🗉 🗴	0	ſ	=
≡ Microsoft Azure 🔎 Search	sources, services, and docs (G+/)		G 🖓 🕸	0	ጽ	pa spla	ul@splas sн access (!	naccess PLASHA	.co.uk	9
Home > SplashAccess Azure	Request API permissions								×	
✓ Search « Øverview	O         Delegated permissions           Your application needs to access the API as the signed-in	ı user.	Application permissi Your application runs signed-in user.	ons ; as a bac	kgroun	d service	e or daemo	n witho	ut a	
<ul><li>Quickstart</li><li>Integration assistant</li></ul>	Configurec Select permissions Apprications permissions :							)	expand a	II <
Manage Branding & properties D Authentication	+ Add a p Add a p API / Perm D The "Admin consent required" column shows the d permission, user, or app. This column may not refler more	efault value for an ct the value in you	organization. However, Ir organization, or in org	user con anizatior	isent ca is where	n be cus e this ap	tomized po p will be us	er ed. <u>Lea</u>	×	
Certificates & secrets     Token configuration	Permission				Admin	conser	nt require	d		
API permissions     Expose an API	Vuser (1)									
App roles     Owners     Roles and administrators	User.Read O Sign in and read user profile				No					
Manifest	User.Read All ③ Dead all users! full profiles			5	Yes					
P Troubleshooting	Add permissions Disperd									

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

sp	olashaccess.	•							
	Dashboard	i.e https://www.oursami.com/idp/shibboleth							
•	Meraki API Settings								
•	ISE API Settings	NetaData For Point (entitle) location							
	Meraki Networks	e https://www.oursaml.com/ido/shibboleth							
j±m,	Group/Room Policies	to regularities duration regularities and a second s							
쓭	Member Groups	<sup>1</sup> Post (Single Sign On Service)         HTTP Post Simple Sign (Single Sign On Service)							
*	Members	i.e https://www.oursami.com/idp/profile/SAML2/POST/SSO i.e https://www.oursami.com/idp/profile/SAML2/POST-SimpleSign/SSO							
₹	WPA2 Groups	HTTP Redirect (Single Sign On Service)							
ē	Device OnBoarding	i.e https://www.oursami.com/idp/profile/SAML2/Redirect/SSO							
	Room WPA2 QR Codes	HTTP Redirect (Sinde Log Out Service)							
Ŵ	Voucher Codes	a https://www.oursaml.com/ido/profiled.com/t							
	Switch/Port Settings 🔹	re-uniterative stream ensuring the homoved exer							
	Device Assign Policy	SOAP (Artifact Resolution Service)							
Ł	Export Logins	i.e https://www.oursami.com/8443/idp/profile/SAML2/SOAP/ArtifactResolution							
÷	Export Guest Logins	X509 Certificate							
Ê	Reports 👻	i.e MJIKQIBAAKCEAEAqz							
Ð	Wireless Health								
ø	Log Files 👻								
÷	Admin Settings 🛛 👻								
٠	Settings 🔶								
	Access Point Locations								
	Appearance	~ Score							
	General	aupe							
	Payment (Stripe)	Le spiasnum							
	SMS	C Update							
	System								
	lext								
	Logout	About Make a Wish Help Support @ Copyright Splash Access-2023 1							

## 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	Edit WLAN *
+ Add × Delete Clone Enable WLAN Disable W	AN Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.
Selected WLANs : 0           Status Y           Name           SplashUDN           1	General     Security     Advanced     Add To Policy Tags       Layer2     Layer3     AAA
	Image: WPA + WPA2     O WPA2 + WPA3     O WPA3     O Static WEP     O None       MAC Filtering     Image: Authorization List*     aws-ise-a     Image: O O O O O O O O O O O O O O O O O O O
Image: Second	Lobby Admin Access         WPA Parameters         WPA Policy         Policy         GTK OSEN         Policy         WPA2 Policy         GTK OSEN         Policy         WPA2 Policy         WPA2 Policy         WPA2 Policy         WFA2 Encryption         AES(CCMP128)         GCMP128         GCMP128         GCMP256         PMF         Disabled         PMF         Disabled         PSK Format         ASCII         PSK Type         Unencrypted         Pre-Shared Key*
	Cancel

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.

Q Search Menu Items	1	Ξ	Interface	6	Services
			Logical		AireOS Config Translator
Dashboard			Ethernet		Application Visibility
			Wireless		Cloud Services
Manitarian		1	Laver2		Custom Application
Monitoring	>	660			lOx
2			Discovery Protocols		mDNS
Configuration	>		VLAN		Multicast
~			VIP		NetFlow
O Administration	>	ııll⊗	Radio Configurations		Python Sandbox
			CleanAir		QoS
C Licensing			High Throughput		RA Throttle Policy
			Media Parameters		Tags & Profiles
Troubleshooting			Network		AD Join
••			Parameters		FOGRE
			RRM		Elex
			Pouting Protocolo		Policy
		(F)			Remote LAN
			Static Routing		RF
		$\bigoplus$	Security		Tags

**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**.

Configuration • > Tags & Profile	s▼ > Policy	Edit Policy Profile					
+ Add × Delete	Clone	General Access Policies	QOS and AVC Mob	ility Advar	nced		
Admin <b>Y</b> Associated <b>9</b> Status Policy Tags	Policy Profile Name	WLAN Timeout			Fabric Profile		v 2
	SplashAccess-PP	Session Timeout (sec)	1800	)	Link-Local Bridging	0	
	default-policy-profile	Idle Timeout (sec)	300	]	mDNS Service Policy	default-mdns-ser	▼ ⊿ <u>Clear</u>
		Idle Threshold (bytes)	0	]	Hotspot Server	Search or Select	▼ 2
		Client Exclusion Timeout (sec)	60	]	User Defined (Private	e) Network	
		Guest LAN Session Timeout	0		Status		
		DHCP			Drop Unicast	0	
		IPv4 DHCP Required	0		DNS Layer Security		
		DHCP Server IP Address			DNS Layer Security Parameter Map	Not Configured	▼ <u>Clear</u>
		Show more >>>			Flex DHCP Option for DNS	ENABLED	
		AAA Policy		]	Flex DNS Traffic	IGNORE	
		Allow AAA Override			Redirect		
		NAC State	0		WLAN Flex Policy		
		Policy Name	default-aaa-policy × 🔻		VLAN Central Switchin	g 🖸	
		Accounting List	Search or Select 🗸		Split MAC ACL	Search or Select	▼ 2
		WGB Parameters			Air Time Fairness Po	licies	
		Cancel				📅 Update & .	Apply to Device

**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**.

Configuration * > Tags & Profiles * > Tags	Edit Policy Tag		,
Policy Site RF AP	A Changes may result in loss of connectivit	y for some clients that are associated to APs with this Policy Tag.	
Add × Delete Clone Policy Tag Name SolashAccess	Name* SplashAccess Description Enter Description		
default-policy-tag	WLAN-POLICY Maps: 5		
	WLAN Profile	Policy Profile	Ŧ
	SplashUDN	SplashAccess-PP	
	#SplashPSK	SplashAccess-PP	
	#SplashWPA3	SplashAccess-PP	
	#SplashDot1x	SplashAccess-PP	
	#SplashWPA3-PSK	SplashAccess-PP	
	H ≺ 1 ► H 10 ▼	1 - 5 of	5 items
	Map WLAN and Policy		
	WLAN Profile* SplashUDN v	Policy Profile* SplashAccess-PP V	
		× •	_

## 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		
Client Association Limit	0	
mDNS Mode	Bridging •	
Cancel		Apply to Device

Add RLAN Profile	×
General Security	
Layer2 Layer3 AAA	
802.1X	DISABLED
MAC Filtering	aws-udn-authZ = 2 Clear
Authentication List	aws-udn-authN Clear
Fallback Mechanism	No Fallback
EAP-Identity-Request Retries Status	DISABLED
EAP-Request Retries Status	DISABLED
Cancel	Apply to Device

## 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</vlan>
	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.

Add RLAN	Policy					×
General	Access Policies	Advanced				
	<b>A</b> C	Configuring in enabled state will res	ult in loss of conr	nectivity for clients associated v	with this policy.	
Policy N	ame*	L2-P1-RLAN-Policy	]	RLAN Switching Policy		
Descript	ion	Enter Description		Central Switching	ENABLED	
Status				Central DHCP		
PoE		0				
Power L	evel	4 🔹				
Cancel						
						lice

Add RLAN Policy			×
General Access Policies	Advanced		
Pre-Authentication	D	Host Mode	singlehost 🗸
VLAN	VLAN0100		
Remote LAN ACL			
IPv4 ACL	Not Configured		
IPv6 ACL	Not Configured		
Cancel			Apply to Device

Add RLAN Policy			×
General Access Policies	Advanced		
Violation Mode	replace 🔻	Split Tunnel Parameter	ers
Session Timeout (sec)	1800	Status	0
mDNS Service Policy	Search or Select 🛛 🗸	ACL Name	Not Configured
User Defined (Private) Net	work	Exclusionlist Params	
Status		Exclusionlist	
Drop Unicast	0	Exclusionlist Timeout	60
AAA Policy Params		DHCP	
AAA Override		IPv4 DHCP Required	0
AAA Policy Name	default-aaa-policy v 2	DHCP Server IP Address	XXX.XXX.XXX.XXX
Accounting List	Not Configured 🔻 💈		
Cancel			Apply to Device

**Step 2.** Apply the RLAN to the policy profile.

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

AP Name	AP Model	~	Slots v	Admin Status	V IP Address V	Base Radio ~ MAC	AP Mode	<ul> <li>Operation</li> <li>Status</li> </ul>	Policy Tag ~	Site Tag ~	RF ~ Tag	Tag ~ Source	Location ~	Country	~
AP3800- Cafe d	AIR-AP380 B-K9	21-	2	0	172.20.229.176	b4de.( )	Local	Registered	PT_SanJo_SJ14_Floor1_6099c	ST_SanJo_SJ14_a45f2_0	TYPICAL	Static	Global/San Jose/SJ14/Floor1	US	

 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 *continuation* Click *continuation*.

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

RLAN-POLIC	CY Maps: 0 Delete		
Port ID	~ RLAN Profile	<ul> <li>RLAN Policy Profile</li> </ul>	~
	I0 🔻 items per page		No items to display
Map RLAN and Po	olicy		
Port ID*	1		
RLAN Profile*	@UDN-PSK 🔻	RLAN Policy Profile*	-PSK
	×		
Cancel			pdate & Apply to Device

#### 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: <a href="https://customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-account-splashudn.com/accounts/customer-account-splashudn.com/accounts/customer-account-splashudn.com/account-splashudn.com

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**.

	sp	lash <mark>acces</mark>	55.
	WPA2 I	Registration	Portal
	Cli	ck below to manage your accou	unt.
		Continue	
~	I agree to the Terr	ms and Conditions.	
	Your Info	Terms & Conditions	Privacy Policy

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 Can't access your account?		
Microsott  Sign in bill@cdnac.com Can't access your account?  Next		
Sign in bill@cdnac.com Can't access your account? Next		
bill@cdnac.com Can't access your account? Next	Sign in	
Can't access your account?	bill@cdnac.com	
Next	Can't access your account?	
Next		
		Next
Sign_in options	Sign-in options	

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.

splashaccess.			🕞 Logout 🛛 🛠
WPA2/Guest Registration Portal Welcome, you can manage your Guest Code(s) and generate a WPA2 pase Account: bill@cdnac.com	isword below.		
Generate a WPA2 password.		0	
WPA2 Password			
7y2x7Xo56C82m4	<b>I</b> D	Cenerate Password	
Scan the QR code to securely onboard your devices.			
Manage Device(s)			2 3
Add Device			0 of 20 Devices
Mac Address	Device Name	Device Description (Optional)	+ Add

Manage Device(s)				
Add Device				
Mac Address	Device Name	Device De:	scription (Optional)	+ Add
Mac Address	Device Name	Device Description	Action	
11:22:33:AA:BB:DD	bill-device	Device Description (Optional)	C Update 🛍 Delete	i Check
70	Bill-iPhone14	Device Description (Optional)	C Update	i Check
AC:	Bill-AppleV	Device Description (Optional)	C Update 🛍 Delete	i Check
11:11:11:11:22	iPad	Device Description (Optional)	C Update	i Check

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

Check device provisioning					
Device is provisioned correctly.					
Close					

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 wi MAC Address	ireless client AP Name	udn		Type ID	State
Proto	ocol Method	Role	UDN-ID		
90dd.5de7.f0c2	AP00A6.CA36.04	114		WLAN 17	Run
11ac	MAB	Local	16762216		
b49c.df89.bba6	AP00A6.CA36.04	114		WLAN 17	Run
11n (2	2.4) MAB	Local	16715577		
b85d.0aa0.47ec	AP00A6.CA36.04	114		WLAN 17	Run
11ac	MAB	Local	16762216		
b8e8.561c.4918	AP7872.5DED.CI	034		WLAN 17	Run
11ac	MAB	Local	16544774		
ccc0.7972.071a	AP7872.5DED.CI	034		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 name: homer's room
```

#### 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 chass		Ls WNCD_D		lc_tbl_client_commo	n_oper_data"
Database Name: WNCD_DB Table Name: table evid: table one: table evid: table client_common_oper_data OID (ID/SRC): 0xfs2b80390df33004a5af0703@0dfe3c6/0x0000000000 Table UID: 30b0343863dscba702155773d0e0cfe06 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			Ls WNCD_D			_oper_data"
Database Name: WNCD_DB Table Name: table ewlc_tbl_client_dot11_oper_data OTD (ID/SRC): 0xa8cfb325ec1b97fe568aa1a0d792de71/0x00000000000 Table Type: ewlc_tbl_client_dot11_oper_data Table LUD: 74ed1eleac918e1b8c20fd04964fed91 Table Flag: Cursor-Enabled Num Records (Non shadow): 3 Num Shadow Records: 0 Num Pending-destroy Records: 0 Table Gen D1: 0 Ack'd Gen ID: 0 Ack'd Gen ID: 0 Cursors Enabled: Enabled Write Cursor Mode: Explicit Num Read Cursors: 1						
show wireless client udn				Mathad		
TAC Address AP Name T	ype in	State	Frococol	Method	VOTE	ODM-TD
90dd.5de7.f0c2 AP00A6.CA36.0414 W b49c.dt89.bba6 AP00A6.CA36.0414 W b65d.0aa0.47ec AP00A6.CA36.0414 W	ILAN 17 ILAN 17 ILAN 17	Run Run Run	11ac 11ac 11ac	MAB MAB MAB	Local Local Local	16762216 16715577 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.

<b>≡ Cisco</b> ISE		Operations · Troubleshoot
Diagnostic Tools Download	Logs Debug Wizard	
Debug Profile Configuration Debug Log Configuration	Node List	
	🖉 Edit 🛛 🖕 Reset to Default	
	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.

<b>≡ Cisco</b> ISE	Operations · Troubleshoot					
Diagnostic Tools Download	l Logs	Debug Wizard				
Debug Profile Configuration Debug Log Configuration		~	~			
	🖉 Edit	← Reset to Default				
		Component Name	Log Level	Description	Log file Name	
	0	sgtbinding	INFO	SGT binding	ise-psc.log	
	0	sphub	INFO	sp-hub log messages	sphub.log	
	0	sponsorportal	INFO	Sponsor portal debug messages	guest.log	
	0	sse-connector	INFO	SSE Connector related log messages	connector.log	
	0	swiss	INFO	Swiss protocol internal messages	ise-psc.log	
	0	sxp	INFO	SXP Listener messages	ise-psc.log	
	0	TC-NAC	INFO	TC-NAC log messages	irf.log	
	0	telemetry	INFO	Telemetry related log messages	sch.log	
	0	theshold-counter	INFO	Threshold Counters	counters.log	
	0	Trustsec	INFO	TrustSec related messages	ise-psc.log	
	0	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 app	lication 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: NonStringifiableExecutio	nContext, 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: NonStringifiableExecut	ionContext, 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: NonStringifiableExecu	tionContext, 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: NonStringifiableExecutio	nContext, 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: NonStringifiableExecut	ionContext, 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: NonStringifiableExecu	tionContext. 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.

E Cisco ISE		Operations · Troubleshoot		1 🔺 License Warning
Diagnostic Tools Download Logs	Debug Wizard			
Appliance node list	Support Bundle Debug Logs	lapse All		
	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.		Steps 11001 Received RADIUS Access-Request
Overview		11017 RADIUS created a new session Detected Host Lookup UseCase (Service-Type = Call Check (10))
Event	5200 Authentication succeeded	15049 Evaluating Policy Group 15008 Evaluating Service Selection Policy
Username	bill@	15041 Evaluating Identity Policy
Endpoint Id	AC:) ⊕	15048 Queried PIP - Normalised Radius.RadiusFlowType
Endpoint Profile	Annie-Device	22072 Selected identity source sequence - All_User_ID_Stores
		15013 Selected Identity Source - Internal Endpoints
Authentication Policy	Default >> MAB	24209 Looking up Endpoint in Internal Endpoints IDStore - bill@cdnac.com
Authonization Policy		24211 Found Endpoint in Internal Endpoints IDStore
Authorization Result	PermitAccess,UDN	22037 Authentication Passed
		15036 Evaluating Authorization Policy
		15016 Selected Authorization Profile - PermitAccess,UDN
Authentication Detail	s	15016 Selected Authorization Profile - PermitAccess, UDN
Source Timestamp	2023-08-30 00:44:22 303	15048 Queried PIP - UDN.Private-group-id
Received Timestamp	2023-08-30 00:44:22.303	Looking up Endpoint in Internal Endpoints IDStore - bill@cdnac.com
Policy Server	ISE-Public	24211 Found Endpoint in Internal Endpoints IDStore
Event	5200 Authentication succeeded	11002 Returned RADIUS Access-Accept
Username	bill@c	
User Type	Host	

## Successful authentication of an unregistered device:

Result		
UserName		
User-Name	10.000	
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.

Cisco Cisco (17.3.2020050	Welcome				
Q Search Menu Items			Interface	6	Services
			Logical		AireOS Config Translator
Dashboard			Ethernet		Application Visibility
			Wireless		Cloud Services
		끘	Layer2		Custom Application
Michael	ĺ.	000	Discovery Protocole		IOx
					mDNS
Configuration	>		VEAN		Multicast
~			414		NetFlow
Administration	>	®llı.	Radio Configurations		Python Sandbox
5			CleanAir		QoS
C Licensing			High Throughout		RA Throttle Policy
			Media Parameters		Tags & Profiles
Troubleshooting			Network		AP Join

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

Configuration - > Services	with a model of the model of t
Global Service Policy	mDNS Flex Profile
mDNS Gateway	ENABLED
Transport	ipv4
Active-Query Timer *	30
mDNS-AP Service Policy	default-mdns-service
	<u>Clear</u>

Con	iguratio	on▼ > Tags & F	Profiles - > WLAN	s					
+	Add	× Delete	Enable WLAN						
Numb	er of WL	ANs selected : 0							
	Status	Name	~	ID	~.	SSID	~.	Security	~
	O	Student-do_Glob	al_NF_bf4ccc47 💊	17		Student-dorm		[WPA2][PSK][AES	S],MAC Filtering
	۹ 1		10 🔻 items per page	9					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.

Edit WLAN			
A Changing WL	AN parameters while it is enabled will r	result in loss of connec	tivity for clients connected to it.
General Security Ad	vanced Add To Policy Tags		
Coverage Hole Detection		Universal Admin	
Aironet IE		Load Balance	
P2P Blocking Action	Disabled 🗸	Band Select	
Multicast Buffer	DISABLED	IP Source Guard	
Media Stream Multicast- direct		WMM Policy	Allowed
11ac MU-MIMO	✓	mDNS Mode	Gateway 🔻
Max Client Connections		Off Channel Scar	Bridging Gateway
		Defer Drierity	
Per WLAN	0		$\Box_3  \Box_4  \bigtriangledown_5$
Per AP Per WLAN	0		$\square_{6}$ $\square_{7}$
Per AP Radio Per WLAN	200	Scan Defer	100
11. DCC Transition Cunner	•		
<b>D</b> Cancel			Update & Apply to Device

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-configureand-troubleshoot-mdns-on-catal.html#toc-hld--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
	Everyone
	Anyone on the Same Network
~ <b>L</b>	Only People Sharing This Home
	Require Password O
	APPLE TV OPTIONS
	Also Allow Nearby to AirPlay O
	APPLE TV OPTIONS Also Allow Nearby to AirPlay
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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA