

User Defined Network

Prescriptive Deployment Guide

December, 2020

Contents

About this Guide	3
Define	4
Design	7
Deploy	15
Process: Pre-requisites	15
Process: Configuring Wireless settings for WLAN Deployment.	31
Process: Cisco UDN Cloud Authentication/SSO	39
Process 1: Azure AD and UDN Cloud	39
Process 2: Cloud Authentication with SAML and Microsoft ADFS	55
Process: Mobile App Customization	69
Process: UDN Workflow	72
Process: Adding devices and Guests to UDN.	77
Process: Assurance and Troubleshooting	86
Appendix A: Configuring mDNS Gateway	100
Appendix B: Randomized MAC Address	102
Appendix C: Disabling Airplay Discovery/Streaming via Bluetooth®	102
Feedback	103

About this Guide

This guide is intended to provide technical guidance to design, deploy and operate Cisco User Defined Network (UDN). It focuses on the steps to enable device level segmentation for 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 UDNs.

This guide contains four major sections:

The Define section defines problem being solved with Cisco UDN and provides information about how to plan for deployment, and other considerations.

The Design section discusses the interaction of the various solution components as well as providing the versions of software used in the solution.

The Deploy section provides information about various procedures to deploy the solution along with recommended practices.

The Operate section shows how to verify that the UDN components have been provisioned correctly.



Define

When on a home network, it's easy enough to use a streaming technology, such as Google Chromecast or Apple Airplay, to stream movies and TV shows. In a shared network environment, such as a school dormitory, it can be much harder to find your TV among all the other student's devices. This can also cause confusion and annoyance as students can accidentally stream to a device owned by a different student. This problem is not just limited to streaming to a TV but for any device using Link Local Multicast protocols.

Cisco UDN (User Defined Network) solves this problem by segmenting the user's devices while still being on the same SSID. Users will be given their own private UDN where only devices they register will be allowed to communicate with each other. This eliminates the problem above and creates a more secure network environment.

Users will be given access to the Cisco UDN application, available on the Google Play store or Apple App store, which will be used to register the devices MAC address before arriving at the shared network environment.

Tech tip

When deploying Cisco UDN, discovery and streaming is limited to registered devices within the UDN for wireless devices such as MacBooks, iPhones, and iPads. For the Apple TV, 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. Please refer to [Appendix C](#) for the procedure to disable AirPlay over Bluetooth if you would like to change this behavior.

Components

Cisco UDN Mobile Application

The Cisco UDN mobile application is used for users to create and register devices to their own personal UDN. By entering their devices' MAC addresses in the application, they register their device for use in that UDN. They can also register any streaming media players such as Apple TV or Amazon Fire TV as members of their UDN by adding their MAC addresses as well. Users may also invite guests into their UDN by sending an invite to the guest allowing them to register their device and allowing them to share devices.

The Cisco UDN Mobile Application is available for download on the Google Play Store and Apple App Store.

Cisco UDN Cloud

The Cisco UDN Cloud service serves as the communication broker between the Mobile App and the on-prem equipment required for the UDN service. The Cisco UDN Mobile App communicates with the Cisco UDN Cloud service and is used for UDN creation as well as registering mobile and other devices within the user's UDN. The Cloud then communicates this information back to the Cisco DNA Center on the customer's premise.

Identity Provider

The identity provider (IdP) is your organization's SSO service used for authentication. Presently Microsoft Azure AD and SAML are supported. SAML is supported with Shibboleth or Microsoft Active Directory Federated Services (ADFS). During the user authentication to the Cisco UDN Cloud using the UDN Mobile App, your SSO service is queried and the results returned. Upon successful authentication, the user is now able to create their UDN "Room" and register devices within.

Tech tip

The IdP discussed here is required for authentication and access to the Cisco UDN Cloud services. It may optionally be used but is not necessary for 802.1X network authentication to the wireless network if Active Directory or LDAP is already used as an internal identity source.

Cisco DNA Center

At the heart of the UDN solution automation is the Cisco DNA Center. UDN is enabled with a workflow that is launched from Cisco DNA Center for establishing trust between the on-premise Cisco DNA Center appliance and the Cisco UDN Cloud services as well as provisioning, and applying UDN specific information to both the Catalyst 9800 wireless controller and Cisco ISE, both required as part of the UDN solution.

In addition to its role in the UDN solution, Cisco DNA Center can optionally centrally manage major configuration and operations workflow areas.

- **Design**—Configures device global settings, network site profiles for physical device inventory, DNS, DHCP, IP addressing, software image repository and management, device templates, and user access.
- **Policy**—Defines business intent for provisioning into the network, including creation of virtual networks, assignment of endpoints to virtual networks, policy contract definitions for groups, and configures application policies.
- **Provision**—Provisions devices and adds them to inventory for management, supports Cisco Plug and Play, creates fabric domains, control plane nodes, border nodes, edge nodes, fabric wireless, Cisco Unified Wireless Network wireless, transit, and external connectivity.
- **Assurance**—Enables proactive monitoring and insights to confirm user experience meets configured intent, using network, client, and application health dashboards, issue management, and sensor-driven testing.
- **Platform**—Allows programmatic access to the network and system integration with third-party systems using APIs, using feature set bundles, configurations, a runtime dashboard, and a developer toolkit.

Tech tip

The Cisco UDN solution does not support fabric enabled wireless if in use as part of a Cisco SD-Access fabric.

Cisco Identity Service Engine (ISE)

Cisco ISE 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 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, it communicates the UDN-specific information required for UDN segmentation back to the wireless controller.

Catalyst 9800 Wireless LAN Controller

Built from the ground-up for intent-based networking and Cisco DNA, Cisco® Catalyst® 9800 Series Wireless Controllers are Cisco IOS® XE based and integrate the RF excellence of Cisco Aironet® access points, creating a best-in-class wireless experience for your evolving and growing organization. The 9800 Series is built on an open and programmable architecture with built-in security, streaming telemetry, and rich analytics.

Tech tip

The Cisco UDN solution only supports the Catalyst 9800 when running in local mode, Cisco Software Defined Access (SDA) is not supported if fabric enabled wireless has been deployed. Cisco UDN is supported if the wireless in an SD-Access fabric has been deployed as over the top using local mode; both control and data plane encapsulated in CAPWAP tunnel between the access point and Catalyst 9800 wireless controller.

Cisco Access Points

The Cisco UDN solution supports all Cisco Wave 2 access points, most notably the Cisco 1800, 2800, 3800, and 4800, as well as Cisco 9100 family of Wi-Fi 6 access points.

Design

This section discusses the solution architecture and how the various components interact with one another. Sample flows discussing the user creation of the UDN and device registration within their room are provided. Finally, the list of components and versions of software validated in this Prescriptive Deployment Guide (PDG) are provided.

Architecture

The following information provides an overview of the UDN solution including solution automation and communication flows for user device registration and subsequent connection to the UDN enabled wireless network. It is broken into two sections including the interaction and provisioning of the solution components and the device UDN registration and subsequent attachment to the wireless network.

Solution overview

The Cisco UDN solution incorporates both Cisco Cloud and onsite 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 UDNs. Cisco UDN cloud is used for UDN tenant creation, device registration, device de-registration, and UDN change/guest invite via the Cisco UDN Mobile App, The Cisco UDN on premise components include Cisco wireless networking using the Catalyst 9800 controller along with Wave 2 Cisco and Catalyst 9100 access points for network connectivity, Cisco ISE for network access control through RADIUS AAA and Cisco DNA Center for provisioning of the Cisco onsite components as well as communications with Cisco UDN Cloud for UDN specific information.

Cisco UDN Mobile App

In addition to cloud and on-premise infrastructure, the Cisco UDN Mobile App, available for both Android and iOS-based devices and downloadable from both the Google Play Store and the Apple AppStore, is used for UDN creation, device registration, and guest invitation. When first opening the application, the user will provide their credentials to gain access to the Cisco UDN service where all UDN creation and maintenance activities are performed. From the Cisco UDN Mobile App users can create their “Room” (UDN), register their mobile devices, register their multimedia devices, and invite/remove other guest devices.

Using the Cisco UDN Mobile App, users can register their devices while offsite or once they arrive on site. If the device is using MAC randomization, which is on by default on Android-based devices, off site registration will not be possible unless it is manually disabled on the device. Should it be undesirable to have the user disable MAC randomization, once on-site and attached to the UDN SSID, they will then be able to register their device.

Tech tip
MAC randomization, implemented on Android devices today, will also be implemented on Apple devices beginning with iOS 14.

Cisco UDN Cloud Service

Cisco UDN Cloud provides the services for the creation and maintenance of UDNs, As just described, the Cisco UDN mobile application is used by users to create and register devices to their own personal UDN. As users using the Cisco UDN Mobile App transparently access the Cisco UDN Cloud, it redirects the authentication requests to your single sign on (SSO service) such as Microsoft Azure AD or acts as a Security Assertion

Markup Language (SAML) 2.0 Service Provider (SP) redirecting authentication requests to an Identity Provider (IdP) such as Shibboleth or Microsoft Active Directory Federated Services (ADFS).

When using Microsoft Azure AD as your IdP, it is either necessary to duplicate the user information contained in Azure AD by manual creation in Cisco UDN Cloud or you can use Group attributes in Azure AD, by enabling Azure AD attribute mapping in Cisco UDN Cloud, eliminating the need to manually enter individual accounts.

Tech tip

Future testing will provide additional support for other SAML based identity access management (IAM) solutions such as Shibboleth. As the Cisco UDN Cloud service has been tested against the SAML 2.0 open standard, other vendors' products conforming to the standard should work fine with the cloud service.

When an end user registers his/her endpoint, the cloud service establishes a device-user mapping and generates the UDN ID associated with the user. Thus, it helps create the right user to device mapping. When the end user sends an invitation, the cloud service relays the invitation and keeps track of it to the guest end user. If a guest end user accepts an invitation to another UDN, the cloud service handles the change of UDN for the end user and retains the owner-device mapping as well as the necessary host UDN mapping. The cloud service also allows the admin to customize the look of the mobile app so it can represent the colors and logo of the organization. The cloud service then establishes communications via a Publisher/Subscriber relationship with your on-premise Cisco DNA Center appliance to communicate the UDN information to both Cisco ISE and the Cisco WLC.

Tech tip

The communications between the UDN Cloud and the on-site Cisco DNA Center presently scales to 30 registration/change events per second per tenant. Your entire organization/company is a tenant in the UDN Cloud.

Cisco DNA Center (on-premise)

Central to the UDN solution is Cisco DNA Center. The on-premise Cisco DNA Center is used for three main things:

- Automation of UDN on Catalyst 9800 and ISE
- Brokers communication between Cisco UDN Cloud UDN services and ISE
- Provides UDN assurance where endpoints can be viewed based on UDN values

For Automation, Cisco DNA Center provides a UDN Workflow for the administrator to configure the Catalyst 9800 wireless controller (WLC) and ISE quickly and easily. Additionally, the on-premise Cisco DNA Center communicates with its cloud counterpart, obtaining UDN creation, registration and change information. For assurance, Cisco DNA Center collects data from different products and provides a clear view of the dashboard showing the user's current device and its UDN association. It also provides information on other devices associated with the current UDN.

The on-premise Cisco DNA Center is responsible for provisioning the wireless controller and ISE with UDN specific information. Prior to running the Cisco UDN workflow at the on-premise Cisco DNAC, it will be necessary to perform a few tasks. These are:

1. Establish pxGrid integration between Cisco DNA Center and Cisco ISE for communication of UDN specific information such as UDN-ID, device MAC addresses.
2. Configure Cisco ISE as the RADIUS AAA server in Cisco DNA Center and creates a UDN Specific authorization profile the applying that to all existing Authentication policies in ISE.

3. Define up to three SSIDs that will be used for the UDN.
4. Discover and provision the Catalyst 9800 wireless controller at Cisco DNA Center.

Tech tip

At the present time, DNAC clustering is **not** supported. Support for DNAC clustering will be available in a future release of the 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 UDN solution:

1. Processes device registration and room assignment/change requests from Cisco UDN Cloud forwarded by the on-premise Cisco DNA Center and replicates this information across all ISE Policy Service Nodes in your deployment.
2. Interacts with the Catalyst 9800 controller in RADIUS authentication requests by retrieving UDN assignment for on-boarding end devices from its local database.
3. Upon successful authentication, sends a RADIUS response to the wireless controller containing three UDN-specific vendor specific attributes (VSA) 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 is no manual, UDN specific configuration required at ISE. All configuration is performed via the on-premise Cisco DNA Center and the Cisco UDN Cloud service. Upon provisioning by the on-premise Cisco DNA Center, a new UDN pxGrid service is added which allows both the on-premise Cisco DNA Center and the cloud service to communicate with ISE via REST APIs. ISE makes use of a new pxGrid “status” topic whenever UDN assignments are created, updated, or deleted.

Upon Cisco DNA Center provisioning of 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 is for UDN properties as to whether 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.

A new logging option, the UDN logging component, has also been established. In a distributed deployment, the Policy Administration Node (PAN) records all activity originating from both the on-premise and cloud instantiations of Cisco DNA Center as well as change of authorization (CoA) activity between ISE and the WLC including CoA responses. The Policy Service Node (PSN) shows run-time activity during device onboarding including UDN lookup results for device MAC address as well as any changes to the local Device-UDN cache when information is replicated from the PAN.

During Cisco DNA Center provisioning of ISE, a new Authorization (AuthZ) Profile is also created and will be automatically applied to all existing Authorization Policies as a condition in addition to any that may exist. This AuthZ profile makes use of RADIUS attributes from the wireless controller as a network access device to determine that both the originating wireless controller and the SSID that the onboarding device is joining are

UDN enabled before performing an actual UDN lookup. This minimizes the number of lookups required at ISE as devices authenticate throughout your network.

Tech tip

The Cisco UDN solution requires an ISE Plus license for every user device. Note that if randomized MAC addresses are enabled on a device, each MAC address will consume one license.

Catalyst 9800 wireless controller

The Cisco UDN solution only supports the IOS based Catalyst 9800 series physical and virtual wireless controllers; AireOS-based controllers and Catalyst 9800 embedded (switch or AP) controllers are not supported. With the introduction of UDN, SSIDs can be defined and dedicated to UDN in addition to those SSIDs dedicated to normal enterprise and guest wireless access. The UDN SSIDs can be configured for either 802.1x, MAC Auth Bypass (MAB), or pre-shared key (PSK). There are no restrictions associated with a mobile device that has been registered with a UDN via the Cisco UDN Mobile App, from accessing any other Enterprise SSID other than they will not have the same segmentation as when attached to the UDN. In the current implementation of UDN, only a single Catalyst 9800 controller or HA pair is supported. As a result, all devices and their UDNs are local to the WLC and the specific SSIDs associated with the UDN and roaming between controllers is not supported.

Prior to discovery and subsequent provisioning of the Catalyst 9800 WLC, it will be necessary to first define those SSIDs that will be used for UDN at the on-premise Cisco DNA Center. With the release of IOS-XE 17.3.1 for the WLC, additional UDN parameters have been added to the WLAN configuration, however, nothing needs to be defined at the WLC prior to execution of the Cisco DNA Center UDN Workflow at the on-premise Cisco DNA Center.

Once the configuration of the SSIDs has been completed at the on-premise Cisco DNA Center, a device discovery is launched to include the Catalyst 9800 in its inventory. After successful discovery of the wireless controller, provisioning of the controller is then launched from Cisco DNA Center. This will provision the WLC for communications with Cisco DNA Center. Once completed, it is at this point that the Cisco UDN Workflow, discussed previously, is launched at Cisco DNA Center for UDN specific configuration at the WLC and ISE. At this point, the UDN is fully functional.

The mDNS Gateway functionality of the Catalyst 9800 WLC is completely interoperable with the UDN functionality. The gateway functionality must be configured separately however, as automated provisioning of this functionality is not yet supported with the current release (2.1.1.3) of Cisco DNA Center. The mDNS Gateway functionality will be required for advertisement of Bonjour services across L3 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 WLC](#) and the [Cisco DNA Service for Bonjour Deployment Guide](#).

If a user's mobile device has been pre-registered off-site the device is all set to access the UDN SSID. If, however, due to MAC randomization they were unable to pre-register their device, they would join any SSID providing Internet access and register their 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 wireless network based on the security implemented.

Having registered to a UDN via the Cisco UDN Mobile App, as devices join the wireless UDN SSID, the wireless controller sends a RADIUS authentication request to ISE. In addition to the authentication method (802.1X, MAB, or PSK) based on 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 RADIUS UDN ID to the wireless controller, if the MAC address is found in the ISE database. The MAC Addresses are populated in the ISE identity database by the Cisco UDN Cloud service at the time of device registration using the Cisco UDN Mobile App. In the event there is no UDN information associated with a device from the cloud service, ISE will not relay any specific UDN info back to the WLC and the device will be granted access if the authentication was successful.

When joining the UDN SSID, if authentication is successful but the device is not registered to a UDN, the device will still gain access to the network and will be assigned a UDN-ID of zero. With UDN-ID of zero, that 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 endpoints associated with a specific UDN attach to the defined UDN SSID, the WLC will segment the various discovery protocol traffic such as mDNS, to only that UDN. This will work across all Wave 2 APs and Catalyst 9100 APs. 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 WLC.

Tech tip

When deploying Cisco UDN, discovery and streaming is limited to registered devices within the UDN for wireless devices such as MacBooks, iPhones, and iPads. For the Apple TV, 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. Please refer to Appendix C for the procedure to disable AirPlay over Bluetooth if you would like to change this behavior.

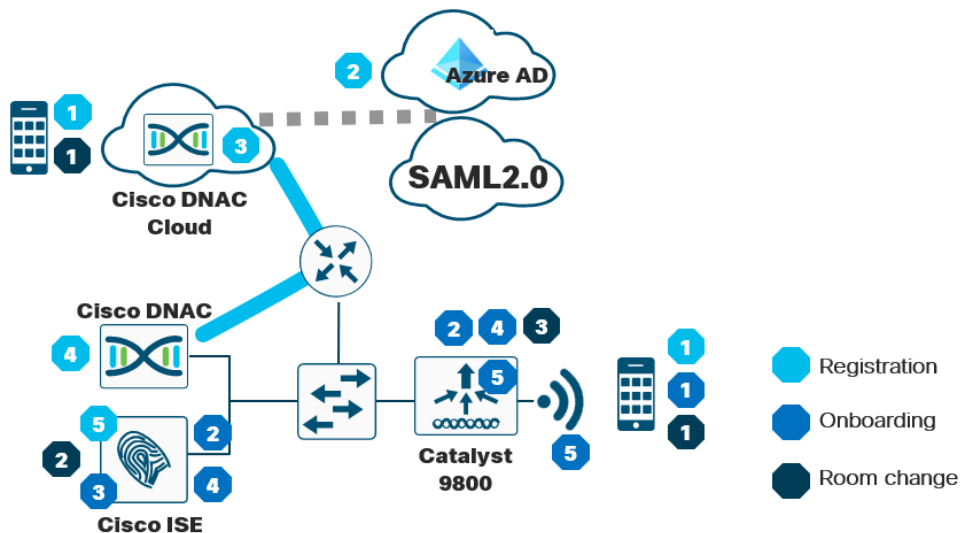
By default, unicast traffic is permitted between UDNs while multicast traffic such as mDNS is always contained within the UDN. The default behavior of allowing unicast communications between UDNs can be changed however, while running the UDN Workflow at Cisco DNA Center or in the wireless security policy associated with the UDN WLAN. With unicast blocking enabled, mobile devices can only communicate with other devices in that UDN or anything northbound, external to the wireless network.

Tech tip

Today the concept of a UDN shared device or services, such as a printer for example, accessible from all UDNs, is not supported. In the future there are plans to support this functionality.

Device registration and onboarding

The following diagram provides an overview of the communications during device registration and subsequently attaching to the wireless network.



Device registration flow

1. Using the Cisco UDN mobile app, the device registers with Cisco UDN Cloud.
2. The user is prompted for authentication credentials. Cisco UDN Cloud authenticates the user either against Azure AD or an Identity Provider (IDP) via SAML 2.0.
3. The UDN is created, and MAC address information for the devices that will be members of that UDN collected. This can be performed offsite, before the device attaches to the UDN if MAC randomization is disabled on the device, or onsite where MAC randomization can be enabled.
4. Upon device registration, Cisco DNAC Cloud communicates with the on-premise Cisco DNA Center which in turn relays registration information for the device including the UDN ID, UDN name and MAC Addresses entered.
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 brought onsite, the UDN SSID will be selected at the device. The SSID can be configured with either a pre-shared key (PSK), 802.1X, or MAB flow to authenticate the device.
2. A RADIUS authentication request is sent to ISE from the wireless controller.
3. ISE checks its database to perform a lookup of the MAC address in its UDN database.
4. Upon a successful lookup, ISE passes the RADIUS response back to the WLC along with vendor specific attributes identifying the
 - private-group-id - Used by the WLC to identify the UDN and isolating multicast and broadcast traffic between UDNs
 - private-group-name - Name of the room/UDN which the user defined
 - 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 UDN. Optionally, if selected to do so during wireless controller

provisioning from the Cisco DNA Center UD Workflow, unicast blocking between UDNs is enabled at the wireless controller.

Room change

1. The device either removes itself or is removed by the owner of the UDN
2. The ISE database is updated with device removal and the MAC address-UDN mapping is removed from the database.
3. ISE send a CoA to the wireless controller for device to re-authenticate.

Product Requirements

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

Device	Version
Cisco DNA Center	2.1.2.3 or later
ISE	2.7 Patch 2 or later with Plus or Apex licenses
Catalyst 9800 Wireless Lan Controller	IOS-XE 17.3.1with DNA Advantage licenses for APs
Cisco Wireless AP	IOS-XE 17.3.1 or later
Cisco UDN Mobile App	1.2
Cisco UDN Cloud	Not Applicable

Scale

The Following table provides scale numbers for the solution.

Device	Scale
Cisco Catalyst 9800-80	Up to 64,000 unique User Defined Networks per controller
Cisco Catalyst 9800-40	Up to 32,000 unique User Defined Networks per controller
Cisco Catalyst 9800-L	Up to 5,000 unique User Defined Networks per controller
Cisco Catalyst 9800-CL	10,000, 32,000 or 64,000 unique User Defined Networks per controller
Cisco ISE	Up to 2 Million Endpoints
Cisco UDN Cloud	30 Registration/Invite/De-Register events per second per Tenant (organization)

Deploy

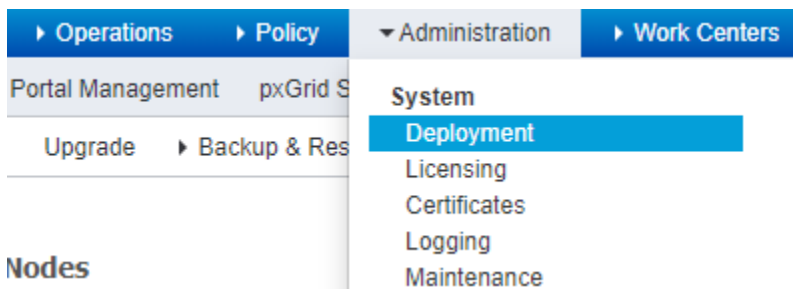
Process: Pre-requisites

This process will take you through the steps necessary to set up your devices to be UDN ready. These include Integrating ISE and Cisco DNA Center, discovery of the Catalyst 9800 Wireless Lan Controller, and creating Network Settings and a Site Hierarchy in Cisco DNA Center.

If you have already done these steps, you can skip ahead to Process: Configuring Wireless settings for WLAN Deployment.

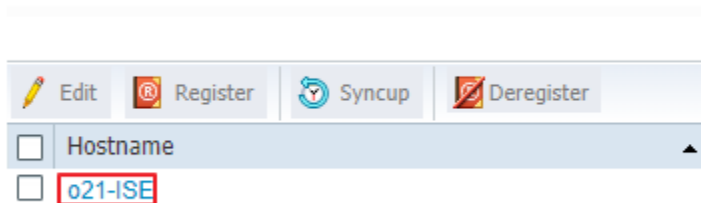
Procedure 1. ISE and Cisco DNA Center Integration

Step 1. Login to the Cisco ISE Primary Admin Node (PAN) and Navigate to **Administration>Deployment**



Step 2. Select the hostname of the ISE node.

Deployment Nodes



Step 3. Under General Setting, make sure the PxGrid checkbox is selected and hit Save.

Edit Node

General Settings Profiling Configuration

Hostname	o21-ISE
FQDN	o21-ISE.ciscodna.net
IP Address	10.4.168.50
Node Type	Identity Services Engine (ISE)

Role **STANDALONE**

Make Primary

☒ 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 ⓘ

Save

Reset

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

Step 5. Check **Automatically approve new certificate-based accounts** and click **Save**.

[All Clients](#)
[Web Clients](#)
[Capabilities](#)
[Live Log](#)
[Settings](#)

PxGrid Settings

☒ Automatically approve new certificate-based accounts

☐ Allow password based account creation

Connected via XMPP o21-ISE.ciscodna.net

Step 6. Navigate to **Administration>System>Setting>ERS Settings**.

Step 7. Select **Enable ERS for Read/Write** and click **Save**.

[Identity Services Engine](#)
[Home](#)
[Context Visibility](#)
[Operations](#)
[Policy](#)
[Administration](#)
[Work Centers](#)

[System](#)
[Identity Management](#)
[Network Resources](#)
[Device Portal Management](#)
[pxGrid Services](#)
[Feed Service](#)
[Threat Centric NAC](#)

[Deployment](#)
[Licensing](#)
[Certificates](#)
[Logging](#)
[Maintenance](#)
[Upgrade](#)
[Backup & Restore](#)
[Admin Access](#)
[Settings](#)

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
Posture
Profiling
Protocols
Proxy
SMTP Server
SMS Gateway
System Time
ERS Settings
Network Success Diagnostics
DHCP & DNS Services
Max Sessions
Light Data Distribution
Interactive Help

ERS Settings

General

External RESTful Services (ERS) is a REST API based on HTTPS over port 9060. The ERS service is disabled by default. An ISE Administrator with the "ERS-Admin" or "ERS-Operator" group assignment is required to use the API. For more information, please visit the ERS SDK page at: <https://10.4.168.50:9060/ers/sdk>

ERS Setting for Administration Node

☒ Enable ERS forRead/Write
 ☐ Disable ERS

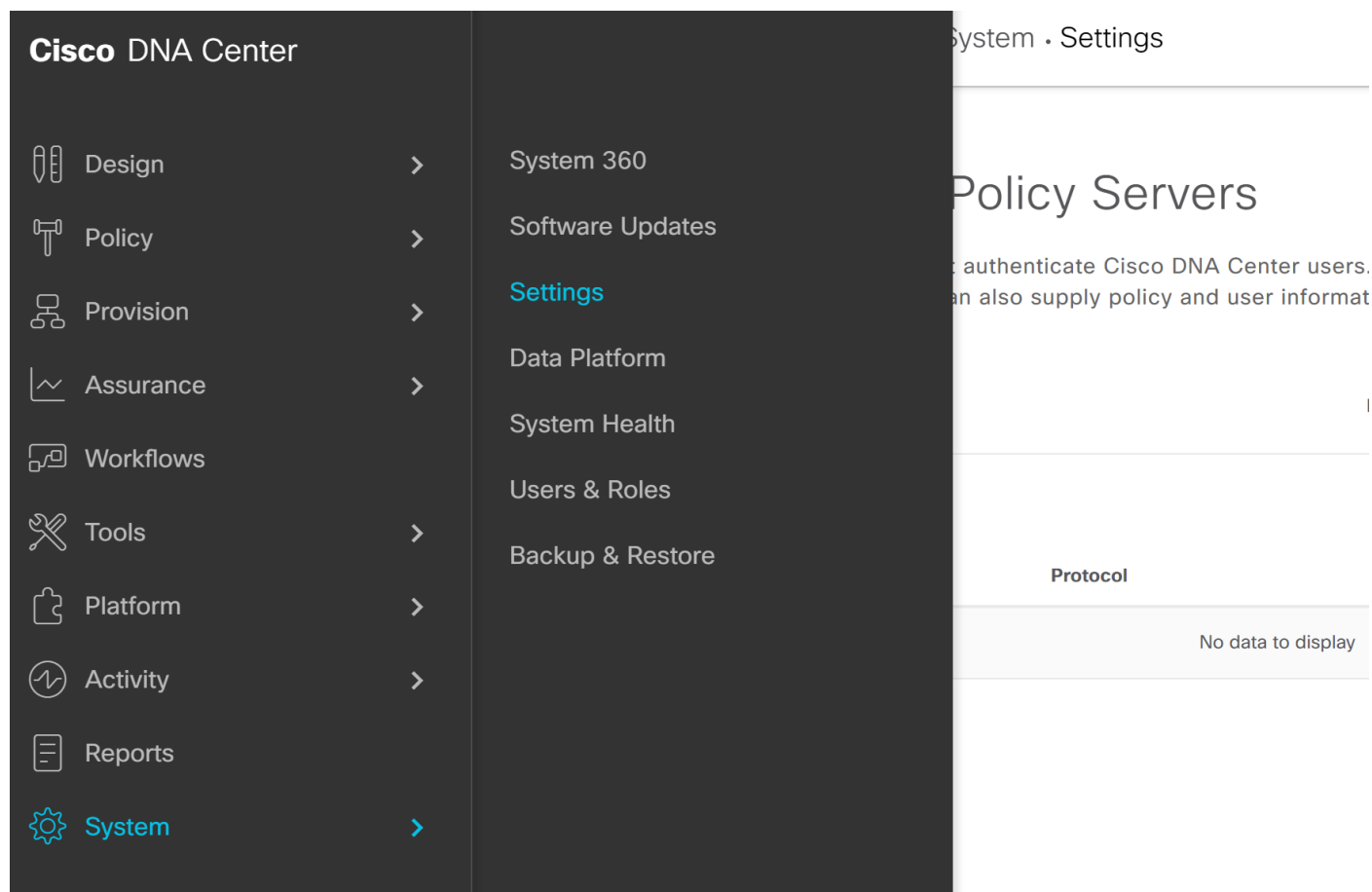
CSRF Check

☐ USE 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)

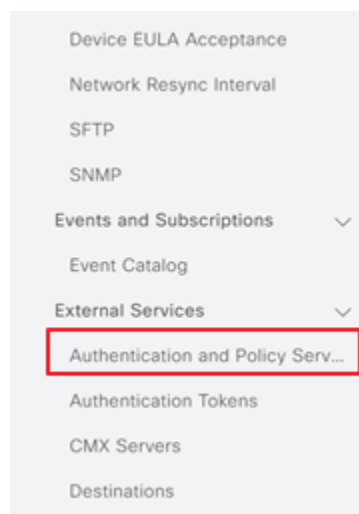
Tech tip

Ensure that CSRF Check is disabled otherwise you will not be able to establish a pxGrid connection between Cisco DNA Center and ISE.

Step 8. In Cisco DNA Center navigate to **System>Settings**.



Step 9. Scroll down on the left and select **Authentication and Policy Servers**.



Step 10. Enter the ISE PAN management IP address and enter a Shared Secret. The shared secret is just an arbitrary secret you define to be used for pxGrid communication between ISE and Cisco DNA Center.

Step 11. Click on the slider next to Cisco ISE Server.

Add AAA/ISE server



Server IP Address*

10.4.168.50

Shared Secret*

.....

[SHOW](#)



Cisco ISE Server

Step 12. Enter the ISE admin credentials.

Step 13. Enter the FQDN for the Cisco ISE server.

Tech tip

The FQDN must be reachable through DNS.



Cisco ISE Server

Username

admin

Password*

....

FQDN

o21-ISE.ciscodna.net

Step 14. Click **Save** and wait for the Status to go from In Progress to Active.

	IP Address	Protocol	Type	Status
	10.4.168.50	RADIUS	ISE	ACTIVE

Step 15. Also ensure that ISE is listed as **Available** in Cisco DNA Center System 360 by navigating from the Cisco DNAC menu to **System > System 360** and scroll down to **Externally Connected Systems**.

Externally Connected Systems

Identity Services Engine (ISE)

As of Jul 28, 2020 3:00 PM

PRIMARY	10.4.168.50	Available
PXGRID	10.4.168.50	Available

Step 16. In ISE navigate to **Administration>pxGrid Services** and under **All Clients**, see that your Cisco DNA Center subscriber name shows up.

All Clients					Web Clients	Capabilities	Live Log	Settings	Certificates	Permissions
Enable	Disable	Approve	Group	Decline	Delete	Refresh	Total Pending Approval(0) ▼			
<input type="checkbox"/>	Client Name		Description		Capabilities		Status			
<input type="checkbox"/>	▶ ise-bridge-o21-ise				Capabilities(0 Pub, 4 Sub)		Online (XMPP)			
<input type="checkbox"/>	▶ ise-admin-o21-ise				Capabilities(5 Pub, 2 Sub)		Online (XMPP)			
<input type="checkbox"/>	▶ ise-fanout-o21-ise				Capabilities(0 Pub, 0 Sub)		Online (XMPP)			
<input type="checkbox"/>	▶ ise-pubsub-o21-ise				Capabilities(0 Pub, 0 Sub)		Online (XMPP)			
<input type="checkbox"/>	▶ ise-mnt-o21-ise				Capabilities(2 Pub, 1 Sub)		Online (XMPP)			
<input type="checkbox"/>	▶ o21-ise				Capabilities(0 Pub, 0 Sub)		Offline (XMPP)			
<input type="checkbox"/>	▶ pxgrid_client_1591847592_dnac_ndp				Capabilities(0 Pub, 0 Sub)		Offline (XMPP)			
<input type="checkbox"/>	▶ pxgrid_client_1591847592				Capabilities(0 Pub, 0 Sub)		Offline (XMPP)			

Procedure 2. Catalyst 9800 Wireless Lan Controller Discovery

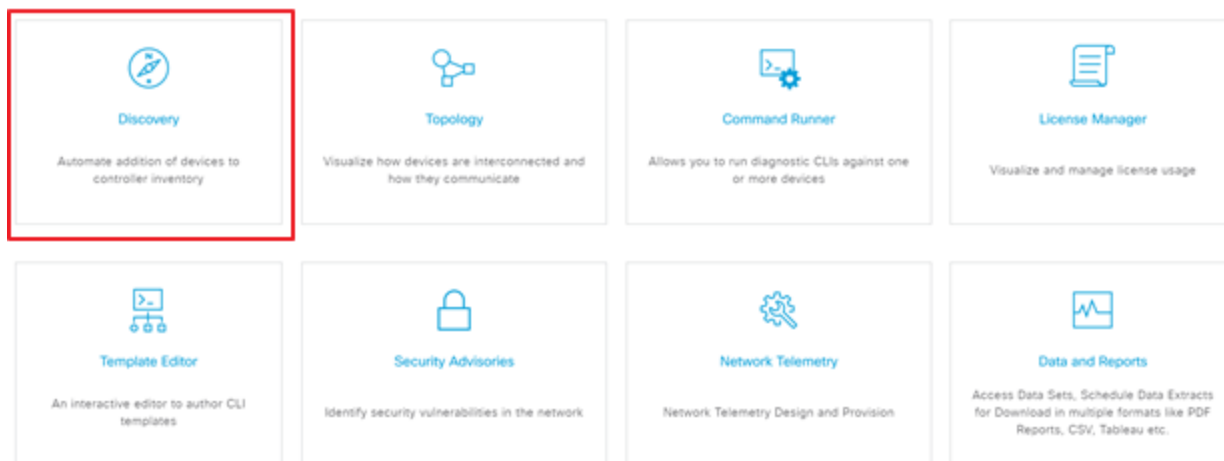
In this procedure we will go through the steps necessary to bring the Catalyst 9800 WLC into Cisco DNA Center's inventory.

Step 1. Login to Cisco DNA Center and select **Discovery** in the Tools section at the bottom of the homepage.

Tech tip

The Catalyst 9800 must only have the initial, Day 0 configuration for IP reachability, SNMP, and SSH/Telnet. Any brownfield wireless configuration including SSID, network, or VLAN configuration will cause issues with Cisco DNA Center provisioning.

Tools



Step 2. Click **Add Discovery**.



Device Controllability is **Enabled**.

Step 3. Add a name for this discovery under **Discovery Name**.

Step 4. Under **Discovery Type** select **IP Address/Range** and in the **From - To** section enter the Management IP for the Catalyst 9800 WLC.

Tech tip

Cisco Wireless Lan Controllers must be discovered using the Management IP. If not Wireless Controller 360 and AP 360 pages will not display data.

Step 5. Under **Preferred Management**, select one of the following options.


- **None:** Allows the device to use any of its IP addresses.
- **Use Loopback:** Specify the device's loopback interface as the management IP.

New Discovery

Discovery Name*

WLC

^ IP ADDRESS/RANGE *

Discovery Type 

☐ CDP ☒ IP Address/Range ☐ LLDP

From* 
10.4.146.5

To* 
- 10.4.146.5



Preferred Management IP 

☒ None ☐ UseLoopBack

Step 6. Expand the Credentials section and click **Add Credentials**.

Preferred Management IP 

☒ None ☐ UseLoopBack

^ CREDENTIALS *

 At least one CLI credential and one SNMP credential are required.

 Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers.

 GLOBAL  Task-specific

 [Add Credentials](#)

CLI

SNMPv2c Read

No credentials to display

No credentials to display

Step 7. Under the CLI section enter the credentials needed to access the CLI of the device and click **Save**.

Add Credentials



CLI

SNMPv2c

SNMPv3

SNMP
PROPERTIES

HTTP(S)

NETCONF

Name/Description*

DNA

Username*

dna

Password*

.....



Enable Password

.....



☐ Save as global settings

Settings will be used for this specific Discovery **only**

Reset

Save

Tech tip

Do not use "admin" as the username for your device CLI credentials. If you do, this can result in you not being able to login to your devices.

Step 8. Next add the SNMP credentials that will be used to connect to the WLC.

Step 9. Click **NETCONF**, leave the default port of 830 and click Save.

Add Credentials



CLI

SNMPv2c

SNMPv3

SNMP
PROPERTIES

HTTP(S)

NETCONF

Port 

830

☐ Save as global settings

Settings will be used for this specific Discovery **only**

Reset

Save

Step 10. Exit out of the **Add Credentials** menu by clicking the **X** at the top right corner.

Step 11. Check to make sure all your credentials are set by checking the blue slider indicators and click **Discover**.

New Discovery ← Back to Dashboard

Discovery Name*

WLC

☒ dna | DNA

☒ RO

SNMPv2c Write

☒ RW

SNMPv3

No credentials to display

HTTP(S) Read

No credentials to display

HTTP(S) Write

No credentials to display

NETCONF

☒ 830

fig changes will be made on network devices during associated to a site. [Learn More](#) | [Disable](#)

Reset

Discover

Step 12. After a few moments you should see your device discovered, check the status indicators to make sure everything was discovered correctly.

Filter

History ▾

IP Address	Device Name	Status	ICMP ▲	SNMP	CLI	NETCONF	⋮
10.4.146.5	o21-wlc	✓	✓	✓	✓	✓	

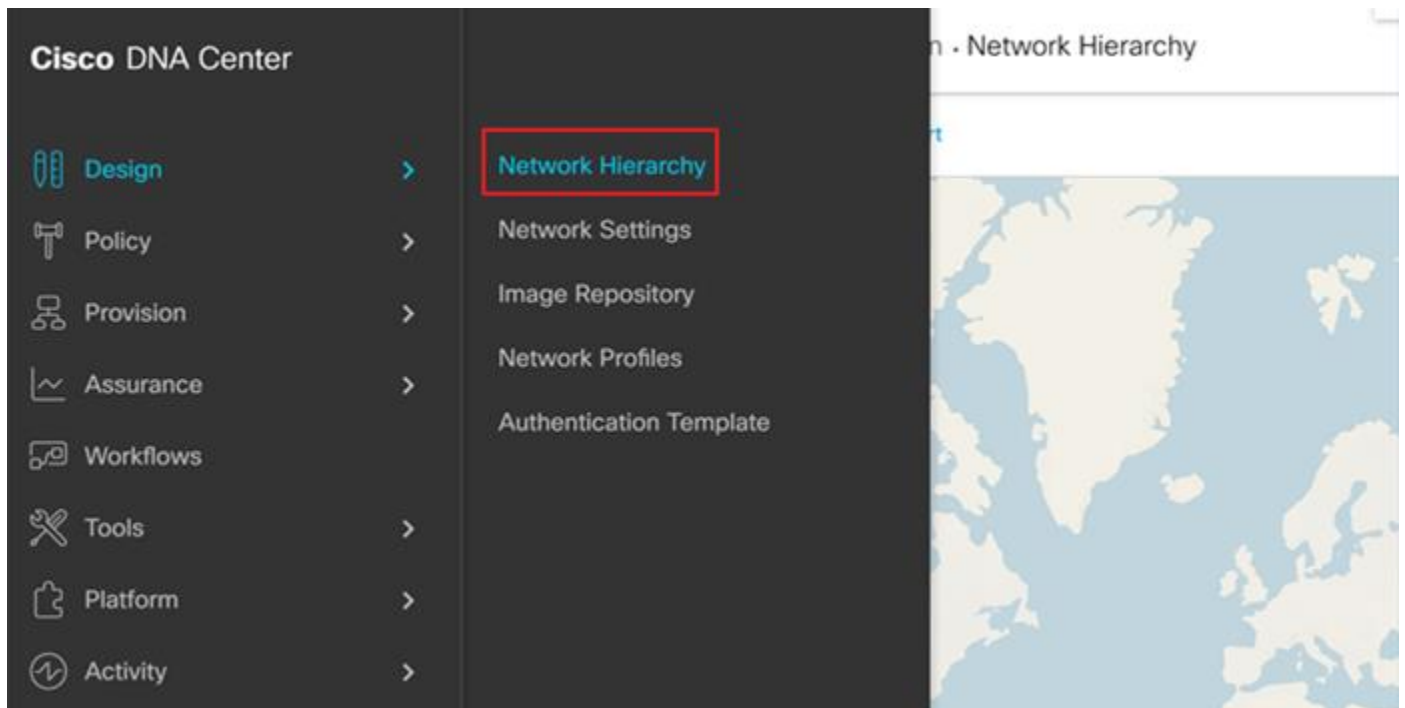
Step 13. Navigate to **Provision>Inventory** and you should now see your WLC as well as any APs connected to the controller in your inventory.

EQ Find Hierarchy		DEVICES (3)					
Global		FOCUS: Inventory					
Unassigned Devices		Filter Add Device Tag Device Actions Take a Tour					
RTP							
	Device Name	IP Address	Device Family	Reachability	Health Score	Site	MAC Address
	AP00A6.CA36.0414	10.118.43.68	Unified AP	Reachable	10	.../RTP-1/RTP-1-1	00:d7:8f:c9:38:40
	AP7872.5DED.CD34	10.4.146.22	Unified AP	Reachable	10	.../RTP-1/RTP-1-1	78:72:5d:ee:65:60
	o21-wlc	10.4.146.5	Wireless Controller	Reachable	10	.../RTP/RTP-1	00:1e:f6:75:5e:00

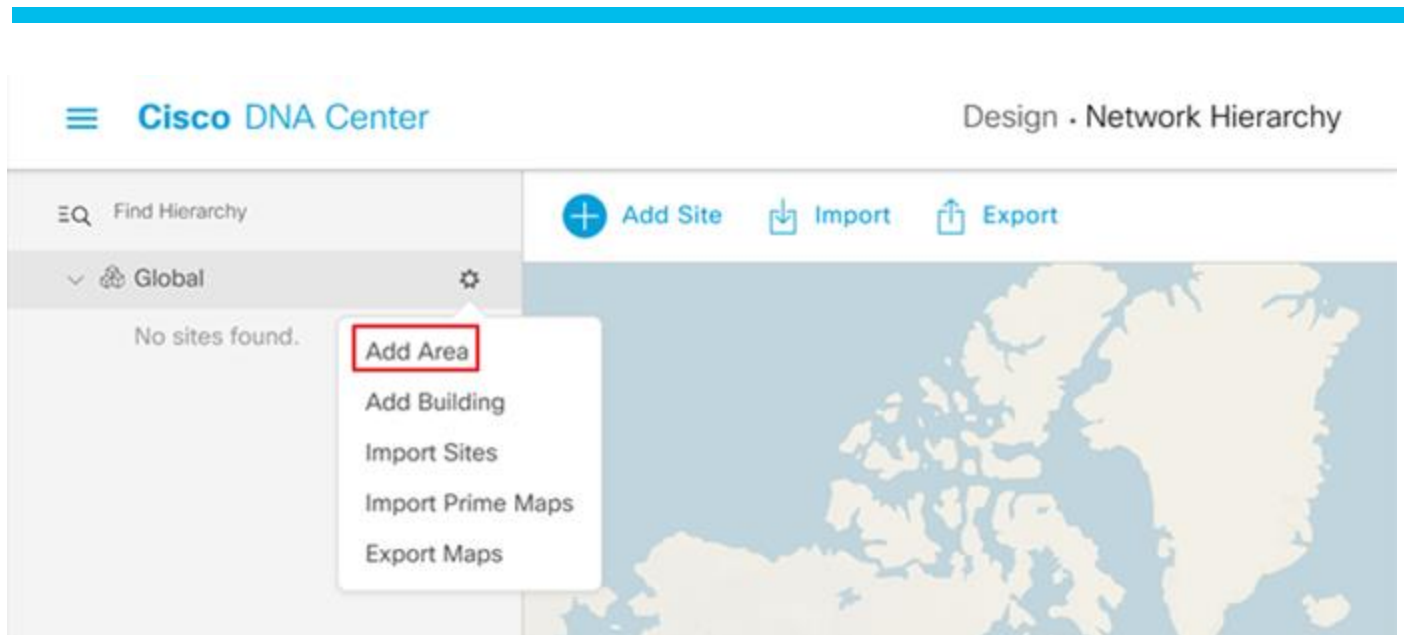
Procedure 3. Creating a Site Hierarchy

Cisco DNA Center uses a **Network Hierarchy** of areas that contain sub-areas of buildings and floors. Devices are assigned to these buildings or floors and will then be provisioned depending on the **Network Settings** configured for that level.

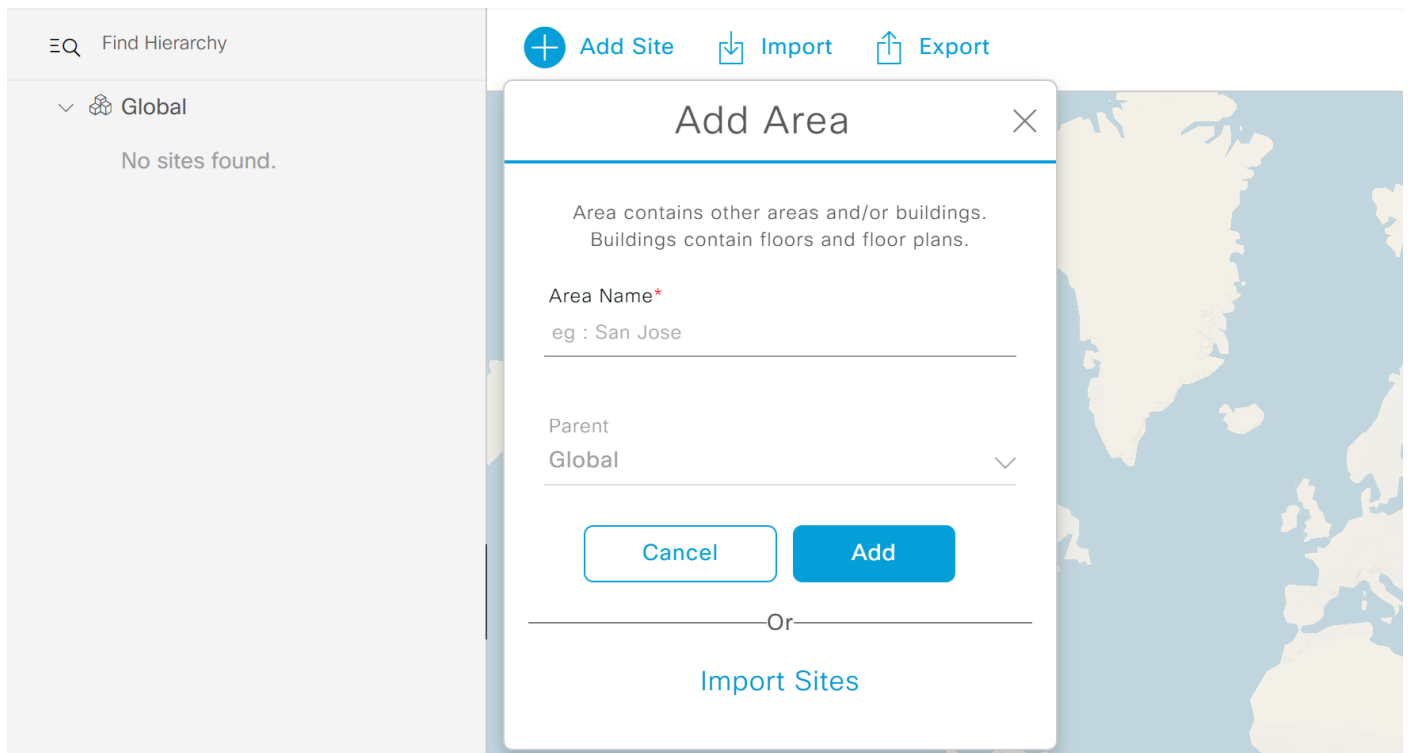
Step 1. In Cisco DNA Center, navigate to **Designs >Network Hierarchy**.



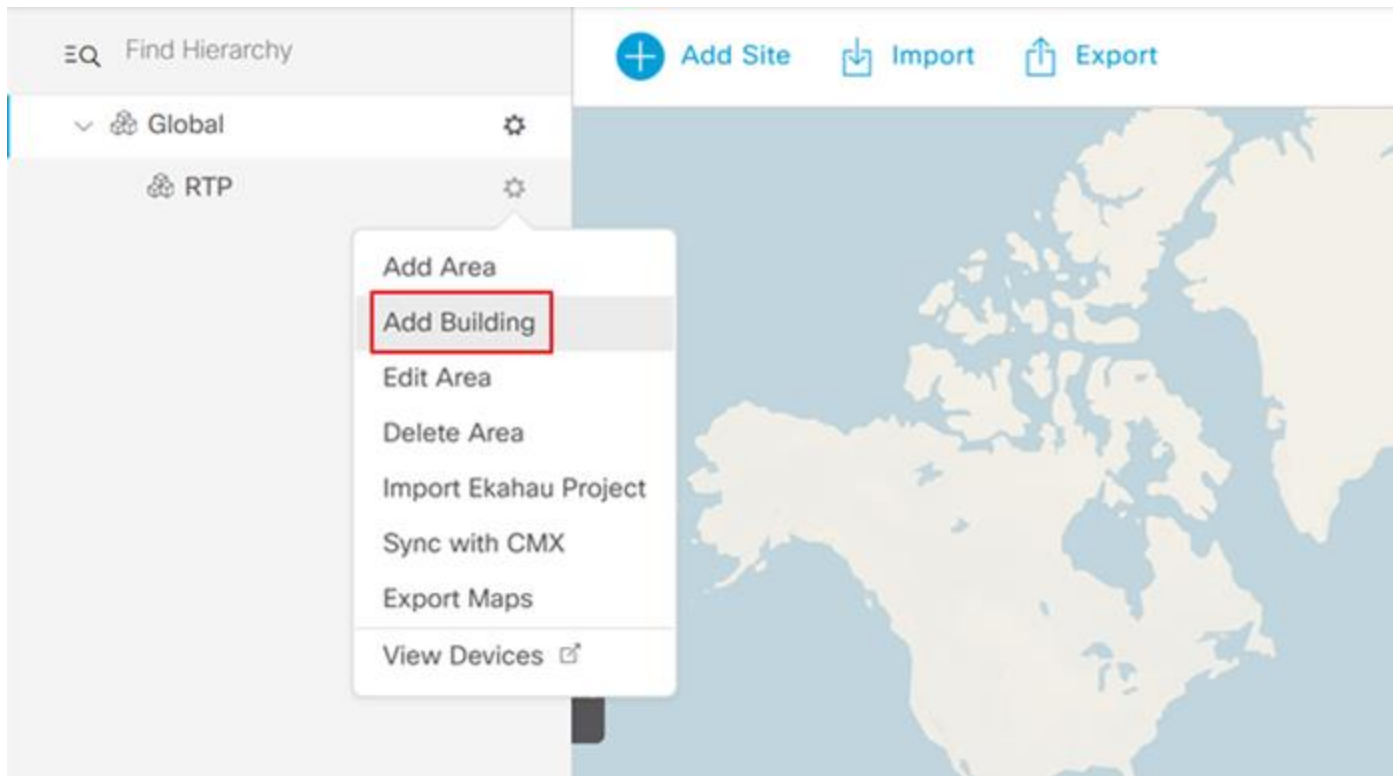
Step 2. Click the cog wheel next to Global and select **Add Area**.



Step 3. In the resulting pop-up enter your **Area Name** and click **Add**.



Step 4. Next to the newly created Area, click the cog wheel and select **Add Building**.



Step 5. In the resulting pop-up enter the building name and address of your building, this will fill in the Latitude and Longitude automatically.

Add Building

×

Area contains other areas and/or buildings. Buildings contain floors and floor plans.

Building Name*

RTP-1

Parent

RTP | Global/

▼

Address ⓘ

Kit Creek Road, Morrisville, North Carolina 27

Latitude*

35.855205

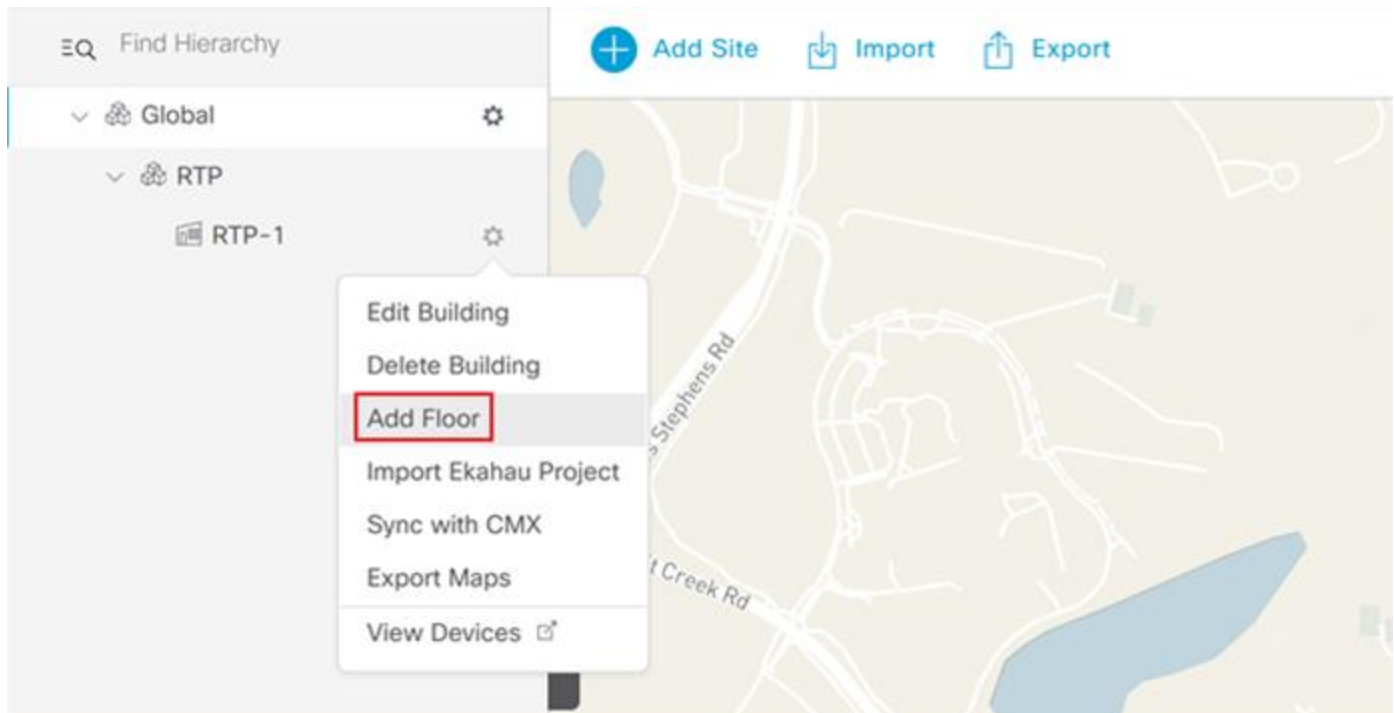
Longitude*

-78.875495

Cancel

Add

Step 6. Next to the newly added building, click the cog wheel and select **Add Floor**.



Step 7. Enter a **Floor Name** and click **Add**. Optionally, upload a floor plan.

Add Floor
×

Floor Name *
RTP-1-1

Parent
RTP-1

Type (RF Model)
Cubes And Walled Offices

Floor Image

Drag floor plan here
or
Upload file

(Supported formats DXF, DWG , JPG, GIF, PNG)

☒ Width (ft)
☐ Length (ft)
Height (ft)

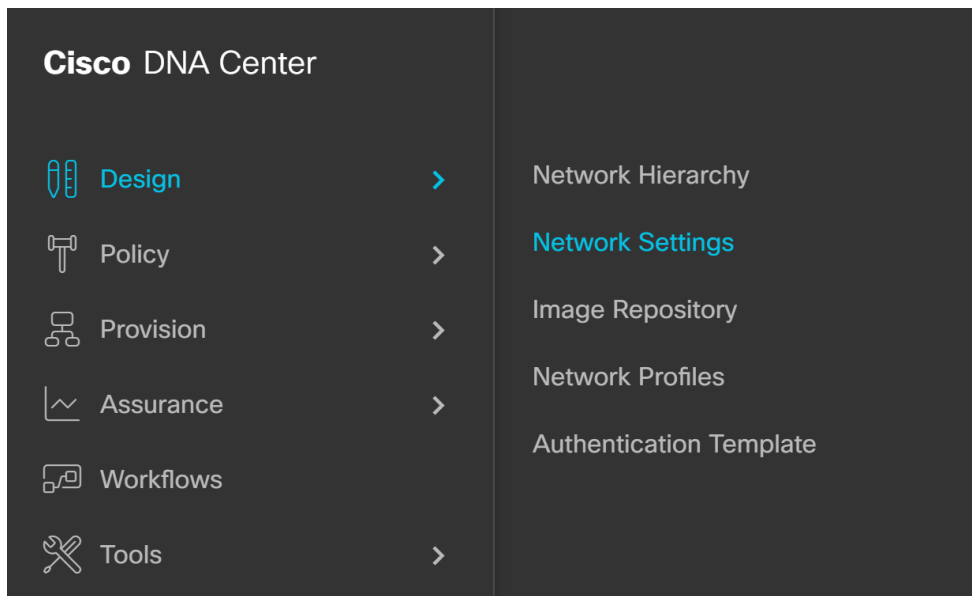
100
100
10

Cancel
Add

Step 8. Repeat these steps for any additional Sites, Buildings, or Floors in your environment.

Procedure 4. Creating Network Settings

Step 1. In Cisco DNA Center navigate to **Design>Network Settings>Network**.



Design • Network Settings

Wireless Telemetry

and NTP using the "Add Servers" link. Or
by using these settings.

Step 2. Click Add Servers and Select **AAA and NTP** and click **OK**.

Add Servers ×

☒ AAA
☐ Netflow Collector
☒ NTP

Cancel OK

Step 3. Under AAA server select the **Client/Endpoint** check box and in the drop down select the IP address for your ISE server.

Setup network properties like AAA and NTP using the "Add Servers" link. Once devices are discovered, DNA Center will deploy using these settings.

AAA Server

☐ Network ☒ Client/Endpoint

CLIENT/ENDPOINT

Servers ☒ ISE ☐ AAA

Protocol ☒ RADIUS ☐ TACACS

Client/Endpoint 10.4.168.50 × ▼

IP Address (Primary) 10.4.168.50 × ▼

Step 4. Scroll down and enter the information for DNS and DHCP servers.

DHCP Server

DHCP

10.4.49.10



Supports both IPv4 and IPv6

DNS Server

Domain Name

ciscodna.net

Primary

10.4.49.10



Supports both IPv4 and IPv6

Step 5. Enter the information for the network NTP server and click **Save**.

NTP Server

 NTP

10.4.0.1

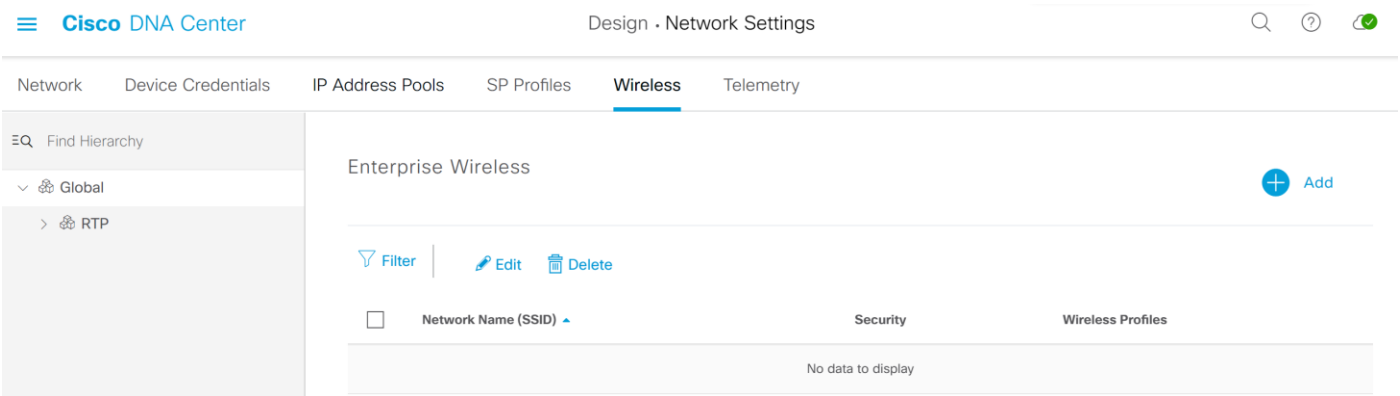


Process: Configuring Wireless settings for WLAN Deployment.

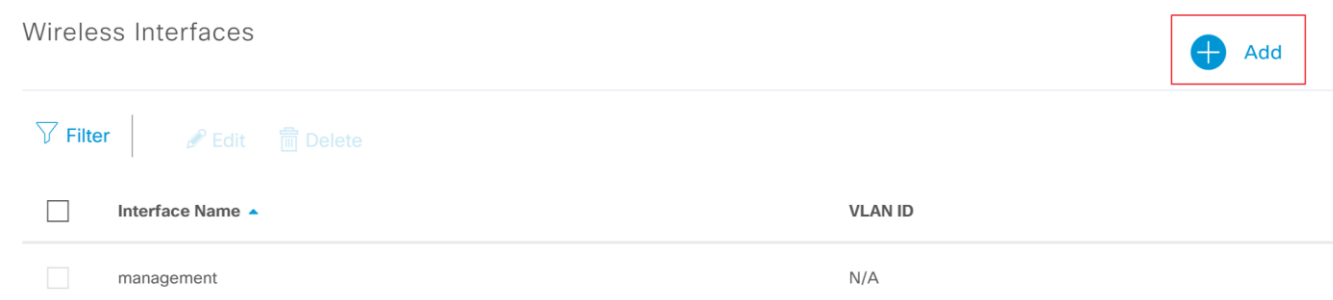
Procedure 1. Configure Wireless Interfaces

Before we configure the SSID, we must first configure the interface the WLAN traffic will be dumped off from the Catalyst 9800 WLC.

Step 1. In Cisco DNA Center, Navigate to **Design>Network Settings>Wireless**.



Step 2. At the Global level, click **Add** next to **Wireless Interfaces**.






Step 3. In the Create a Wireless Interface side panel enter the **Interface Name** and the **VLAN ID** for the corresponding VLAN on the network and click **Save**.

Tech tip

This will be the VLAN the wireless traffic is dumped off from the Catalyst 9800 WLC.

Step 4. You should now see your newly created interface below the **Wireless Interfaces** section.

Wireless Interfaces

 Filter  Edit  Delete		
<input type="checkbox"/>	Interface Name ▲	VLAN ID
<input type="checkbox"/>	management	N/A
<input type="checkbox"/>	Student	45

Procedure 2. Configuring the Wireless Networks

In this section we will be creating the Wireless SSID to be used for UDN. The WLAN in this example makes use of a PSK.

Tech tip

Cisco DNA Center must be used to create the wireless SSIDs on the Catalyst 9800 wireless controller. Issues with both UDN creation and telemetry will ensue if the SSID is created through the WLC user interface and not at Cisco DNA Center. Editing the WLC SSID from the WLC UI is fine after initial creation.

Step 1. In Cisco DNA Center, navigate to **Design>Network Settings>Wireless** and click **Add** next to **Enterprise Wireless**.

Enterprise Wireless



 Filter |  Edit  Delete

<input type="checkbox"/>	Network Name (SSID) ▲	Security	Wireless Profiles
--------------------------	-----------------------	----------	-------------------

Step 2. This will bring up the **Create an Enterprise Wireless Network** workflow.

Step 3. Name your Wireless Network and select your level of security. For this guide we will be using **WPA2 Personal**.

Step 4. Check the box next to **Mac Filtering**. When configuring WPA2 Enterprise with 802.1X MAC filtering should not be enabled.

Wireless Network Name(SSID)*

Student-dorm

Type Of Enterprise Network *

☒ Voice and Data

☐ Data only

Wireless Option

☒ Dual band operation (2.4GHz and 5GHz)

☐ Dual band operation with band select

☐ 5GHz only

☐ 2.4GHz only

SSID STATE

Admin Status:



Broadcast SSID:



Level Of Security *

☐ Enterprise ☒ Personal ☐ Open Secured

☐ Open

☒ WPA2 ☐ WPA3

More secure

A password (Pre-Shared Key PSK with WPA2 encryption) is needed to access the wireless network.

WPA3 feature is supported for Wireless Controller version 8.10 & above, For Catalyst 9800 Controllers version 16.12 & above.

☐ Fast Lane

☒ Mac Filtering

Pass Phrase*

.....

[SHOW](#)

Tech tip

Enabling MAC Filtering will not be needed for UDN in Cisco DNA Center 2.1.1.3 as it will automatically be configured during the UDN Workflow.

Step 5. When finished click Next, this will bring up the **Wireless Profile** page.

Step 6. Name the wireless profile and under **Fabric** select **No**.

Step 7. Under **Select Interface**, choose the interface created in the previous steps.

Create an Enterprise Wireless Network

1

Enterprise Wireless Network

2

Wireless Profiles

Wireless Profile Name *

dorm

Fabric

☐ Yes ☒ No

Select Interface

Student



☐ Flex Connect Local Switching

Sites 0 sites.

Step 8. Click **Sites** and in the resulting pop-up select the sites at which you want to deploy this SSID.

Sites

Choose a site

☐ Global (1)

☒ RTP (1)

☒ RTP-1 (1)

☒ RTP-1-1

Step 9. When done click **Finish**. You should now see your new wireless network under **Enterprise Wireless**.

Enterprise Wireless

Filter | Edit Delete

<input type="checkbox"/>	Network Name (SSID) ▲	Security	Wireless Profiles
<input type="checkbox"/>	Student-dorm	wpa2_personal	dorm

Procedure 3. Provision the WLC

In this section, we will now push the configuration down to the Catalyst 9800 WLC.

Step 1. In Cisco DNA Center navigate to **Provision>Inventory**.

Step 2. Click the check box next to your WLC and under **Actions** select **Provision>Provision Device**.

DEVICES (1) Global > RTP Take a Tour

FOCUS: **Inventory** ▾

DEVICE TYPE **All** Routers Switches APs WLCs REACHABILITY **All** Reachable Unreachable

Filter | [+ Add Device](#) [Tag Device](#) **Actions** ▾ 1 Selected Last updated: 10:19 AM

<input checked="" type="checkbox"/>	Device Name ▴	IP Address	Support Type	Site	Reachability	MAC Address	Device Role	Info
<input checked="" type="checkbox"/>	o21-wlc	10.4.146.5	Support			00:1e:f6:75:5e:00	ACCESS	17

Inventory >

Software Image >

Provision >

Device Replacement >

Others >

Assign Device to Site

Provision Device

LAN Automation

LAN Automation Status

Learn Device Config

Configure WLC HA

Step 3. In the resulting pop-up click **Choose a Site**, then select where you would like to assign the WLC and click **Save** and **Next**.

Choose a site ×

Find Hierarchy

Global (1)

RTP (1)

RTP-1 (1)

RTP-1-1

Step 4. In the Configuration screen double check to make sure everything looks correct and click **Next**.

Serial Number

9F55JE5UJLN

Devices

o21-wlc.ciscodna.net

WLC Role

☒ Active Main WLC ⓘ

☐ Guest Anchor

Managing 1 Primary location(s)

Select Secondary Managed AP Locations

Assign Interface

Interface Name	VLAN ID
Student	45

Show 10 entries Showing 1 - 1 of 1

Rolling AP Upgrade

☐ Enable

AP Reboot Percentage

25

ⓘ

Mobility Group

Name default [Configure](#)

Step 5. Hit **Next** on both the Model Configuration and Advanced Configuration pages.

Step 6. On the summary page double check your configuration, when finished click **Deploy**.

1

Assign Site

2

Configuration

3

Model Configuration

4

Advanced Configuration

5

Summary

o21-wlc.ciscodna.net

Device Details

Device Name:

Platform Id:

Device IP:

Device Location:

Device Role:

o21-wlc.ciscodna.net

C9800-CL-K9

10.4.146.5

Global/RTP/RTP-6/RTP-6-1

Active Main WLC

Network Setting

NTP Server:

AAA Network ISE Server:

AAA Network Primary Server:

AAA Client ISE Server:

AAA Client Primary Server:

DHCP Server:

DNS Domain Name:

DNS Primary Server:

10.4.0.1

10.4.168.50

10.4.168.50

10.4.168.50

10.4.168.50

10.4.49.10

ciscodna.net

10.4.49.10

SSID (dorm)

Name:

Type:

Security:

Fast Transition:

Traffic Type:

Fabric Enabled:

Fast Lane enabled:

Mac Filtering Enabled:

Flex Connect enabled:

Broadcast Enabled:

Admin Status:

Wireless Option:

Session Timeout (in sec)

Student-dorm

Enterprise

wpa2_personal

Adaptive

Voice + Data

No

No

Yes

No

Yes

Enabled

Dual band operation (2.4GHz and 5GHz)

1800

Procedure 4. Provisioning of the APs

Step 1. Navigate to **Provision>Inventory** in Cisco DNA Center.

Step 2. Any APs connected to the WLC will show up in inventory.

Step 3. Select the APs you would like to provision then under Actions select **Provision>Provision Device**.

DEVICES (3)

FOCUS: **Inventory** ▾

Filter | **Add Device** | Tag Device | Actions ▾ ① | Take a Tour | 2 Selected

<input type="checkbox"/>	Device Name ▴	IP	Reachability	Health Score
<input checked="" type="checkbox"/>	AP00A6.CA36.0414	1	Reachable	10
<input checked="" type="checkbox"/>	AP7872.5DED.CD34	1		10
<input type="checkbox"/>	o21-wlc.ciscodna.net	1		10

Inventory >
Software Image >
Provision >
Telemetry >
Device Replacement >
Others >

Assign Device to Site
Provision Device
LAN Automation
LAN Automation Status
Learn Device Config
Configure WLC HA

Step 4. Select the floor you would like to deploy for each AP and click **Next**.

1 Assign Site
2 Configuration
3 Summary

Serial Number
FCW2036P0Z3

Devices
AP00A6.CA36.0414

Global/RTP/RTP-6/RTP-6-1 ×

FCW2224NZM9

AP7872.5DED.CD34

Global/RTP/RTP-6/RTP-6-1 ×

☐ Apply to All

Step 5. Select the RF profile to be used by each AP and click **Next**.

1 Assign Site
2 **Configuration**
3 Summary

Serial Number	Device Name	RF Profile
FCW2036P0Z3	AP00A6.CA36.0414	TYPICAL ▾
		<input type="checkbox"/> Apply to All
FCW2224NZM9	AP7872.5DED.CD34	TYPICAL ▾

Step 6. On the summary page, doublecheck the configuration and click **Deploy**.

1

Assign Site

2

Configuration

3

Summary

AP00A6.CA36.0414

AP7872.5DED.CD34

Device Details

Device Name:

Serial Number:

Mac Address:

Device Location:

RF Profile:

Default Profile:

Radio Type:

Channel Width:

2.4GHz/5GHz Data Rates(In Mbps):

AP00A6.CA36.0414

FCW2036P0Z3

00:d7:8f:c9:38:40

Global/RTP/RTP-6/RTP-6-1

TYPICAL

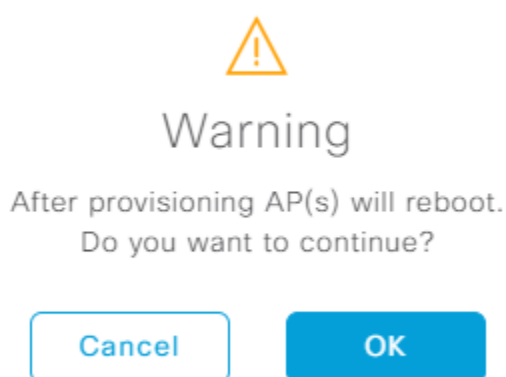
No

2.4GHz/5GHz

20 MHz

9,12,18,24,36,48,54/6,9,12,18,24,36,48,54

Step 7. Click **OK** on the warning saying the APs will reboot.



Process: Cisco UDN Cloud Authentication/SSO

Authentication for the Cisco Mobile App is performed via Single Sign On (SSO) using an external Identity Provider. The IdP can either be Azure AD or a SAML 2.0 enabled service. At the present time only Shibboleth, Microsoft Azure AD, or Microsoft ADFS have been validated using SAML 2.0. The following processes will be provided showing you the use of Azure AD or the use of SAML 2.0 in conjunction with Microsoft ADFS; one of these two authentication methods can be selected:

- Process 1 Microsoft Azure AD/OpenID protocol
- Process 2 Microsoft ADFS/SAML 2.0 protocol

Shibboleth and Azure AD are two other options when using SAML, but they will not be covered here. Even though not covered the Cisco UDN Cloud configuration will be the same with the exception that the Domain and Metadata URL will obviously be unique.

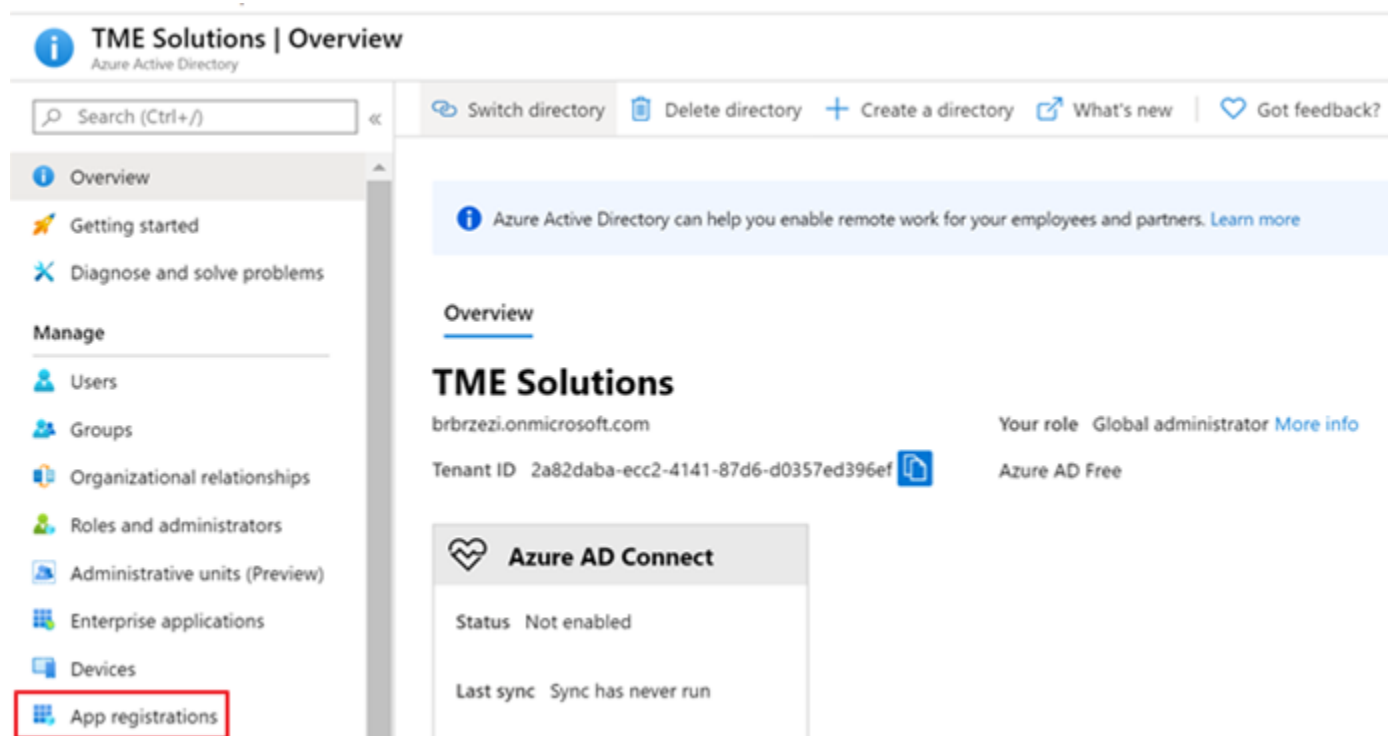
Process 1: Azure AD and UDN Cloud

This process will take you through the steps for creating a tenant in the UDN cloud as well as the corresponding Microsoft Azure AD configuration for use with the OpenID protocol. UDN users must be defined in both Azure AD as well as in Cisco UDN Cloud. Within this process, we will show two procedures. The first procedure will make use of Azure AD group attributes such that manual user creation is not required at Cisco UDN Cloud. As a member of a specific group in Azure AD, the user will be authenticated, and by virtue of that group attribute being matched, the user identity will be created in DNA Center Cloud automatically. The second is the manual

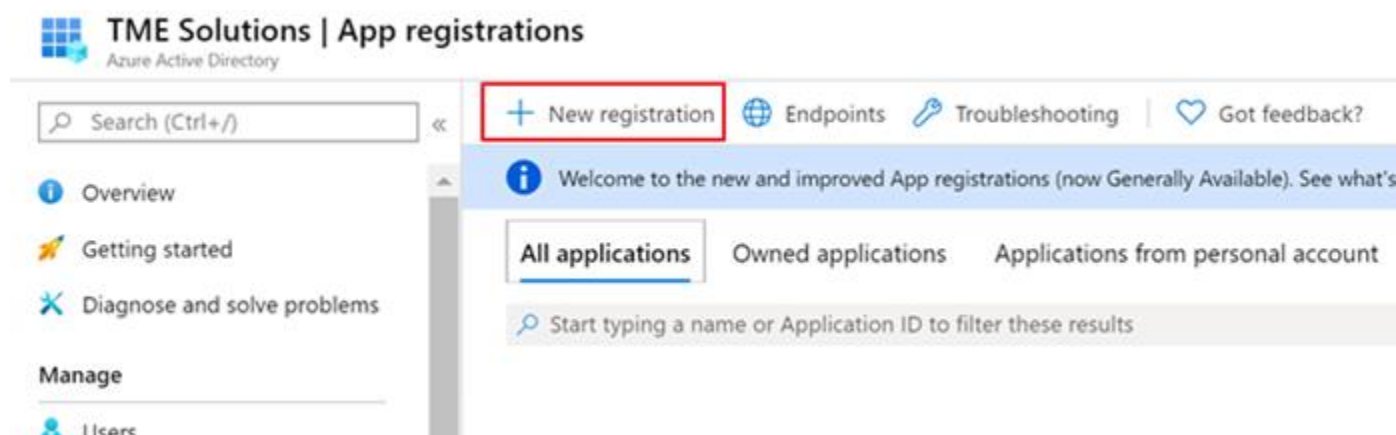
creation of users in both Azure AD as well as the required, duplicate user information being added to Cisco UDN Cloud.

Procedure 1. Azure AD Configuration

Step 1. Navigate to Azure AD and under **Manage** select **App Registrations**.



Step 2. Select **+ New registration**.



Step 3. In the **Register an application** screen, enter a name.

Step 4. Under Redirect URI, select **Web** and enter the following:
https://dnaservices.cisco.com/idm/api/v1/oid/acs

Step 5. When finished click **Register**.

Register an application

* Name

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

UDN-TME



Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (TME Solutions only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[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.

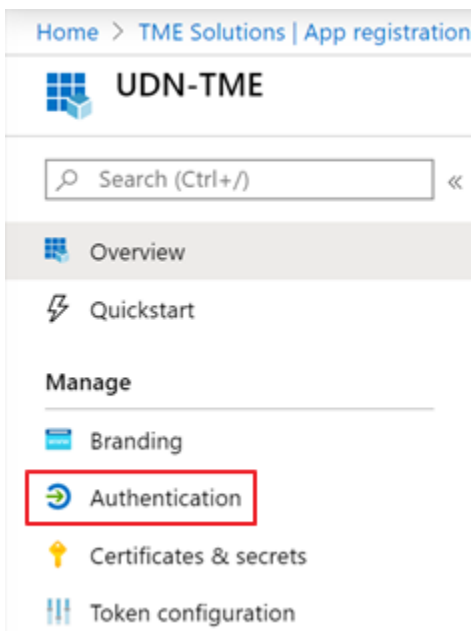
Web



https://dnaservices.cisco.com/idm/api/v1/oid/acs



Step 6. Once created click **Authentication**.



Step 7. Select **+ Add a platform**.

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

[+ Add a platform](#)

Step 8. Select Mobile and desktop applications.

Configure platforms

Web applications



Web

Build, host, and deploy a web server application. .NET, Java, Python

Mobile and desktop applications



iOS / macOS

Objective-C, Swift, Xamarin



Android

Java, Kotlin, Xamarin



Mobile and desktop applications

Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

Step 9. Under Custom redirect URIs enter the following: **com.sabretooth://sabretooth**

Step 10. Click **Configure** when finished.

Configure Desktop + devices



[← All platforms](#)

[Quickstart](#)

[Docs](#)

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred as reply URLs. [Learn more about redirect URIs and the restrictions](#)

- ☐ <https://login.microsoftonline.com/common/oauth2/nativeclient>
- ☐ https://login.live.com/oauth20_desktop.srf (LiveSDK)
- ☐ <msale465f597-4622-4360-9ca4-daff84822cfb://auth> (MSAL only)

Custom redirect URIs

com.sabretooth://sabretooth

In the next steps we will be collecting information to configure AAD as an SSO source for UDN cloud. Please capture this information in a separate document or notepad.

Step 11. Click **Overview** and capture the **Application (client) ID**.

Home > TME Solutions | App registrations > UDN-TME

UDN-TME

Search (Ctrl+/) «

Overview Quickstart Manage Branding Authentication

Delete Endpoints

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer)

Display name : UDN-TME

Application (client) ID : **e465f597-4622-4360-9ca4-daff84822cfb**

Directory (tenant) ID : 2a82daba-ecc2-4141-87d6-d0357ed396ef

Object ID : 0019faf0-3a05-4cfe-bcb0-9eeb33911e5f

Step 12. Click **Endpoints**.

Home > TME Solutions | App registrations > UDN-TME

UDN-TME

Search (Ctrl+/) «

Delete **Endpoints**

Step 13. Collect the information for the following:

- **OAuth 2.0 token endpoint (v1)**
- **OAuth 2.0 authorization endpoint (v1)**
- **OpenID Connect metadata document**

Tech tip

In the OpenID Connect metadata document you must remove the /v2.0 from the URL.

Endpoints



OAuth 2.0 authorization endpoint (v2)

<https://login.microsoftonline.com/2a82daba-ecc2-4141-87d6-d0357ed396ef/oauth2/v2.0/authorize>



OAuth 2.0 token endpoint (v2)

<https://login.microsoftonline.com/2a82daba-ecc2-4141-87d6-d0357ed396ef/oauth2/v2.0/token>



OAuth 2.0 authorization endpoint (v1)

<https://login.microsoftonline.com/2a82daba-ecc2-4141-87d6-d0357ed396ef/oauth2/authorize>



OAuth 2.0 token endpoint (v1)

<https://login.microsoftonline.com/2a82daba-ecc2-4141-87d6-d0357ed396ef/oauth2/token>



OpenID Connect metadata document

<https://login.microsoftonline.com/2a82daba-ecc2-4141-87d6-d0357ed396ef/v2.0/.well-known/openid-configuration>



Microsoft Graph API endpoint

<https://graph.microsoft.com>



Federation metadata document

<https://login.microsoftonline.com/2a82daba-ecc2-4141-87d6-d0357ed396ef/federationmetadata/2007-06/federationmetadata.xml>



WS-Federation sign-on endpoint

<https://login.microsoftonline.com/2a82daba-ecc2-4141-87d6-d0357ed396ef/wsfed>



SAML-P sign-on endpoint

<https://login.microsoftonline.com/2a82daba-ecc2-4141-87d6-d0357ed396ef/saml2>



SAML-P sign-out endpoint

<https://login.microsoftonline.com/2a82daba-ecc2-4141-87d6-d0357ed396ef/saml2>



Step 14. Navigate to **Certificates & secrets** and select **+New client secret**.

Home > TME Solutions > App registrations > UDN-TME > Certificates & secrets

UDN-TME | Certificates & secrets

Search (Ctrl+J)

- Overview
- Quickstart
- Manage
 - Branding
 - Authentication
 - Certificates & secrets**
 - Token configuration
 - API permissions
 - Expose an API
 - Owners
 - Roles and administrators (Previous)
 - Manifest
- Support & Troubleshooting
 - Troubleshooting
 - New support request

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

Thumbprint	Start date	Expires
No certificates have been added for this application.		

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	Value
No client secrets have been created for this application.		

Step 15. Provide a description and select an expiration for the client secret.

Add a client secret

Description

UDN Cloud

Expires

- ☐ In 1 year
☒ In 2 years
☐ Never

Add

Cancel

Step 16. Click **Add**, then collect the value for your newly created client secret.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	Value
UDN Cloud	5/7/2022	y8qX=f=q=kR79OCeW8egm0cSBS-0CKTF

Step 17. Navigate back to your AAD overview and capture the domain.

Home > TME Solutions | Overview

TME Solutions | Overview

Azure Active Directory

Search (Ctrl+/)

Switch directory Delete directory + Create a directory What's new Got feedback?

Overview

Getting started

Diagnose and solve problems

Manage

- Users
- Groups
- Organizational relationships
- Roles and administrators
- Administrative units (Preview)
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy

Azure Active Directory can help you enable remote work for your employees and partners. [Learn more](#)

Overview

TME Solutions

.onmicrosoft.com

Tenant ID 2a82daba-ecc2-4141-87d6-d0357ed396ef

Your role Global administrator [More info](#)

Azure AD Free

Azure AD Connect

Status Not enabled

Last sync Sync has never run

Make sure to save all captured information for the steps in Procedure 2.

Once the previous steps are completed, we will now optionally create and collect the Azure AD Group information necessary for the Cisco UDN Mobile App SSO at DNA Center Cloud. Remember that the benefit of using group attributes is that there will be no need to duplicate user creation in Cisco UDN Cloud; they only need to be present in Azure AD and assigned to the appropriate group.

Step 18. Navigate to Groups to create a new group and click +Add Group.

Microsoft Azure

Home > TME Solutions >

Groups | All groups

TME Solutions - Azure Active Directory

All groups

Deleted groups

+ New group

Try out the ne

Step 19. After creation of the group, make note of its **Object ID** as it will be required when configuring Cisco UDN Cloud. Navigate to **Groups** select the desired group and click **Members** then **Add Members** to the appropriate group.

Microsoft Azure

Home > TME Solutions > Groups | All groups >

Student
Group

Overview
Diagnose and solve problems

Manage
Properties
Members
Owners
Administrative units (Preview)
Group memberships
Applications
Licenses
Azure role assignments

Delete | Got feedback?

Try out the new Groups experience improvements (improved search and filtering). Click to enable the preview. →

Student
Students in dorms

Membership type: Assigned
Source: Cloud
Type: Security
Object Id: b8082fe5-0e65-44d3-80f3-e1bd9333e945
Creation date: 6/26/2020, 11:31:43 AM

Home > TME Solutions > Groups | All groups >

Student | Members
Group

Overview
Diagnose and solve problems

Manage
Properties
Members
Owners
Administrative units (Preview)
Group memberships

+ Add members | Remove | Refresh | Bulk activities | Columns | Got feedback?

Try out the new Groups experience improvements (improved search and filtering). Click to enable the preview. →

Direct members

	Name	Type
<input type="checkbox"/>	JD John Doe	User
<input type="checkbox"/>	LD Lisa Doe	User
<input type="checkbox"/>	MA Marge	User

Step 20. Navigate back to the Azure AD Tenant Overview page and select **App registrations** then select the App previously configured.

Microsoft Azure

Home >

TME Solutions | App registrations

Azure Active Directory

- Overview
- Getting started
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units (Preview)
- Enterprise applications
- Devices
- App registrations**

New registration Endpoints Troubleshooting Got feedback?

Welcome to the new and improved App registrations (now Generally Available). See what's new.

All applications **Owned applications** Applications from personal account

Start typing a name or Application ID to filter these results

Display name

UD	UDN-TME
----	---------

Step 21. Select **Token Configuration** and click **+Add groups claim**.

Microsoft Azure

Home > TME Solutions | App registrations >

UDN-TME | Token configuration

Search (Ctrl+/) Got feedback?

- Overview
- Quickstart
- Integration assistant (preview)

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration**

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim + Add groups claim

Claim ↑↓	Description
----------	-------------

Step 22. The Edit groups claim window opens. Select **Security groups** and then click the radio buttons for **ID-Group ID**, **Access-Group ID**, and optionally **SAML-Group ID**.

Edit groups claim



Adding the groups claim applies to Access, ID, and SAML token types. [Learn more](#)

Select group types to include in Access, ID, and SAML tokens.

- ☒ Security groups
- ☐ Directory roles
- ☐ All groups (includes distribution lists but not groups assigned to the application)
- ☐ Groups assigned to the application

Customize token properties by type

^ ID

- ☒ Group ID
- ☐ sAMAccountName
- ☐ NetBIOSDomain\sAMAccountName
- ☐ DNSDomain\sAMAccountName
- ☐ On Premises Group Security Identifier
- ☐ Emit groups as role claims

^ Access

- ☒ Group ID
- ☐ sAMAccountName
- ☐ NetBIOSDomain\sAMAccountName
- ☐ DNSDomain\sAMAccountName
- ☐ On Premises Group Security Identifier
- ☐ Emit groups as role claims

^ SAML

- ☒ Group ID

Add

Cancel

Step 23. Click **Add** and the Optional claims for groups are created. The remaining configuration steps to use group attributes will be completed in the next procedure to be completed at Cisco UDN Cloud.

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim

+ Add groups claim

Claim ↑↓	Description	Token type ↑↓	Optional settings
groups	Optional formatting for group claims	ID, Access, SAML	Default

Procedure 2. Cloud Tenant Creation and setup.

Step 1. Log in to <https://UDN.cisco.com> Using your **CCO ID**.

Cisco DNA Center Cloud

Welcome back.

Log In With Cisco

Create a new account

Log In With SSO

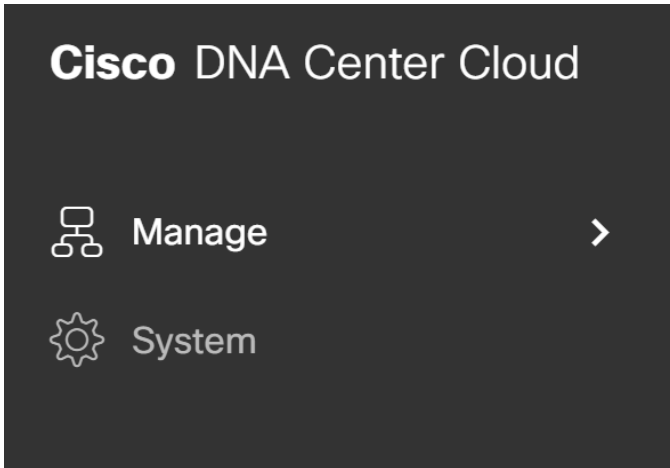
Step 2. A pop up will appear confirming that this is the profile you would like to register with, click to agree to the terms and select **Create Account**.

The screenshot shows a 'Confirm CCO Profile' dialog box. At the top is the Cisco DNA Center Cloud logo. Below it, the text reads: 'Confirm that this is the Cisco profile you would like to register with, or [login to a different CCO](#).' There are three input fields: 'Your Name', 'Your Email', and 'Organization Name', each with a greyed-out placeholder. Below these fields is a blue-bordered box containing an information icon and the text: 'Smart Account selection not required (dev/qa mode)'. At the bottom, there is a checkbox that is checked, followed by the text: 'I agree that Cisco DNA Center Cloud is governed by the [Cisco Universal Cloud Agreement](#) and that I have read and acknowledge the [Cisco Privacy Agreement](#). Note: If you do not have the authority to bind your company and its affiliates, or if you do not agree with the terms of the Universal Cloud Agreement, do not check this box.' At the very bottom is a blue 'Create Account' button.

Step 3. A tenant will then be created in the UDN cloud with the CCO used with administrator privileges.

Procedure 3. Configuring Single Sign-on with individual user information

Step 1. Once logged into the UDN cloud, Click the menu button at the top left of the screen and select **System**.



Step 2. Select **Single-Sign-On**. Then click the slider next to **Enable SSO Access**.

The screenshot shows the 'Single Sign-On' configuration page. On the left is a sidebar with a menu containing 'General', 'User Management', 'Authentication Token', 'Cisco Support', and 'Single Sign-On' (which is highlighted with a blue bar). The main content area is titled 'Single Sign-On'. Below the title, it says: 'You can use Security Assertion Markup Language (SAML) with Cisco DNA Center Cloud to authenticate external users through 'Single Sign-On'.' At the bottom of the main area, there is a toggle switch labeled 'Enable SSO Access'. The switch is currently in the 'off' position, indicated by a grey box and an 'X' icon.

Step 3. Enter the information taken in the previous steps to the corresponding attribute. When finished click **Next** and **Enable SSO**.

Set up your SSO gateway

To Authenticate end users from a selected directory, we need to configure your SSO gateway provider using SAML. Once you connect your active directory, you will be able to see your user group attributes and map them to their access roles.

The screenshot shows the SSO gateway configuration form. It is divided into three main sections: 'idP', 'ENDPOINTS', and 'ID CLIENT CREDENTIALS'. The 'idP' section has a dropdown menu for 'idP' with 'Microsoft Azure' selected, and a text field for 'idP URL' containing 'brbrzezi.onmicrosoft.com'. Below this is a 'Scope' section with three buttons: 'Open ID', 'Email', and 'Profile'. The 'ENDPOINTS' section has three text fields for 'Endpoint URL', all containing 'https://login.microsoftonline.com/2a82...'. The 'ID CLIENT CREDENTIALS' section has a text field for 'Client ID' containing 'e465f597-4622-4360-9ca4-daff84822' and a 'SHOW' button.

Step 4. You should now see the single sign-on confirmation screen.

Done!

Single Sign-On is enabled for mapped users. You can now invite them to log in DNA Center Cloud via Single Sign-On.

 Single Sign-On is enabled 

What's Next?

[Manage User](#)

[Manage SSO Configuration](#)

[Home](#)

Step 5. To optionally continue to configure group attributes, select **Manage SSO Configuration** as seen in the screenshot above and scrolling down on the page click on **SSO User Setting** then click on the slider.

SSO User Setting

Single Sign-On is enabled for all invited users. [Manage User](#)

Map attributes from Active Directory



[Add Attributes Mapping](#)

Attributes ▲

Value

Step 6. Click **Add Attributes Mapping** and the configuration window opens. For **Attribute** enter “**groups**”; note that this is case sensitive. For **Value** use the Group **Object ID** collected during group creation and select the appropriate role. For normal users this will be the **ACCOUNT-USER-ROLE**. Click **Add**.

Add Attributes Mapping

Attribute*

groups

Value*

b8082fe5-0e65-44d3-80f3-e1bd9333e945

Role*

ACCOUNT-USER-ROLE

Cancel

Add

You will notice that two “groups” attributes are added, one for **ACCOUNT-USER-ROLE** and the other for Observer role. This is normal.

SSO User Setting

Single Sign-On is enabled for all invited users. [Manage User](#)

Map attributes from Active Directory ☒ ⓘ

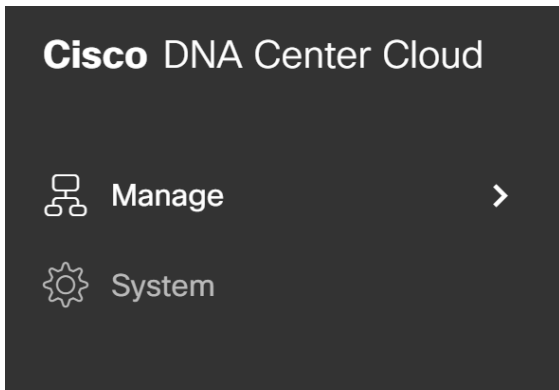
Add Attributes Mapping

Attributes ▲	Value	Role
groups	b8082fe5-0e65-44d3-80f3-e1bd9333e945	ACCOUNT-USER-ROLE
groups	b8082fe5-0e65-44d3-80f3-e1bd9333e945	Observer

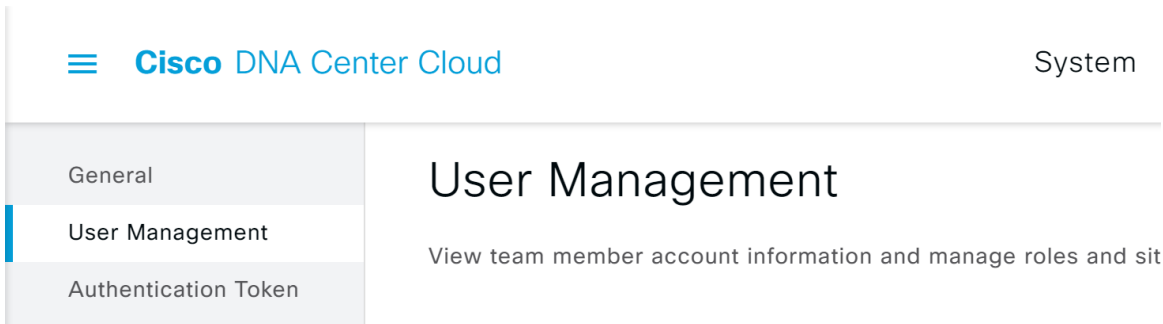
Procedure 4. Enroll Admin and Student Users

The following steps are only required if Azure AD group attributes aren't being used. In the following we are only showing the addition of users within Cisco UDN Cloud. It is assumed that a corresponding user exists in Azure AD.

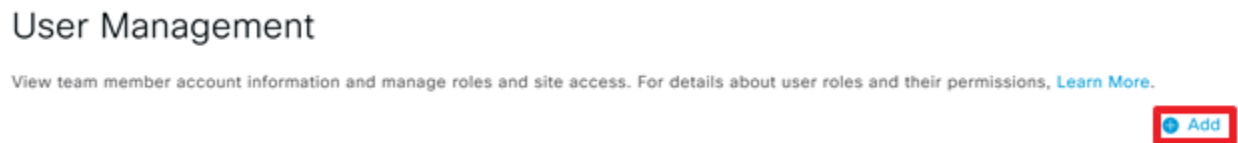
Step 1. In the UDN cloud, Click the menu button at the top left of the screen and select **System**.



Step 2. Select **User Management**.



Step 3. Click **Add** at the top right corner.



Step 4. Enter the email and role of the new user with the role of **ACCOUNT-USER-ROLE** for students and **ADMIN** for additional admin users.

Add Team Member ×

Enter your team member's email address. Please notify them via your communication channel to join this account.

Email*
jane@brbrzezi.onmicrosoft.com

Role
ACCOUNT-USER-ROLE ∨

Step 5. Repeat these steps for all wanted users.

Process 2: Cloud Authentication with SAML and Microsoft ADFS

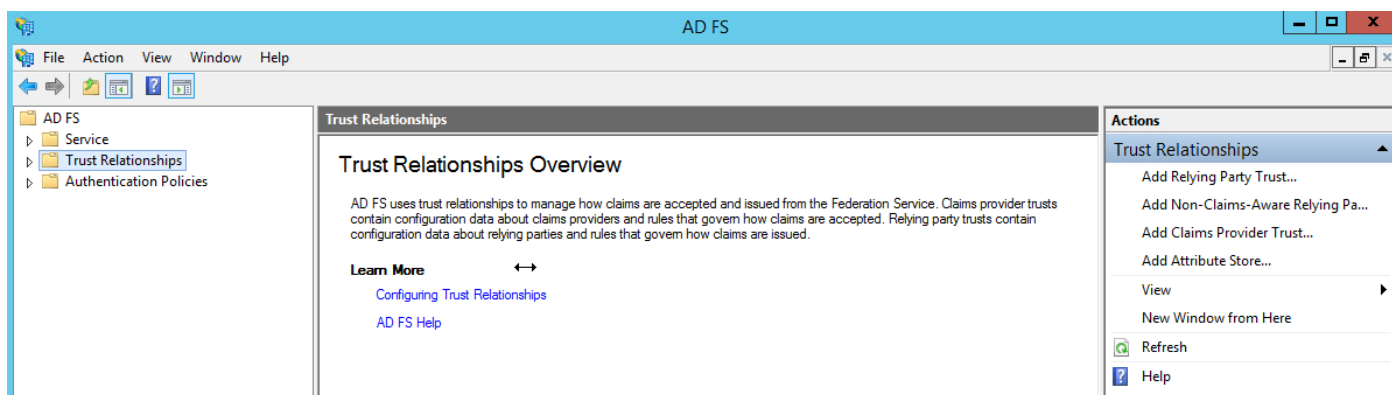
In addition to support for OpenID and Microsoft Azure AD, Cisco UDN Cloud authentication using SAML 2.0 is also supported. In this process, we will detail the steps required to configure Microsoft ADFS using SAML to provide the cloud authentication for the Cisco UDN Mobile App.

Tech tip

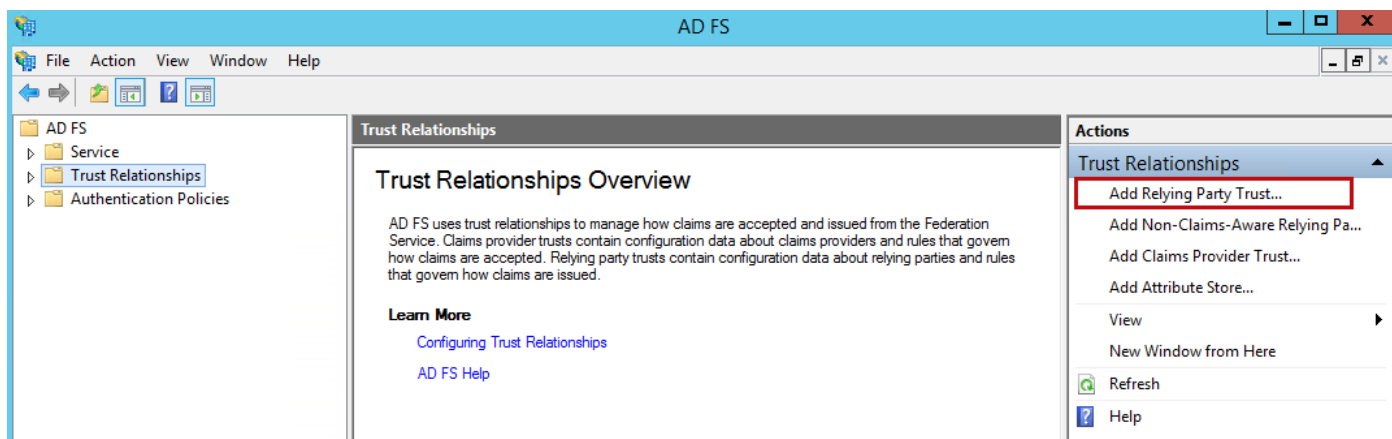
This process assumes that you have Microsoft ADFS installed in your environment. It is beyond the scope of this document to discuss design and deployment of ADFS in your environment. Also be aware that these steps were documented using Microsoft Windows Server 2016 in conjunction with ADFS v4.0 (2016).

Procedure 1. Configure Microsoft ADFS

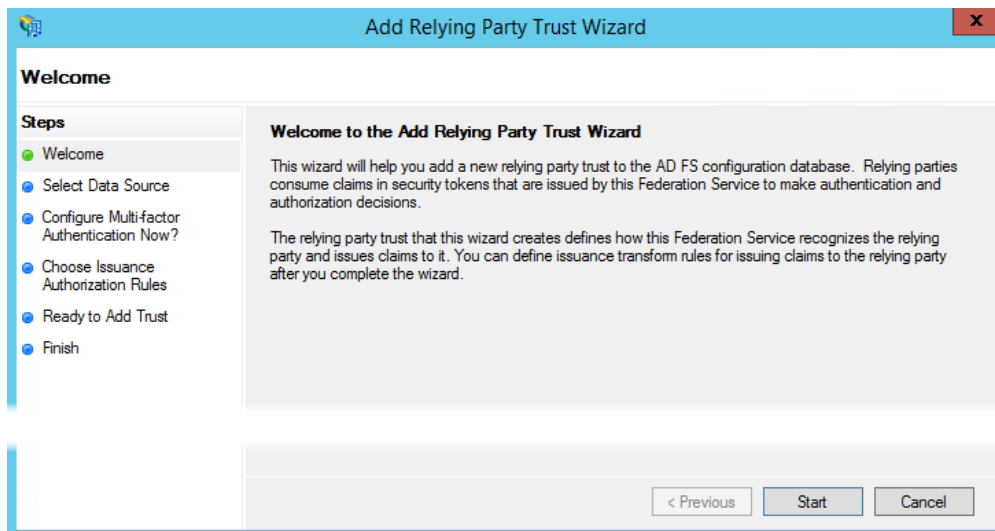
Step 1. Open the Microsoft ADFS Management Console.



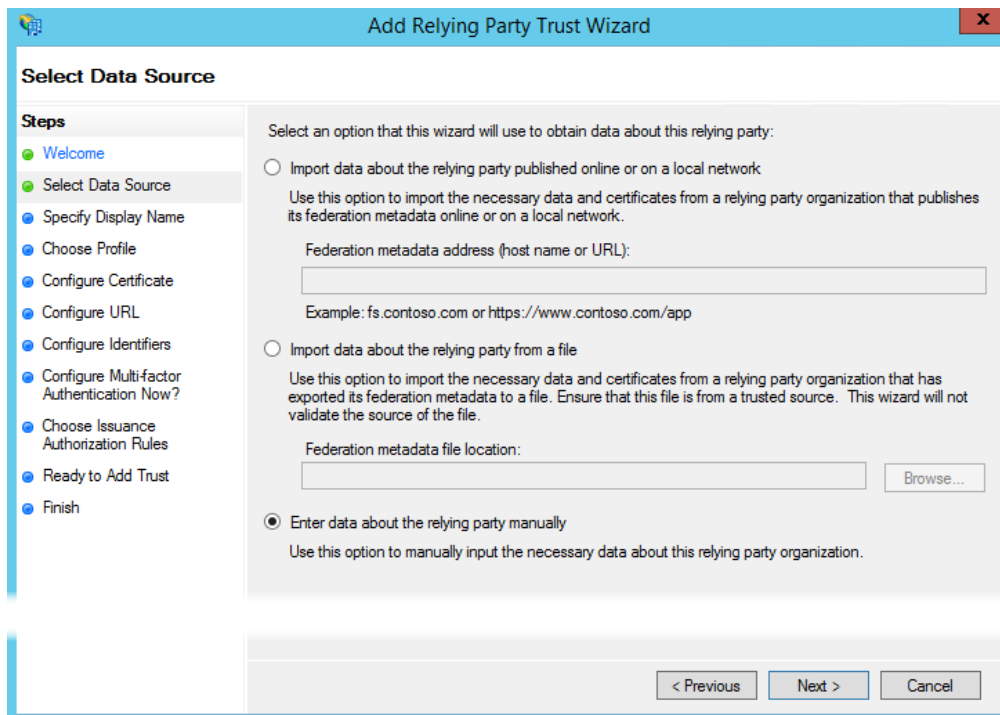
Step 2. Navigate to **Trust Relationships > Relying Party Trusts > Add Relying Party Trust...**



Step 3. The **Add Relying Party Trust Wizard** opens. Click **Start**.



Step 4. In the Select Data Source window choose the third option, **Enter data about the relying party manually**.



Step 5. For the **Display Name** add a name to identify the relying party. This can be any meaningful name you want to use and then click **Next**.

Add Relying Party Trust Wizard

Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name:
https://dnaservices.cisco.com

Notes:
UDN Cloud IDM

< Previous Next > Cancel

Step 6. Select the first option, **Add FS profile**.

Add Relying Party Trust Wizard

Choose Profile

This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

☒ **AD FS profile**
This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

☐ AD FS 1.0 and 1.1 profile
This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

< Previous Next > Cancel

Step 7. Optionally, choose a certificate to be used for token encryption of claims sent to this relying party then click **Next**. Otherwise, just click **Next**.

Add Relying Party Trust Wizard

Configure Certificate

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

View... Browse... Remove

< Previous Next > Cancel

Step 8. In the **Configure URL** window, check the **Enable support for SAML 2.0 WebSSO protocol** box and then enter in the following URL <https://dnaservices.cisco.com/idm/api/v1/saml/acs> and click **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' window with the 'Configure URL' step selected in the left-hand 'Steps' pane. The main area contains instructions about AD FS protocols and two configuration options. The first option, 'Enable support for the WS-Federation Passive protocol', is unchecked. The second option, 'Enable support for the SAML 2.0 WebSSO protocol', is checked. Below the checked option, the 'Relying party SAML 2.0 SSO service URL' is entered as 'https://dnaservices.cisco.com/idm/api/v1/saml/acs'. The 'Next >' button is highlighted with a red box.

Add Relying Party Trust Wizard

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☐ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: <https://fs.contoso.com/adfs/ls/>

☒ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

<https://dnaservices.cisco.com/idm/api/v1/saml/acs>

Example: <https://www.contoso.com/adfs/ls/>

< Previous **Next >** Cancel

Step 9. In the **Configure identifiers** window, enter <https://dnaservices.cisco.com.com/idm/api/v1/saml/metadata> click **Add** and the **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' window with the 'Configure Identifiers' step selected in the left-hand 'Steps' pane. The main area contains instructions about unique identifier strings. The 'Relying party trust identifier' is entered as 'https://dnaservices.cisco.com.com/idm/api/v1/saml/metadata', and the 'Add' button next to it is highlighted with a red box. The 'Next >' button at the bottom is also highlighted with a red box.

Add Relying Party Trust Wizard

Configure Identifiers

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Configure Multi-factor Authentication Now?

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

<https://dnaservices.cisco.com.com/idm/api/v1/saml/metadata> **Add**

Example: <https://fs.contoso.com/adfs/services/trust>

Relying party trust identifiers:

Remove

< Previous **Next >** Cancel

Step 10. Select **I do not want to configure multi-factor authentication...** if you do not want to make use of the optional multi-factor authentication settings then click **Next**.

Add Relying Party Trust Wizard

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?**
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

☒ I do not want to configure multi-factor authentication settings for this relying party trust at this time.
☐ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

< Previous Next > Cancel

Step 11. Select **Permit all users...** such that authentication requests from the relying party trust for every user, will be permitted. Our example depicts the default scenario. Click **Next**.

Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules**
- Ready to Add Trust

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

☒ **Permit all users to access this relying party**
 The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

☐ **Deny all users access to this relying party**
 The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

< Previous Next > Cancel

Step 12. Verify that the setting in the various tabs are correct and click **Next**.

Add Relying Party Trust Wizard

Ready to Add Trust

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust**
- Finish

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring	Identifiers	Encryption	Signature	Accepted Claims	Organization	Endpoints	Note
Specify the display name and identifiers for this relying party trust.							
Display name: https://dnaservices.cisco.com							
Relying party identifiers: https://dnaservices.cisco.com/idm/api/v1/saml/metadata							

< Previous Next > Cancel

Step 13. Addition of the relying party trust is now completed. Check the box next to **Open the edit...** and click **Close**.

Add Relying Party Trust Wizard

Finish

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish**

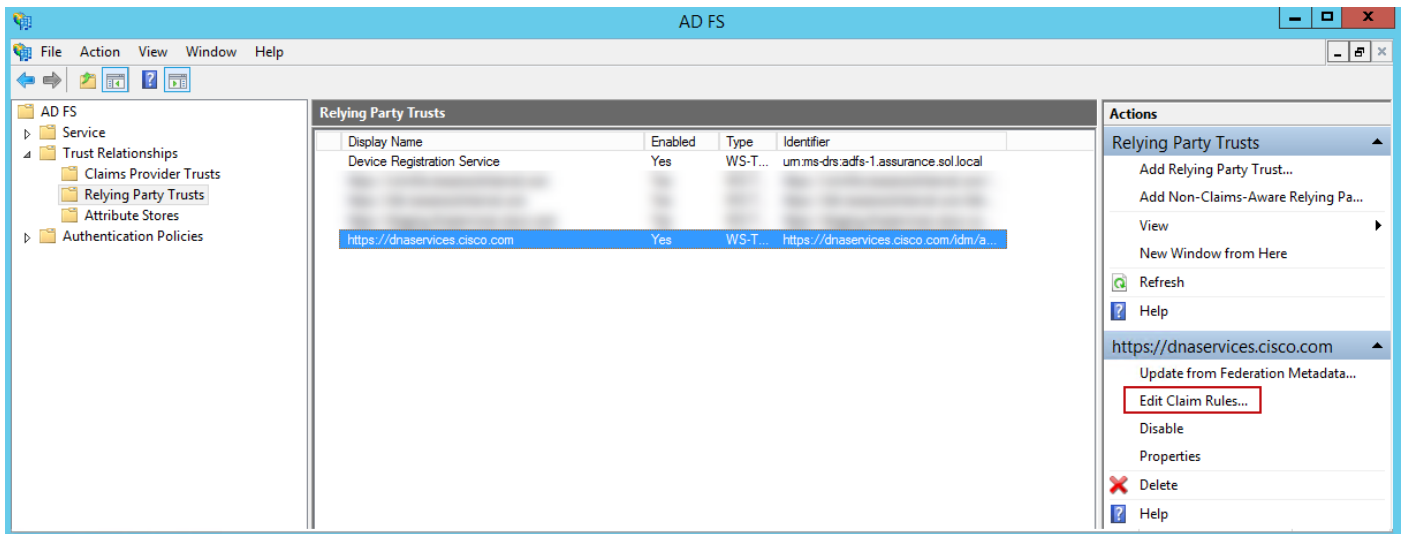
The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

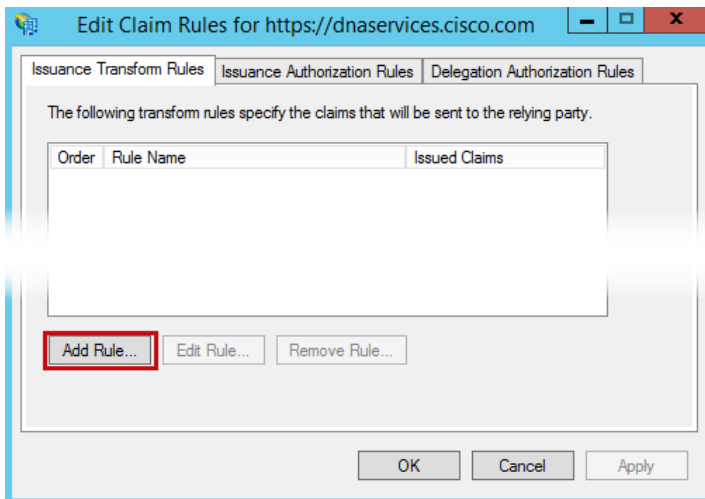
☒ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

Close

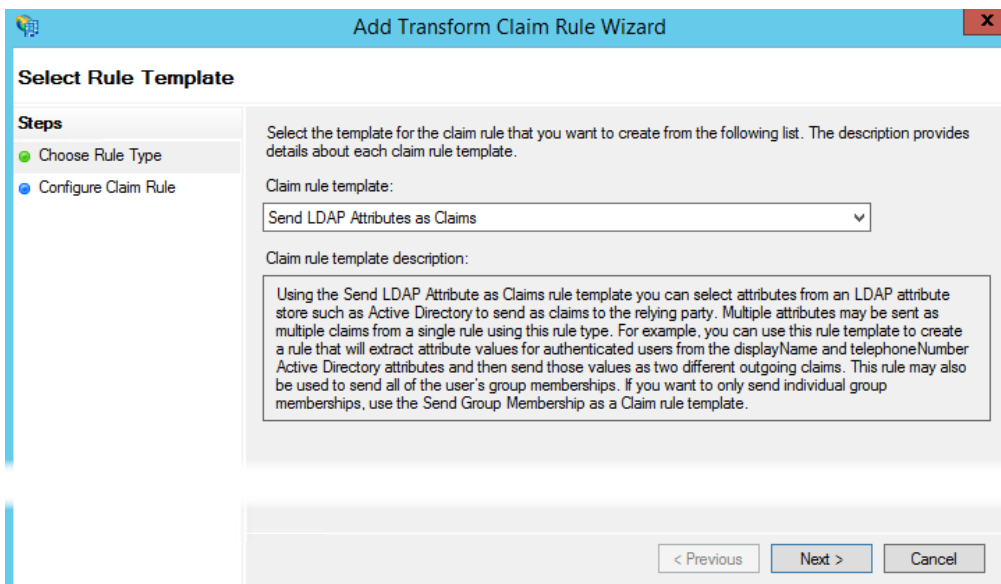
Step 14. Once completed, from the ADFS Management Console, select the relying party trust you just created and select **Edit Claims Rules...**



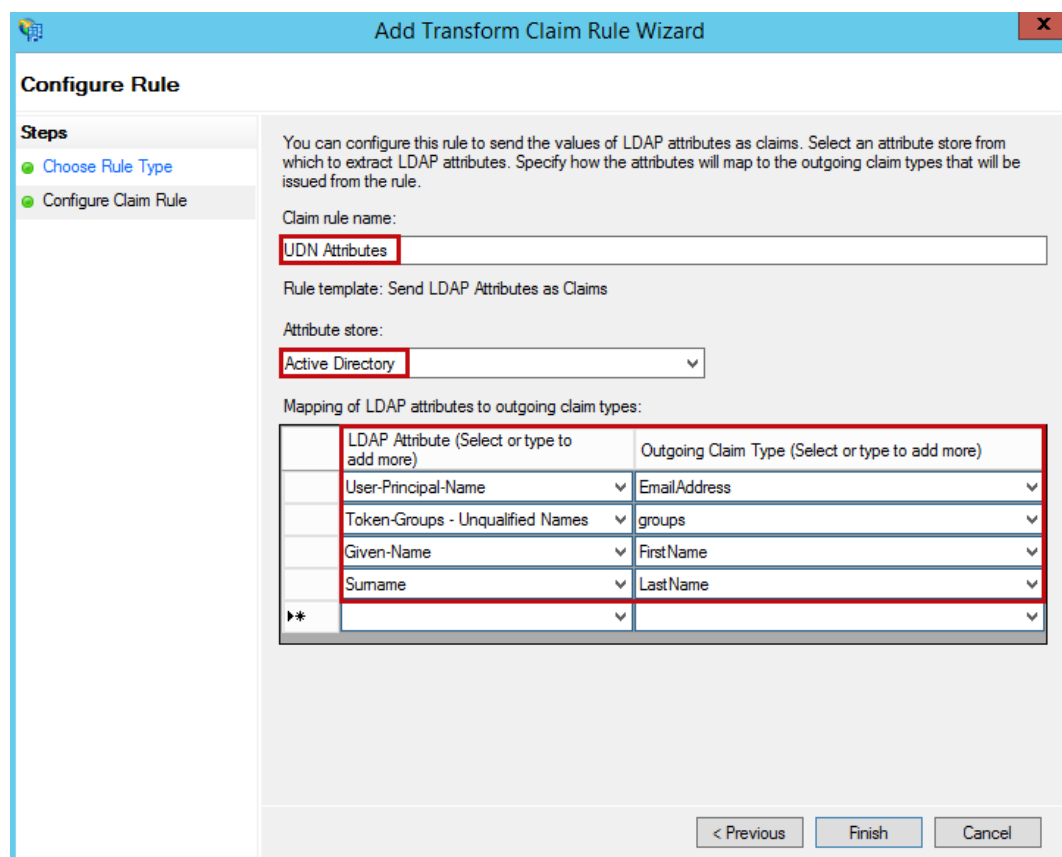
Step 15. Next select Add Rule.



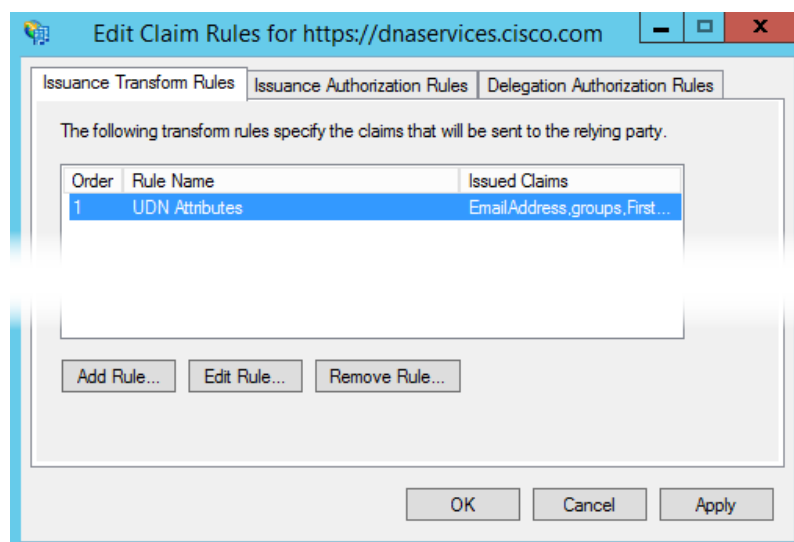
Step 16. In the drop-down select **Send LDAP Attributes as Claims** then click **Next**.



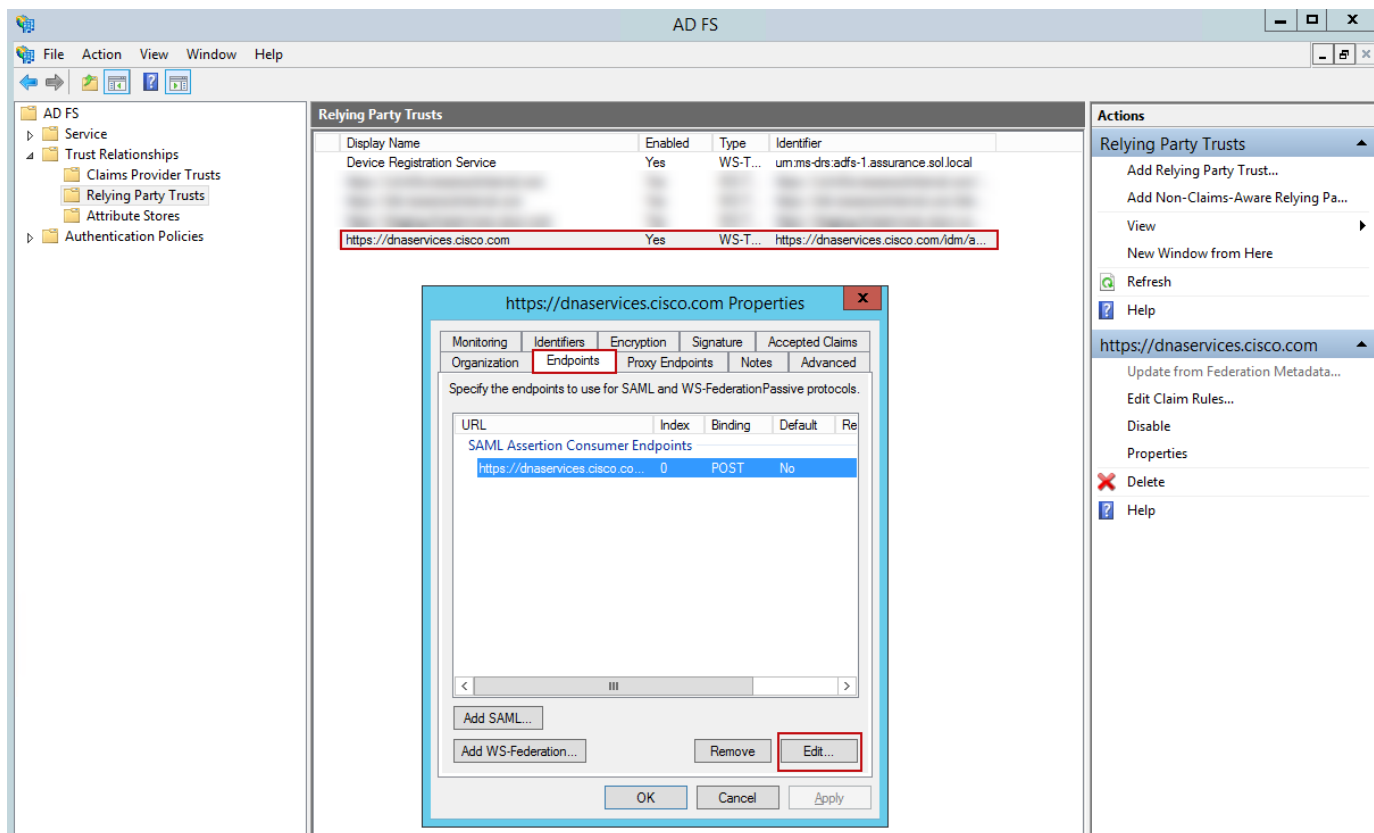
Step 17. In this step, we add each of the LDAP attributes that we want to match. Define an arbitrary **Claim rule name** then select **Active Directory** for the **Attribute store**. It is then necessary to define **User-Principal-Name**, **Token-Groups**, **Given-Name** and **Surname** using **EmailAddress** or **UserID** (for **User-Principal Name**), **groups**, **FirstName** and **LastName** respectively as seen below for the **Outgoing Claim Type**. With these attributes configured, users will be automatically created in the UDN Cloud eliminating the need to do that manually. The values used for the **Outgoing Claim Type** have been typed in as they are unavailable from the drop-down. These values must match exactly as seen below; they are case sensitive. Once complete click **OK**.



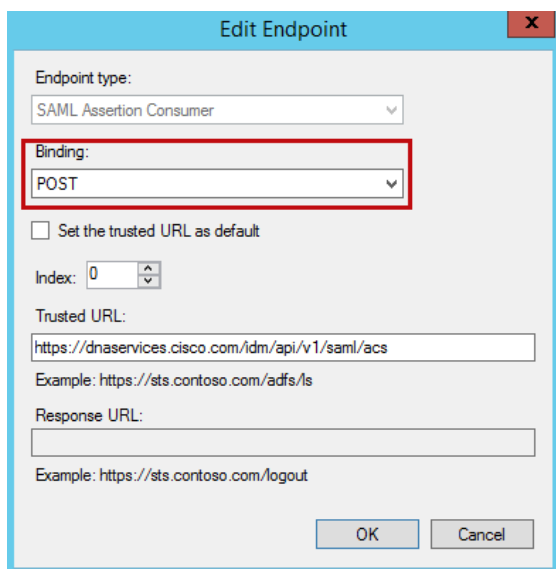
Step 18. Next click **Apply** and then **OK**.



Step 19. At the ADFS Management Console, right click on the relying party trust you created and in the drop-down menu select **Properties**. Go to the **Endpoints** tab and select the URL then click **Edit**.



Step 20. Verify that the **Binding** is set to **Post** and that the Trusted URL is set to **https://dnaservices.cisco.com/idm/api/v1/saml/acs**. Click **OK**.



Step 21. Go to the **Monitoring** tab. Add **https://dnaservices.cisco.com/idm/api/v1/saml/metadata** then click **Apply** and **OK**.

https://dnaservices.cisco.com Properties [X]

Organization	Endpoints	Proxy Endpoints	Notes	Advanced
Monitoring	Identifiers	Encryption	Signature	Accepted Claims

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

☐ Monitor relying party

☐ Automatically update relying party

This relying party's federation metadata data was last checked on:
 < never >

This relying party was last updated from federation metadata on:
 < never >

[OK] [Cancel] [Apply]

Step 22. Go to the **Identifiers** tab and enter **https://dnaservices.cisco.com/idm/api/v1/saml/acs**. Click **Add**, then **Apply**, and finally **OK**.

https://dnaservices.cisco.com Properties [X]

Organization	Endpoints	Proxy Endpoints	Notes	Advanced
Monitoring	Identifiers	Encryption	Signature	Accepted Claims

Specify the display name and identifiers for this relying party trust.

Display name:

Relying party identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party identifiers:

[OK] [Cancel] [Apply]

Step 23. You should now see the following. This completes the configuration required at Microsoft ADFS.

https://dnaservices.cisco.com Properties

Organization	Endpoints	Proxy Endpoints	Notes	Advanced
Monitoring	Identifiers	Encryption	Signature	Accepted Claims

Specify the display name and identifiers for this relying party trust.

Display name:

Relying party identifier:

 Add

Example: https://fs.contoso.com/adfs/services/trust

Relying party identifiers:

 Remove

< III >

OK Cancel Apply

Procedure 2. Cloud Tenant Creation and setup.

Step 1. Log in to **https://UDN.cisco.com** Using your **CCO ID**.

Cisco DNA Center Cloud

Welcome back.

Log In With Cisco

Create a new account

Log In With SSO

Step 2. A pop up will appear confirming that this is the profile you would like to register with, click to agree to the terms and select **Create Account**.

Cisco DNA Center Cloud

Confirm CCO Profile

Confirm that this is the Cisco profile you would like to register with, or [login to a different CCO](#).

Your Name

XXXXXXXXXX

Your Email

XXXXXXXXXX@XXXXXX.XX

Organization Name



Smart Account selection not required (dev/qa mode)



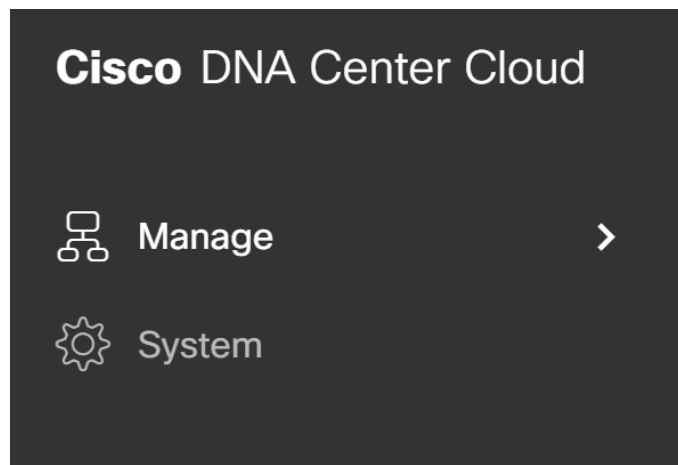
I agree that Cisco DNA Center Cloud is governed by the [Cisco Universal Cloud Agreement](#) and that I have read and acknowledge the [Cisco Privacy Agreement](#). Note: If you do not have the authority to bind your company and its affiliates, or if you do not agree with the terms of the Universal Cloud Agreement, do not check this box.

Create Account

Step 3. A tenant will then be created in the UDN cloud with the CCO used with administrator privileges.

Procedure 3. Configuring Single Sign-on with individual user information

Step 1. Once logged into the UDN cloud, Click the menu button at the top left of the screen and select **System**.



Step 2. Select **Single-Sign-On**. Then click the slider next to **Enable SSO Access**.

General
User Management
Authentication Token
Cisco Support
Single Sign-On

Single Sign-On

You can use Security Assertion Markup Language (SAML) with Cisco DNA Center Cloud to authenticate external users through 'Single Sign-On'.

☐
X
Enable SSO Access

Step 3. Prior to proceeding with the SSO configuration, you will need to have the SAML metadata URL to complete the UDN Cloud configuration. At the Microsoft ADFS Management Console, navigate to **Service > Endpoints** and in the **Metadata** section you will find the metadata XML file. Make note of the path to the file which will be required in the next step.

Enabled	Proxy Enabled	URL Path	Type	Authentication
No	No	/adfs/services/trust/2005/issuetoikmixedsymmetrictripl...	WS-Trust 2005	SAML Token
Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3	Kerberos
No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	Certificate
Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	Certificate
No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3	Certificate
No	No	/adfs/services/trust/13/username	WS-Trust 1.3	Password
No	No	/adfs/services/trust/13/usernamebasictransport	WS-Trust 1.3	Password
Yes	Yes	/adfs/services/trust/13/usernamemixed	WS-Trust 1.3	Password
No	No	/adfs/services/trust/13/issuetoikenasymmetricbasic256...	WS-Trust 1.3	SAML Token
No	No	/adfs/services/trust/13/issuetoikenasymmetricbasic256sha...	WS-Trust 1.3	SAML Token
Yes	Yes	/adfs/services/trust/13/issuetoikmixedasymmetricbasic...	WS-Trust 1.3	SAML Token
No	No	/adfs/services/trust/13/issuetoikmixedasymmetricbasic...	WS-Trust 1.3	SAML Token
Yes	Yes	/adfs/services/trust/13/issuetoikmixedasymmetricbasic2...	WS-Trust 1.3	SAML Token
No	No	/adfs/services/trust/13/issuetoikmixedasymmetricbasic2...	WS-Trust 1.3	SAML Token
No	No	/adfs/services/trust/13/issuetoiksymmetricbasic256...	WS-Trust 1.3	SAML Token
No	No	/adfs/services/trust/13/issuetoiksymmetricbasic256sha...	WS-Trust 1.3	SAML Token
No	No	/adfs/services/trust/13/issuetoiksymmetrictripledes...	WS-Trust 1.3	SAML Token
No	No	/adfs/services/trust/13/issuetoiksymmetrictripledesha...	WS-Trust 1.3	SAML Token
No	No	/adfs/services/trust/13/issuetoikmixedasymmetrictripledes...	WS-Trust 1.3	SAML Token
No	No	/adfs/services/trust/13/issuetoikmixedasymmetrictripledes...	WS-Trust 1.3	SAML Token
No	No	/adfs/services/trust/13/windows	WS-Trust 1.3	Windows
No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3	Windows
No	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3	Windows
Yes	No	/adfs/services/trusttcp/windows	WS-Trust 2005	Local Wind
No	No	/adfs/services/trust/artifactresolution	SAML-ArtifactResolution	Anonymous
Yes	Yes	/adfs/oauth2/	OAuth	Anonymous
Metadata				
Yes	Yes	/adfs/services/trust/mex	WS-MEX	Anonymous
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata	Anonymous
Yes	No	/adfs/fs/federationserver/service.asmx	ADFS 1.0 Metadata	Anonymous
Proxy				
Yes	No	/adfs/proxy/	Web Application Proxy	Proxy Trust
Yes	No	/adfs/proxy/EstablishTrust/	Web Application Proxy	Password
Other				
No	No	/adfs/portal/updatepassword/	HTTP	Anonymous

Step 4. Back at the Cisco UDN Cloud UI, once SSO is enabled the configuration window opens. Select **SAML** for the **Protocol**. For **IdP**, select **Other** from the drop-down. For **Domain**, enter your Active Directory domain name. Under **Metadata URL** enter **https://<ADFS server FQDN>/FederationMetadata/2007-06/FederationMetadata.xml**. Click **Next**.

Set up your SSO gateway

To authenticate end users from a selected directory, you need to configure your SSO gateway identity provider (IdP). Then, you can configure your user group attributes and map them to Cisco DNA Center Cloud roles.

Protocol

☐ OpenID ☒ SAML

CDNA Metadata URL for IdP ⓘ <https://dnaservices.cisco.com/idm/api/v1/saml/metadata>

IdP*

Other

Domain*

test.cisco.com

Metadata URL*

[/adfs.test.cisco.com/FederationMetadata](#)

You will now have a chance to map Active Directory Attributes used for SSO. The benefit of doing so is that when a user authenticates for the first time with the Cisco UDN Mobile App, the user will be automatically created in the UDN Cloud tenant, eliminating the requirement to create them manually. Should you choose not to do so, the manual user creation is documented in the preceding process (Azure AD).

Step 5. Select **Yes to Map attributes**. For **Attribute** we use the **Token-Groups** attribute from ADFS. This is taken from ADFS in Procedure1/Step16 earlier. Enter **groups** which is mapped to **Token-Groups** in ADFS and for **Value** enter the name of an existing AD group; note that these are all case sensitive and must match exactly. For **Role**, select **ACCOUNT-USER-ROLE** from the drop-down and click **Next**.

Do you want to map attributes from Active Directory?

SSO will be enabled for all the invited users. You may also map attributes from Identity Provider so you can assign roles to groups of SSO users.

Map attributes from Active Directory

☒ Yes ☐ No

Attribute*	Value*
groups	Students
Role*	
ACCOUNT-USER-ROLE	

Step 6. In the summary screen that appears, select **Enable SSO**.

Step 7. You have nearly completed the SSO Configuration for the Cisco UDN Cloud. If you select Manage SSO Configuration from the completion window that appears, you will notice that a second attribute mapping is automatically created with a **Role** of **Observer**. This is completely normal and in fact required. Do not delete that mapping or SSO will break.

▼ SSO User Setting

Single Sign-On is enabled for all invited users. [Manage User](#)

Map attributes from Active Directory ☒ ⓘ

Add Attributes Mapping

Attributes ^	Value	Role	Action
groups	Students	ACCOUNT-USER-ROLE	...
groups	Students	Observer	...

Process: Mobile App Customization

Procedure 1. Support Contacts

In this section, you can provide contact information for the helpdesk in case the student needs assistance with UDN. You can provide all contact methods or a subset. The preview screen will reflect what the student will see when they select **Settings > Contact us** within the UDN Mobile App

Step 1. Navigate to **Manage>Mobile Customization>Support Contacts**.

Step 2. Enter an Email, URL or Phone Number to be used for UDN support.

Mobile Customization

Support Contacts

Organization Logo

SSID

What support contact information do you want to be displayed in the mobile application?

PREVIEW:

Review the below, this will be available for end users to see throughout the mobile app in case they should need to contact support.

What methods of support do you want to provide to end users?

Email Address

|

URL

https://sjsu.edu

Phone Number

123-456-7890

[Reset to last saving](#)

Save



Procedure 2. Organization Logo

In this section a company or school logo can be uploaded which will be visible by users in the Cisco UDN Application. The logo must be in PNG format, less than 1 MB, and equal to or larger than 512 x 512 pixels.

Mobile Customization


Support Contacts

Organization Logo

SSID

Add a logo to quickly customize your app experience.

Upload the logo you would like to use:



Choose a file or drag and drop to upload.

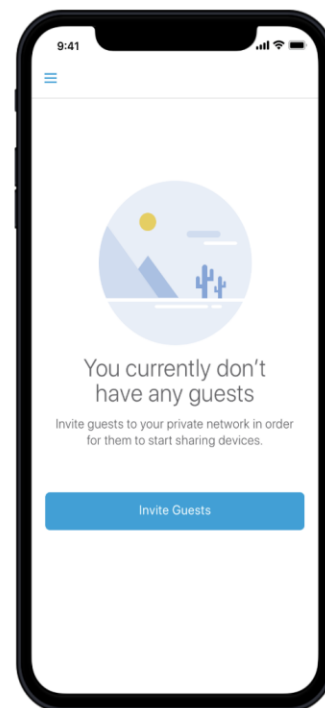
Accepted files: .png

Accepted sizes: up to 1 MB

[Reset to last saving](#)

[Save](#)

PREVIEW:



Procedure 3. Add SSID to UDN Cloud

In this section you can add up to three SSIDs used at the campus. This is needed for two reasons.

- **Disable Mobile App Wi-Fi scanning** – While this is a nice feature, you may not want the students to scan while on the campus network. Wi-Fi scanning will be disabled when connected to the SSID specified here.
- **MAC Address Randomization** – Certain wireless devices, for security, use a random MAC Address for each SSID it connects to. While not a bad practice, this can cause issues with device registration. Adding the SSID here makes it so users can only add random MAC addresses while connected to the SSID. More information about Randomized MAC Addresses can be found in Appendix B.

Tech tip

At least one SSID is needed for the UDN Mobile App to work.

Step 1. In the UDN Cloud navigate to **Manage>Mobile Customization>SSID**.

Step 2. Enter the SSID to be used for UDN and click **Save**.

Mobile Customization

Support Contacts

Organization Logo

SSID

Add User Defined Network SSID's

Configure up to 3 UDN enabled SSID's. These should be the same as the ones configured in your DNAC as part of the UDN workflow.

SSID

Student-dorm|



[Reset to last saving](#)

Save

Process: UDN Workflow

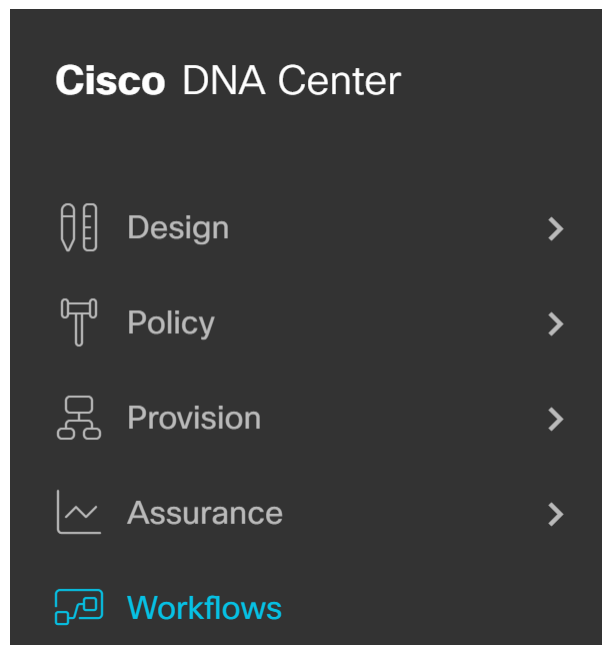
Procedure 1. Cisco DNA Center UDN Workflow

This section will go through the UDN Workflow on Cisco DNA Center to integrate with the UDN cloud as well as enable UDN on the SSID.

Tech tip

At the present time, DNAC clustering is **not** supported. Support for DNAC clustering will be available in a future release of the solution.

Step 1. In Cisco DNA Center Navigate to **Workflows**.



Step 2. Click **Configure Cisco User Defined Network** and then **Let's do it**.



Configure Cisco User Defined Network

Choose the Sites and enable/disable UDN service for each SSID/Site

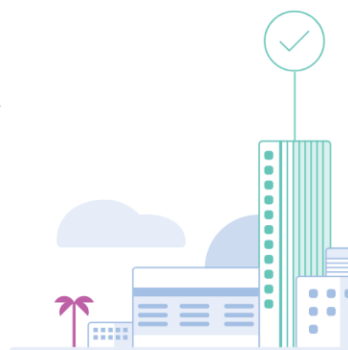
Step 3. On the welcome page click **Configure Cloud Service**.

Welcome to Cisco User Defined Network

Let's start with configuring the Service

Our first few steps require the configuration to happen in the cloud portal for this service. Once done with the service configuration, you will return to Cisco DNA Center to configure your network.

- ☑ Connect your Active Directory and Select Attributes
- ☑ Map Roles and Permissions for your users
- ☑ Customize the mobile application
- ☑ Open a secure connection with an Authentication Token between the cloud service and on-prem.



First steps...

[Configure Cloud Service](#)

Step 4. This will take you back to the UDN cloud, login if you are not already.

Step 5. Navigate to **System>Authentication Token**.

Step 6. Enter the FQDN for your Cisco DNA Center and then click **Generate New Token**.

Authentication Token

Connect cloud to DNA Center by following a few steps.

1. Ensure ISE is connected in DNAC.
2. Save the token into the DNAC Settings and make sure that UPN capabilities before provisioning.
3. In advanced settings, enable UPN in your network settings.

The token is only valid for 30 minutes, after which a new token must be generated.

Cisco DNA Center*

o21-dnac.ciscodna.net

Token

e0055719050140ce85e000c1ff42fbc51f
0756f758864ef090165e6e5a81e3f6

[Generate New Token](#)

Copy Token

Step 7. Once generated, click **Copy Token**.

4a9352dbb60247b5b4da3e62ac6301ee4
882a8c73c3e4338947c67046ae06f81

[Generate New Token](#)

Copy Token

Step 8. Navigate back to Cisco DNA Center and click **Next**.

Step 9. Paste the **Authentication Token** copied from the previous step and click **Connect**.

OK, now lets complete the connection with
the cloud service

Paste your authentication token below to complete the secure connection
between Cisco DNA Center and Cisco User Defined Network cloud service portal.

Authentication Token

Paste Token Here

Connect



Connection validated, please click Next to proceed



Step 10. You should now see the Connection validated message, click **Next** to continue.

Step 11. In the next screen, select the site you would like to deploy UDN and hit **Next**.

Tech tip

This must correspond with the Sites at which you deployed the SSID.

Which sites would you like the Cisco User Defined Network service to be enabled for in your network?

First select the campuses, buildings or floors that you would like to provide Cisco User Defined Network. In the next step, you will select the specific SSIDs from the sites you select here.

[Why are some of my sites not visible in the selection dropdown?](#)

Select Sites

☐ Disable User Defined Network Service

Search Dropdown

Global/RTP/RTP-1

Global/RTP/RTP-1/RTP-1-1

Step 12. In the next screen, select the SSID to be used for UDN and click **Next**.

Step 13. Optionally, click the slider next to **Unicast Traffic Containment**.

Tech tip

Unicast Traffic Containment enables segmentation of all traffic between different UDNs. Without this option only link-local multicast traffic is filtered between UDNs.

Almost Done! Lastly, define the SSIDs that will be used for Cisco User Defined Network.

For each site, select or confirm the SSIDs that you would like to include for the Cisco User Defined Network Service.

Global/RTP/RTP-6/RTP-6-1

SSID(s)*

Student-dorm

Controllers Included
o21-wlc.ciscodna.net

Unicast Traffic Containment



☐ Apply Individually ☒ Apply to all

Step 14. Select when you would like to provision and click **Next**.

Schedule when you would like to provision this in your network and when to activate the service.

Schedule your network provisioning below. Remember, end users will not be able to connect registered devices until deployment is successfully completed to your network.

☒ Now ☐ Later

Step 15. Look over the summary and when ready click **Configure**.





Configuration Summary

Review your details before completing configuration and if needed, make any changes.

Authentication Token

✔ Token Validated

Selected Sites & SSIDs [Edit](#)

Sites 	SSIDs 	Unicast Filtering	Controllers
Global/RTP/RTP-6/RTP-6-1	Student-dorm	Enabled for all	o21-wlc.ciscodna.net
1 Records			Show Records: 25  1 - 1 <  >

Scheduling [Edit](#)

Fri Jun 12 2020 15:02:00 GMT-0400 (Eastern Daylight Time)

Step 16. Your SSID will now be configured for UDN.

Done! Cisco User Defined Network has been configured.

Nice job! Your end users will now be able to create their personal network and connect registered devices, just like at home. What's next? You're done for now, but feel free to take a look at the options below.

1 site(s) and 1 SSID(s) Validation completed. Provision started. ✔

Tech tip

If the client VLAN spans multiple VLANs or the UDN SSIDs are on different VLANs mDNS gateway needs to be configured on the Catalyst 9800 WLC. These steps can be found in Appendix A: Configuring .

Operate

Process: Adding devices and Guests to UDN.

This section will go over the user experience in using the Cisco UDN application to add their devices as well as guest users.

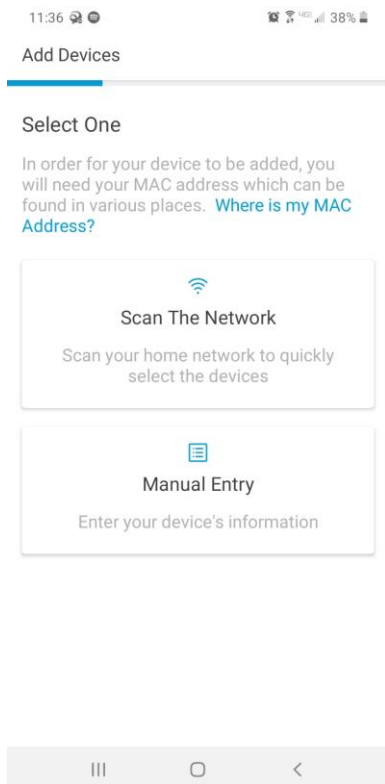
Procedure 1. Adding devices to UDN.

Step 1. Open the Cisco UDN mobile app and login using your email and password.

Step 2. Select **Manual Entry**.

Tech tip

The **Scan the Network** feature is currently only available on Android at this time. This option will allow you to scan the network you are currently connected to for endpoints.



Step 3. Enter the **Device Type** and give it a name.

1:08

39%

Manual Entry

Enter your device details

Fill in the following information so that your device will be added. [Where is my MAC Address?](#)

Device Type

Computer

Device Name

Bryan's Macbook Air

MAC Address

11:11:11:11:11:11

[Scan MAC Address](#)

Next

III

O

<

Step 4. Enter the MAC address manually or you can scan it in using your phones camera or a picture. Hit **Next** when finished.

Tech tip

If you get a message saying the device can only be added when on-premise. It is because it is using a randomized MAC address. You can either turn off this setting if available or wait until you are on the SSID before registering. More information can be found in [Appendix B](#).

This device can be added only when this device is connected to the on-premise network

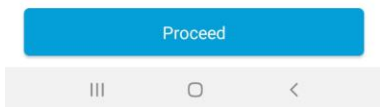
The MAC address entered is randomized, due to the nature of random MAC addresses, please add this device to the app once the device is connected to the on-premise network

Got it

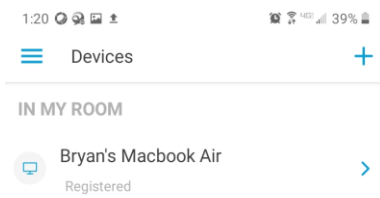


Great! Your 1 device(s) are being added.

Good news! Your devices are being added to your network and will be available in this app soon.

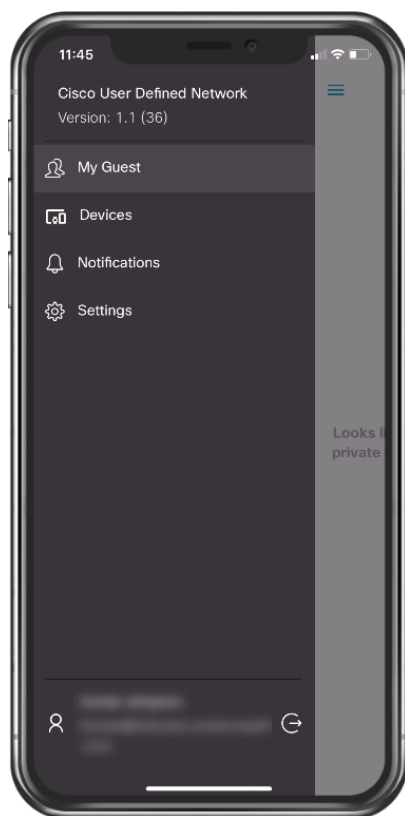


Step 7. Your device will now show up after a few seconds as registered.

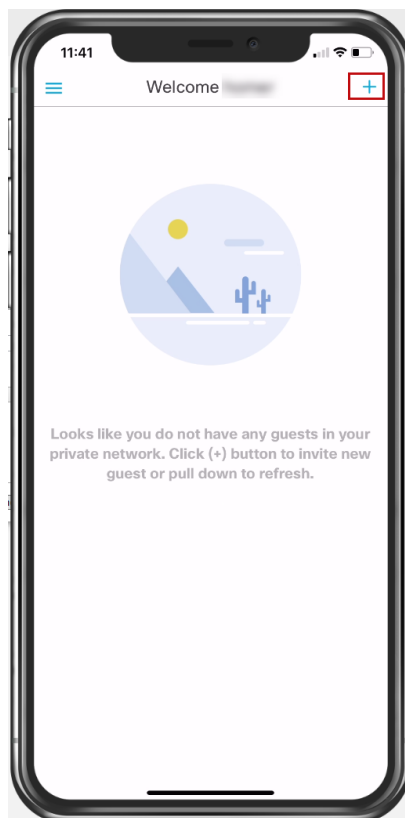


Procedure 2. Inviting Guest Users

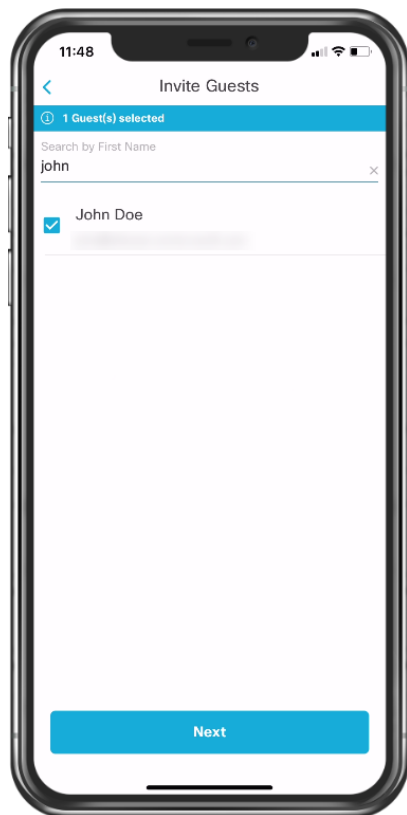
Step 1. In the Cisco UDN application, navigate to **My Guest**.



Step 2. On the **My Guest** page, click the + in the top right corner.



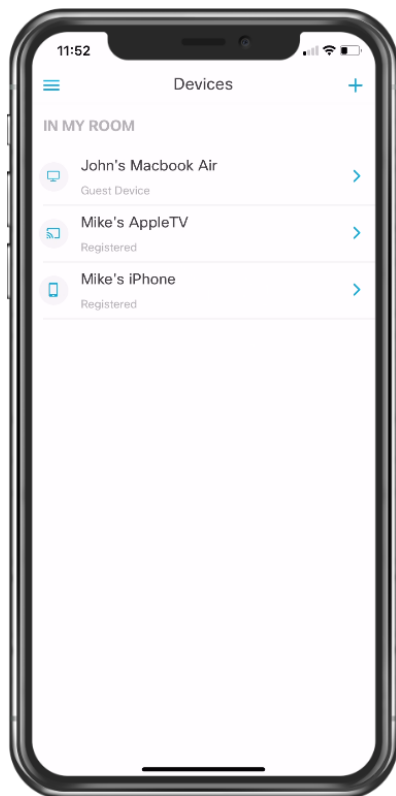
Step 3. In the search bar, start typing the name of the person you would like to invite. The person you are searching for will show up in the space below, select that user and click **Next**.



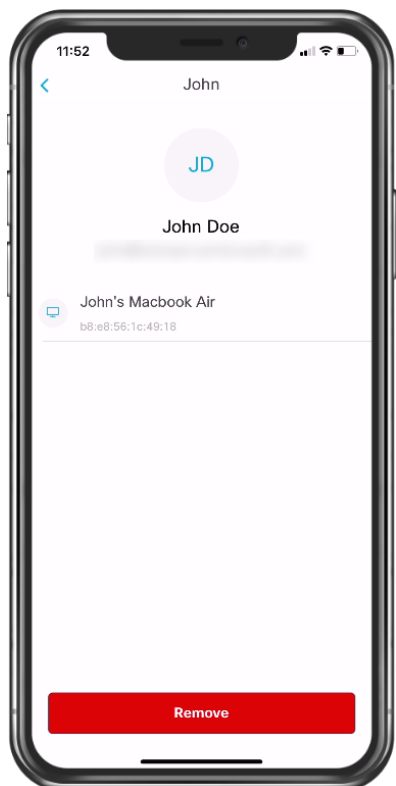
Step 4. Once accepted you will now see the invited user in the **My Guests** section.



Step 5. In the **Devices** section, you will now see the guest devices alongside the registered devices. These devices can now communicate freely with each other.

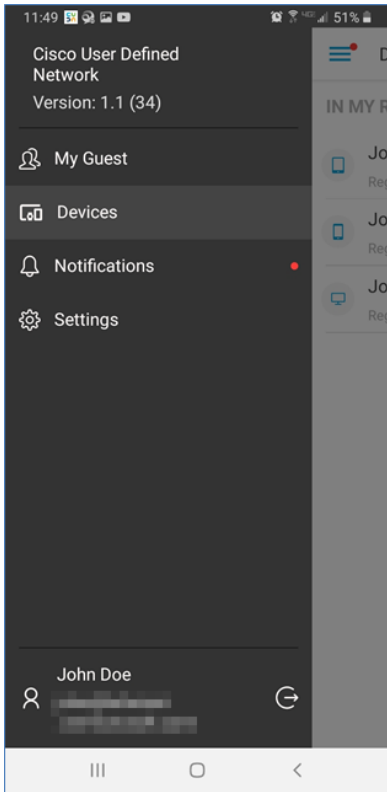


Step 6. To remove a guest user from your UDN. Select the user in the **My Guests** page and click **Remove**.



Procedure 3. Joining another user's UDN

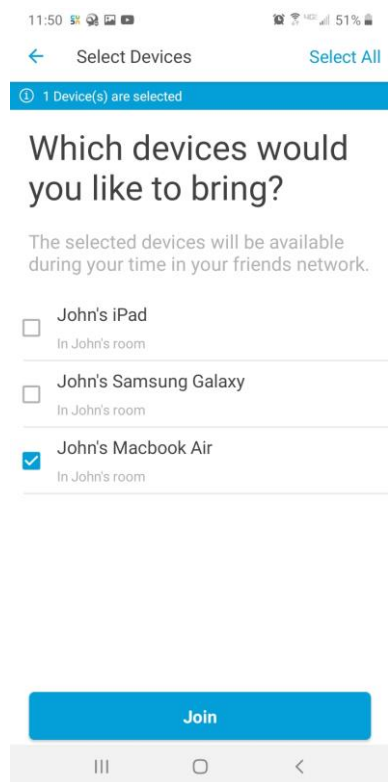
Step 1. When invited to join another user's UDN, you will receive a notification. To view this notification, hit the menu button then click **Notifications**.



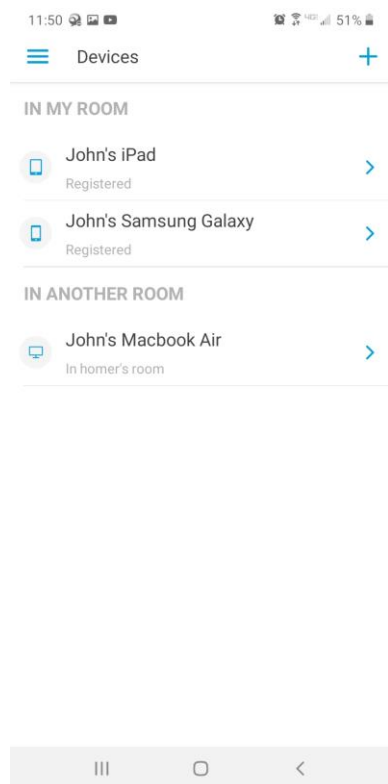
Step 2. Here you will see the invitation to join another room. Click the invitation and in the resulting pop up click **Accept**.



Step 3. On the next screen select the devices from your UDN you would like to bring over to the other user's room and click **Join**.



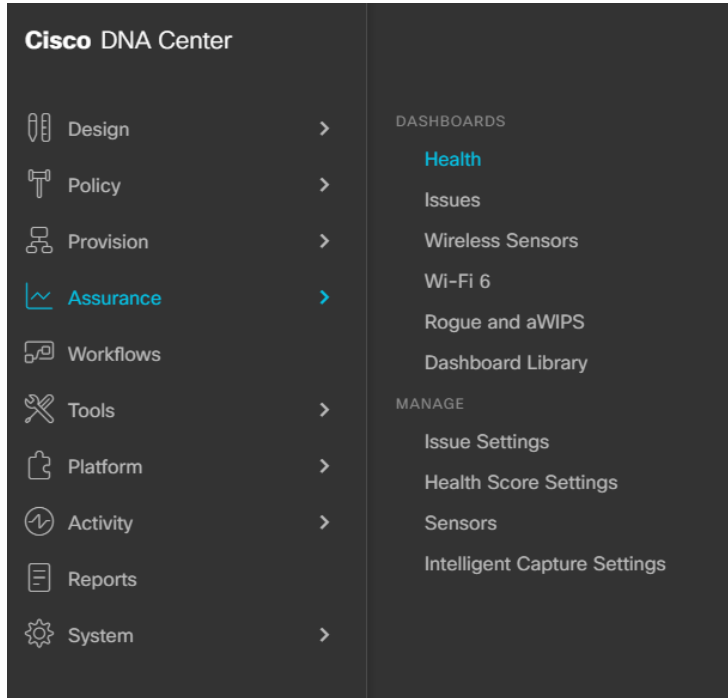
Step 4. Navigate back to **My Devices**. Notice that the device selected in the previous step is now under **In Another Room**. This device can now communicate freely with devices in the other user's room.



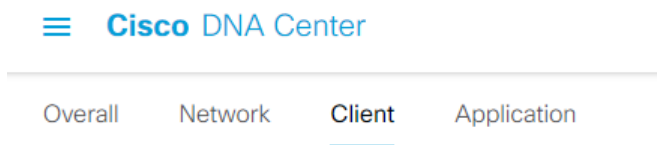
Process: Assurance and Troubleshooting

Procedure 1. Assurance with UDN

Step 1. Login to Cisco DNA Center and navigate to **Assurance>Health**.



Step 2. Click **Client**.



Step 3. Scroll down until you see the **Client Devices** section.

Client Devices (3)

LATEST TREND

TYPE **Wireless** Wired HEALTH **All** Inactive Poor Fair Good No Data

DATA Onboarding Time >= 10 s Association >= 5 s DHCP >= 5s Authentication >= 5 s RSSI <= -72 dBm SNR <= 9 dB

Filter

Identifier ⓘ	IPv4 Address	Device Type
F2-DA-AA-AE-36-6A	10.4.145.11	Linux-Workstation
C8-E0-EB-18-82-CC	10.4.145.15	Apple-Device
B8-E8-56-1C-49-18	10.4.145.14	OS_X-Workstation

Step 4. Click on the devices MAC address you would like to know more about. This will bring us to the **Client 360** page.

Step 5. Scroll down until you find the **Detail Information** section.


Detail Information Jun 19, 2020 12:34 PM

Device Info	Connectivity	RF	User Private Network
Information			
Device Type	Workstation		
Operating System	AppleCoreMedia/1.0.0.15G1217 (Macintosh; U; Intel Mac OS X 10_11_6; en_us)		
User Name	mac_B8:E8:56:1C:49:18		
Host Name	admins-Air		
MAC Address	B8:E8:56:1C:49:18		
IPv4 Address	10.4.145.14		
IPv6 Address	fe80:0:0:0:bae8:56ff:fe1c:4918		
Status	CONNECTED		
VLAN ID	45		

Step 6. Click the **User Private Network** tab. This will show you useful information including the UDN Name, Owner, UDN ID.

Step 7. Under Connected UDN we see all the other devices connected to this UDN.

Detail Information Jun 19, 2020 12:34 PM

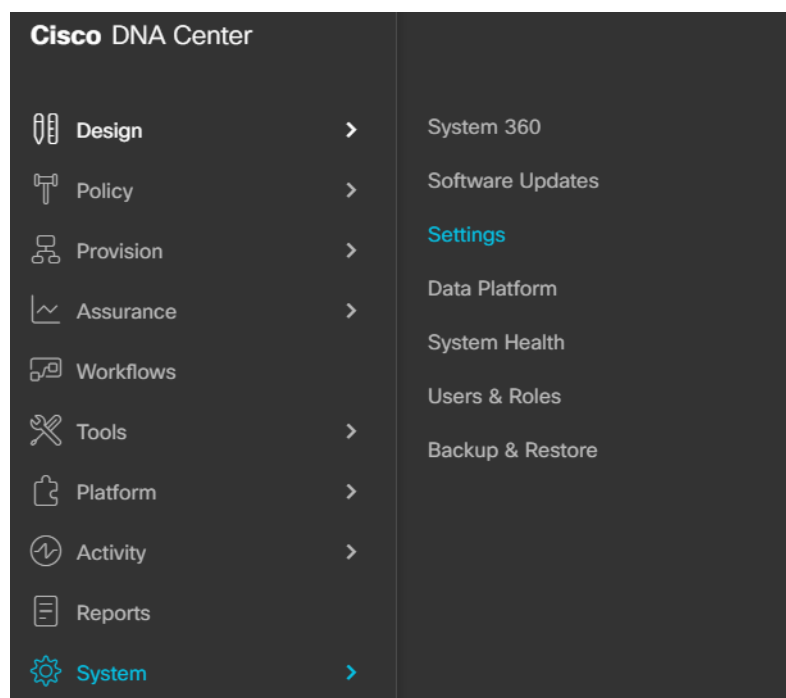
Device Info	Connectivity	RF	User Private Network	
REGISTERED UPN				
UPN Name	John's room			
UPN ID	16544774			
UPN Owner	John Doe			
CONNECTED UPN				
UPN Name	John's room			
UPN ID	16544774			
UPN Owner	John Doe			
Current Status	Active			
MAC Address 	Device Owner	Device Name	Device Type	Current Status
B8:E8:56:1C:49:18	John Doe	admins-Air	Workstation	connected
F2:DA:AA:AE:36:6A	John Doe	Galaxy-Note9	Linux-Workstation	disconnected

Procedure 2. UDN Configuration Verification

UDN Cloud to Cisco DNA Center Trust Established

This process will verify the trust relationship between the UDN Cloud and Cisco DNA Center.

Step 1. In Cisco DNA Center, navigate to **System>Settings**.



Step 2. Navigate to **External Services>Authentication Tokens**

Step 3. Verify the connection is established.

Settings / External Services

Authentication Tokens

Authenticate and open a secure connection between Cisco DNAC and User Private Networks Cloud portal through the use of token encryption keys.

[Where do I get my token key?](#)

[Replace Token?](#)

Connection Established

Your DNAC appliance is now connected to your User Private Network Cloud Portal.

[What are the next steps for setting up UPNs in DNAC?](#)



Step 4. Log in to the UDN Cloud and navigate to **System>Authentication Token**.

Step 5. Verify the connection is established to your Cisco DNA Center.

General

User Management

Authentication Token

Cisco Support

Single Sign-On

Authentication Token

✔ Connection established to your DNA Center.

Claimed to DNAC Name o21-dnac.cisco.com

[Disassociate](#)

ISE and Cisco DNA Center PxGrid Connection

This process will verify the connection between ISE and Cisco DNA Center is up.

Step 1. Login to ISE and navigate to **Administration>pxGrid Services**.

Administration Work Centers

System	Network Resources	pxGrid Services
Deployment	Network Devices	Feed Service
Licensing	Network Device Groups	Profiler
Certificates	Network Device Profiles	Threat Centric NAC
Logging	External RADIUS Servers	Third Party Vendors
Maintenance	RADIUS Server Sequences	
Upgrade	NAC Managers	
Backup & Restore	External MDM	
Admin Access	Location Services	
Settings		
Identity Management	Device Portal Management	
Identities	Blacklist	
Groups	BYOD	
External Identity Sources	Certificate Provisioning	
Identity Source Sequences	Client Provisioning	
Settings	Mobile Device Management	
	My Devices	
	Custom Portal Files	
	Settings	

Step 2. Under **All Clients**, see that your Cisco DNA Center subscriber name shows up.

All Clients	Web Clients	Capabilities	Live Log	Settings	Certificates	Permissions
✔ Enable	❌ Disable	✔ Approve	➕ Group	❌ Decline	❌ Delete	➕ Refresh
Total Pending Approval(0)						
<input type="checkbox"/>	Client Name	Description	Capabilities	Status		
<input type="checkbox"/>	▶ ise-bridge-o21-ise		Capabilities(0 Pub, 4 Sub)	Online (XMPP)		
<input type="checkbox"/>	▶ ise-admin-o21-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)		
<input type="checkbox"/>	▶ ise-fanout-o21-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)		
<input type="checkbox"/>	▶ ise-pubsub-o21-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)		
<input type="checkbox"/>	▶ ise-mnt-o21-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)		
<input type="checkbox"/>	▶ o21-ise		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		
<input type="checkbox"/>	▶ pxgrid_client_1591847592_dnac_ndp		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		
<input type="checkbox"/>	▶ pxgrid_client_1591847592		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		

Tech tip

Note that this is showing up as Offline, this is expected as newer Cisco DNA Centers are using PxGrid v2.

Step 3. Click the **Web Clients** tab.

Step 4. See that your Cisco DNA Center subscriber name shows up and the status here is **ON**.

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
Client Name						IP Address	
ise-mnt-o21-ise	o21-ise	o21-ise-2955	CN=o21-ise.cisc...	/topic/com.cisco.ise.se...	/topic/com.cisco.ise.se...	10.4.168.50	ON
pxgrid_client_1591847592	o21-ise	o21-ise-2970	CN=admin			10.4.168.3	ON
ise-admin-o21-ise	o21-ise	o21-ise-2977	CN=o21-ise.cisc...			10.4.168.50	ON
ise-fanout-o21-ise	o21-ise	o21-ise-2978	CN=o21-ise.cisc...	/topic/wildcard		127.0.0.1	ON
pxgrid_client_1591847592_dnac_ndp	o21-ise	o21-ise-2982	CN=admin	/topic/com.cisco.ise.co...		10.4.168.3	ON
ise-fanout-o21-ise	o21-ise	o21-ise-2984	CN=o21-ise.cisc...	/topic/distributed	/topic/distributed	10.4.168.50	ON
ise-bridge-o21-ise	o21-ise	o21-ise-2985	CN=o21-ise.cisc...			127.0.0.1	OFF
ise-bridge-o21-ise	o21-ise	o21-ise-2986	CN=o21-ise.cisc...			127.0.0.1	ON

ISE Policy for UDN

This process will verify the UDN Authorization Profile has been pushed.

Step 1. Login 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.

▼ Authorization Policy (12)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
Search							
✓	Wireless Black List Default	AND	<div>Wireless_Access</div> <div>IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist</div>	<div>× Blackhole_Wireless_Access</div> <div>× UPN</div>	<div>Select from list</div>	0	⚙
✓	Profiled Cisco IP Phones	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled Cisco-IP-Phone		<div>× Cisco_IP_Phones</div> <div>× UPN</div>	<div>Select from list</div>	0	⚙
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones		<div>× Non_Cisco_IP_Phones</div> <div>× UPN</div>	<div>Select from list</div>	0	⚙
⚠	Unknown_Compliance_Redirect	AND	<div>Network_Access_Authentication_Passed</div> <div>Compliance_Unknown_Devices</div>	<div>× Cisco_Temporal_Onboard</div> <div>× UPN</div>	<div>Select from list</div>	0	⚙
⚠	NonCompliant_Devices_Redirect	AND	<div>Network_Access_Authentication_Passed</div> <div>Non_Compliant_Devices</div>	<div>× Cisco_Temporal_Onboard</div> <div>× UPN</div>	<div>Select from list</div>	0	⚙
⚠	Compliant_Devices_Access	AND	<div>Network_Access_Authentication_Passed</div> <div>Compliant_Devices</div>	<div>× PermitAccess</div> <div>× UPN</div>	<div>Select from list</div>	0	⚙

UDN Enabled on Catalyst 9800

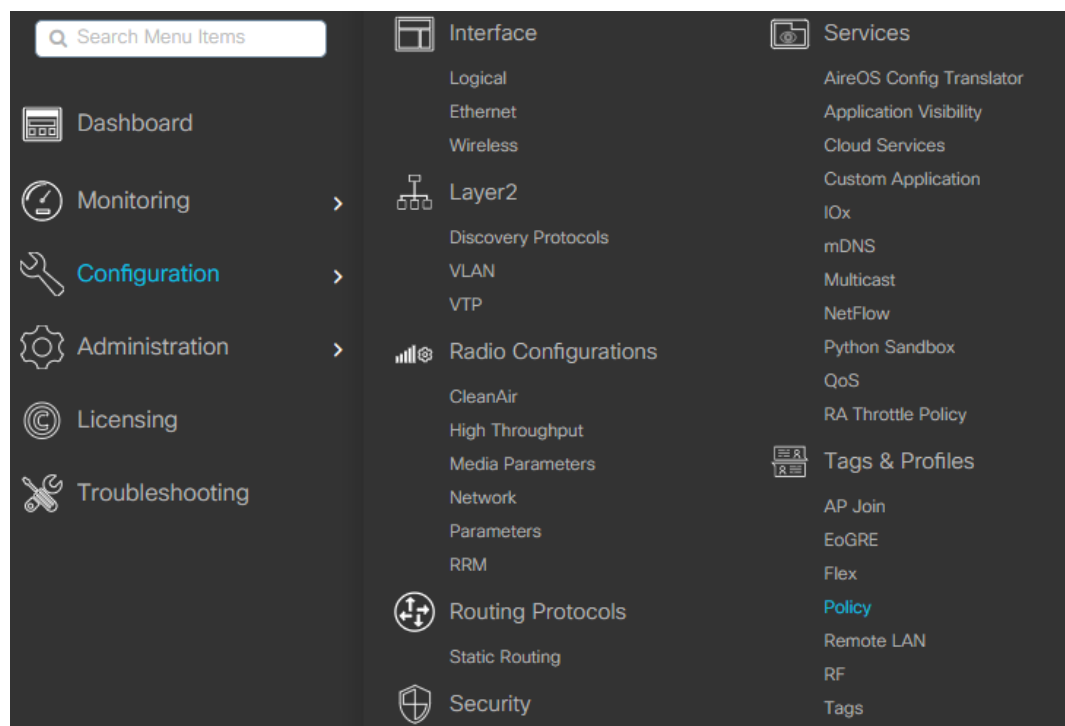
This process will verify the UDN configuration has been pushed to the Catalyst 9800.

Tech tip

An AP must be attached to the Catalyst 9800 for this process to show up.

Step 1. Login to the Catalyst 9800 WLC.

Step 2. Navigate to **Configuration>Tags & Profiles>Policy**.



Step 3. Click the Policy Profile used for UDN.

[Configuration](#) > [Tags & Profiles](#) > [Policy](#)

+ Add × Delete

	Status	Policy Profile Name
<input type="checkbox"/>	✓	default-policy-profile
<input type="checkbox"/>	✓	Student-do_Global_NF_bf4ccc47

1 10 items per page

Step 4. Under the **Advanced** tab check to make sure the UDN Status box is checked and optionally, Drop Unicast if selected earlier during the Cisco DNA Center UDN workflow. Also, make sure that under **AAA Policy** the **Policy Name** is set to **default-aaa-policy** and that **Accounting List** is set to **default**.

Tech tip

The Account List setting is necessary for both WPA2 Enterprise and PSK for CoA to function correctly at the WLC for UDN enabled WLANs. Normally with PSK it is not necessary to make use of RADIUS accounting, however, for CoA to function correctly during a room change for a registered UDN device, the default list must be specified.

Edit Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)	<input type="text" value="1800"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="180"/>
Guest LAN Session Timeout	<input type="checkbox"/>

DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

[Show more >>>](#)

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input type="checkbox"/>
Policy Name	<input type="text" value="default-aaa-policy"/> <input type="button" value="x"/>
Accounting List	<input type="text" value="default"/> <input type="button" value="i"/> <input type="button" value="x"/>

Fabric Profile	<input type="checkbox"/> <input type="text" value="Search or Select"/>
mDNS Service Policy	<input type="text" value="default-mdns-service"/> <input type="button" value="Clear"/>
Hotspot Server	<input type="text" value="Search or Select"/>

User Defined (Private) Network

Status	<input checked="" type="checkbox"/>
Drop Unicast	<input checked="" type="checkbox"/>

Umbrella

Umbrella Parameter Map	<input type="text" value="Not Configured"/> <input type="button" value="Clear"/>
Flex DHCP Option for DNS	<input checked="" type="checkbox"/> <input type="button" value="ENABLED"/>
DNS Traffic Redirect	<input type="checkbox"/> <input type="button" value="IGNORE"/>

WLAN Flex Policy

VLAN Central Switching	<input type="checkbox"/>
Split MAC ACL	<input type="text" value="Search or Select"/>

Air Time Fairness Policies

2.4 GHz Policy	<input type="text" value="Search or Select"/>
----------------	---

Procedure 3. Troubleshooting Commands

This section will go over useful commands when troubleshooting UDN.

Catalyst 9800 Wireless LAN Controller

These commands will be run on the Catalyst 9800.

show wireless client udn

This command will show all the clients currently connected and which UDN they are connected to.

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

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 crypto pki trustpoints

This command can be used to verify the Certificates are present.

```
o21-wlc#show wireless profile policy detailed pol
o21-wlc#show crypto pki trustpoints
Trustpoint TP-self-signed-646034279:
  Subject Name:
    cn=IOS-Self-Signed-Certificate-646034279
    Serial Number (hex): 01
  Persistent self-signed certificate trust point
  Using key label TP-self-signed-646034279
```

```
Trustpoint SLA-TrustPoint:
  Subject Name:
    cn=Cisco Licensing Root CA
    o=Cisco
    Serial Number (hex): 01
  Certificate configured.
```

```
Trustpoint DNAC-CA:
  Subject Name:
    ou=Cisco DNA Center
    o=Cisco Systems
    cn=2ada7115-490e-7abb-b4df-91ae5b093905
    Serial Number (hex): 00D2D34FE7F3EBC1BB
  Certificate configured.
```

```
Trustpoint ca:
  Subject Name:
    c=US
    st=California
    l=San Jose
    o=Cisco Virtual Wireless LAN Controller
    cn=CA-vWLC/emailAddress=support@vwlc.com
    Serial Number (hex): 01
  Certificate configured.
```

```
Trustpoint ewlc-tp1:
  Subject Name:
    c=US
    st=California
    l=San Jose
    o=Cisco Virtual Wireless LAN Controller
    cn=CA-vWLC/emailAddress=support@vwlc.com
    Serial Number (hex): 01
  Certificate configured.
  SCEP URL: http://10.4.146.5:80/cgi-bin
```

```
Trustpoint sdn-network-infra-iwan:
  Subject Name:
    cn=sdn-network-infra-ca
    Serial Number (hex): 790EF0235D403915
  Certificate configured.
```

show network-assurance summary

This command can be used to verify assurance connectivity.

```
o21-wlc#sh network-assurance summary
-----
Network-Assurance           : True
Server Url                  : https://10.4.168.4
ICap Server Port Number    : 32626
Sensor Backhaul SSID       :
Authentication              : Unknown
AP client event frequency (seconds) : 30
```

show telemetry internal connection

```
o21-wlc#show telemetry internal connection
Telemetry connections

Index Peer Address      Port  VRF Source Address  Peer      State
-----
1 10.4.168.4            25103  0 10.4.146.5        <unknown> Active
```

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

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

```
o21-wlc#show wireless profile policy detailed Student-do_Global_NF_bf4ccc47 | include User
User Defined (Private) Network      : Enabled
User Defined (Private) Network Unicast Drop : Enabled
```

show tech-support wireless udn

This command shows a ton of useful information when troubleshooting.

```
s21-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): 0xa8cfb325ec1b97fe568a1a0d792de71/0x00000000000000000000000000000000
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
b49e.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
```

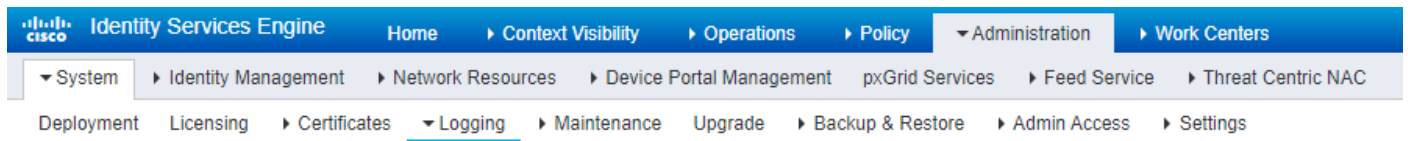
ISE

This section will provide troubleshooting information for Cisco ISE.

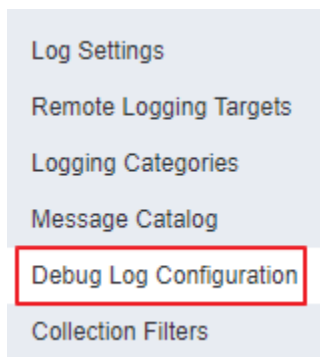
Turning on UDN logging on Cisco ISE.

Before we can view the UDN Logs, we must first turn logging on.

Step 1. On ISE, Navigate to **Administration>System>Logging**.





Step 2. Select **Debug Log Configuration**.



Step 3. Select your Node from the list.



Node List

 Edit
  Reset to Default

Node Name	Replication Role
<input type="radio"/> o21-ISE	STANDALONE

Step 4. Scroll down on the list until you see **UPN** under Component Name.

Step 5. Change the log level of UPN to **DEBUG** and click Save.

 Edit
  Reset to Default

Component Name	Log Level	Description
<input type="radio"/> prrt-JNI	INFO	prrt policy decision request processing layer related messages
<input type="radio"/> pxgrid	INFO	pxGrid messages
<input type="radio"/> RBAC	INFO	Rbac related messages
<input type="radio"/> Replication-Deployment	INFO	Logger related to Deployment Registration,Deregistration,Sync and In...
<input type="radio"/> Replication-JGroup	WARN	Logger related to JGroup Node State
<input type="radio"/> ReplicationTracker	INFO	PSC replication related debug messages
<input type="radio"/> report	INFO	Debug reports on M&T nodes
<input type="radio"/> RuleEngine-Attributes	INFO	Additional rule evaluation attributes in audit logging at DEBUG
<input type="radio"/> RuleEngine-Policy-IDGroups	INFO	Additional policy vs id group audit logging at DEBUG
<input type="radio"/> runtime-AAA	WARN	AAA runtime messages (prrt)
<input type="radio"/> runtime-config	WARN	AAA runtime configuration messages (prrt)
<input type="radio"/> runtime-logging	WARN	customer logs center messages (prrt)
<input type="radio"/> saml	INFO	SAML messages
<input type="radio"/> scep	INFO	SCEP log messages
<input type="radio"/> session-trace	INFO	Session Trace messages
<input type="radio"/> sgtbinding	INFO	SGT binding
<input type="radio"/> spog	DEBUG	Spog-app exim messages
<input type="radio"/> sponsorportal	INFO	Sponsor portal debug messages
<input type="radio"/> sse-connector	INFO	SSE Connector related log messages
<input type="radio"/> swiss	INFO	Swiss protocol internal messages
<input type="radio"/> sxp	INFO	SXP Listener messages
<input type="radio"/> TC-NAC	INFO	TC-NAC log messages
<input type="radio"/> threshold-counter	INFO	Threshold Counters
<input type="radio"/> Trustsec	INFO	TrustSec related messages
<input type="radio"/> UPN	DEBUG	User Private Network messages
<input type="radio"/> va-runtime	INFO	Vulnerability Assessment Runtime messages
<input type="radio"/> va-service	INFO	Vulnerability Assessment Service messages
<input type="radio"/> vcs	INFO	Context directory debug messages
<input type="radio"/> vcs-db	INFO	Indexing Engine debug messages
<input type="radio"/> wirelesssetuphelper	INFO	Wireless Setup Helper debug messages

Tech tip

The name UPN will be changed to UDN in future releases.

Step 6. Now that we have logging on, we can now 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:

```

ISE Live Logs

Operations>RADIUS>Live Logs

Successful authentication of a registered device:

Private-group-id	Private-group-id=16762216
Private-group-name	Private-group-name=homer's room
Private-group-owner	Private-group-owner=1
RADIUS Username	B8:5D:0A:A0:47:EC
NAS-Identifier	o21-wlc
Device IP Address	10.4.146.5
CPMSessionID	0592040A0000000CE7F915AE
Called-Station-ID	00-d7-8f-c9-38-40:Student-dorm
CiscoAVPair	service-type=Call Check, audit-session-id=0592040A0000000CE7F915AE, method=mab, client-iiif-id=4261413430, vlan-id=45, cisco-wlan-ssid=Student-dorm, wlan-profile-name=Student-do_Global_NF_bf4ccc47

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
- 15048 Queried PIP - Normalised Radius.RadiusFlowType
- 15041 Evaluating Identity Policy
- 15013 Selected Identity Source - Internal Endpoints
- 24209 Looking up Endpoint in Internal Endpoints IDStore - B8:5D:0A:A0:47:EC
- 24211 Found Endpoint in Internal Endpoints IDStore
- 22037 Authentication Passed
- 24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
- 15036 Evaluating Authorization Policy
- 15048 Queried PIP - Radius.NAS-Port-Type
- 15048 Queried PIP - EndPoints.LogicalProfile
- 15048 Queried PIP - Network Access.AuthenticationStatus
- 15016 Selected Authorization Profile - PermitAccess,UPN
- 15016 Selected Authorization Profile - PermitAccess,UPN
- 15048 Queried PIP - UPN.Private-group-id
- 24209 Looking up Endpoint in Internal Endpoints IDStore - B8:5D:0A:A0:47:EC
- 24211 Found Endpoint in Internal Endpoints IDStore
- 11002 Returned RADIUS Access-Accept

Successful authentication of an unregistered device:

Name	Endpoint Identity Groups:Unknown
RADIUS Username	B4:9C:DF:89:BB:A6
NAS-Identifier	o21-wlc
Device IP Address	10.4.146.5
CPMSessionID	0592040A0000001DEB76DA42
Called-Station-ID	00-d7-8f-c9-38-40:Student-dorm
CiscoAVPair	service-type=Call Check, audit-session-id=0592040A0000001DEB76DA42, method=mab, client-iiid=1811940745, vlan-id=45, cisco-wlan-ssid=Student-dorm, wlan-profile-name=Student-do_Global_NF_bf4ccc47

Result

UserName	B4:9C:DF:89:BB:A6
User-Name	B4-9C-DF-89-BB-A6
Service-Type	Administrative
Class	CACS:0592040A0000001DEB76DA42:o21-ISE/380150263/1576
cisco-av-pair	profile-name=Unknown
LicenseTypes	Base license consumed

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
- 15048 Queried PIP - Normalised Radius.RadiusFlowType
- 15041 Evaluating Identity Policy
- 15013 Selected Identity Source - Internal Endpoints
- 24209 Looking up Endpoint in Internal Endpoints IDStore - B4:9C:DF:89:BB:A6
- 24211 Found Endpoint in Internal Endpoints IDStore
- 22037 Authentication Passed
- 24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
- 15036 Evaluating Authorization Policy
- 15048 Queried PIP - Radius.NAS-Port-Type
- 15048 Queried PIP - EndPoints.LogicalProfile
- 15048 Queried PIP - Network Access.AuthenticationStatus
- 15016 Selected Authorization Profile - PermitAccess,UPN
- 15016 Selected Authorization Profile - PermitAccess,UPN
- 15048 Queried PIP - UPN.Private-group-id
- 15048 Queried PIP - UPN.Private-group-name
- 15048 Queried PIP - UPN.Private-group-owner
- 15043 Dynamic attribute value is unavailable
- 24209 Looking up Endpoint in Internal Endpoints IDStore - B4:9C:DF:89:BB:A6
- 24211 Found Endpoint in Internal Endpoints IDStore
- 11002 Returned RADIUS Access-Accept



Device registration CoA:

Steps

```
11100 RADIUS-Client about to send request - ( port = 1700 , type = Cisco CoA )
11101 RADIUS-Client received response
```

Other Attributes

ConfigVersionId	55
Event-Timestamp	1593090786
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
CoASourceComponent	UPN Cloud triggered
CoAReason	UPN change
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
Device IP Address	10.4.146.5
CPMSessionID	c6df3313-c1c5-4b23-9cea-965af7672348
CiscoAVPair	Private-group-id=16715577, Private-group-name=Jane's room, Private-group-owner=1

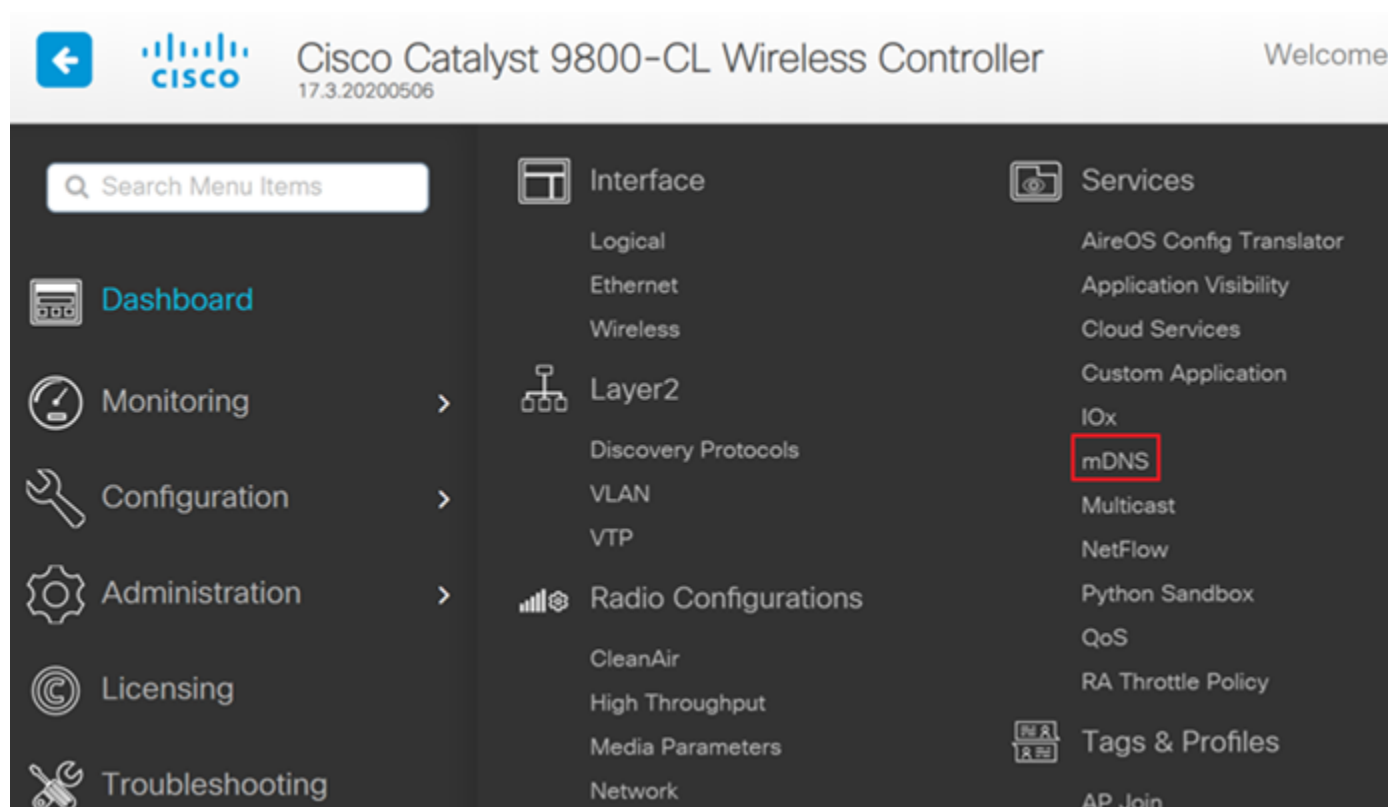
Appendix A: Configuring mDNS Gateway

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.

Tech tip

The mDNS Gateway feature on the Catalyst 9800 controller is incompatible with other Cisco solutions such as DNA Services for Bonjour or Wide Area Bonjour implemented at Cisco DNA Center. It should only be used in settings where these other services haven't been implemented.

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



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

Configuration ▾ > Services ▾ > mDNS

Global Service Policy mDNS Flex Profile

mDNS Gateway

ENABLED ☒

Transport

ipv4 ▾

Active-Query Timer *

30

mDNS-AP Service Policy

default-mdns-service ▾

[Clear](#)

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

Configuration ▾ > Tags & Profiles ▾ > WLANs

[+ Add](#) [× Delete](#) [Enable WLAN](#) [Disable WLAN](#)

Number of WLANs selected : 0

<input type="checkbox"/>	Status ▾	Name ▾	ID ▾	SSID ▾	Security ▾
<input type="checkbox"/>		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 mDNS Mode dropdown to **Gateway**. Click **Update & Apply** when finished.

Edit WLAN ✕

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

General

Security

Advanced

Add To Policy Tags

Coverage Hole Detection

☒

Aironet IE

☐

P2P Blocking Action

Disabled

Multicast Buffer

DISABLED

Media Stream Multicast-direct

☐

11ac MU-MIMO

☒

Max Client Connections

Per WLAN

0

Per AP Per WLAN

0

Per AP Radio Per WLAN

200

11v BSS Transition Support

Universal Admin

☐

Load Balance

☐

Band Select

☐

IP Source Guard

☐

WMM Policy

Allowed

mDNS Mode

Gateway

Off Channel Scanning

Bridging

Gateway

Drop

Defer Priority

☐ 0

☐ 1

☐ 2

☐ 3

☐ 4

☒ 5

☒ 6

☐ 7

Scan Defer Time

100

Cancel

Update & Apply to Device

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

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

Tech tip

The Cisco UDN solution does not solve the problem of Universal Plug and Play (UPnP) across VLANs.

Appendix B: Randomized MAC Address

MAC Addresses are being used to track and log users in public spaces, this data is then used for marketing purposes or sold to third parties. To combat this, device manufacturers have implemented random MAC addresses. This makes the user MAC address unique per network making companies unable to track the device. The address is kept consistent per network, meaning once associated with an SSID it will not have to authenticate again. This is why when using a device with random MAC address with UDN you must be on the UDN SSID before registering the device.

Appendix C: Disabling Airplay Discovery/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 an environment such as university dormitories, hospitals, and long term healthcare facilities as an example, these

default settings will allow other people to not only discover but stream to your Apple TV as well if they are on the same wired or wireless network or within 30 feet of the device in the case of Bluetooth.

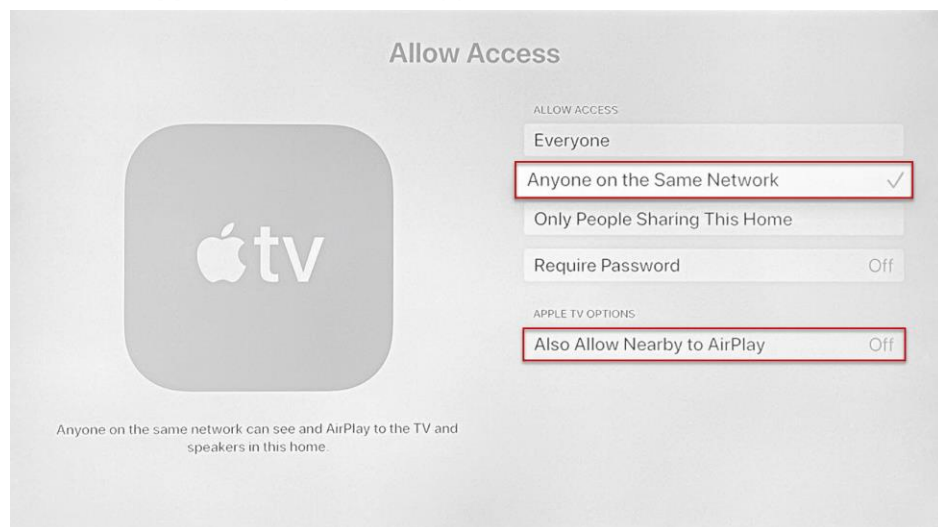
When deploying Cisco UDN, discovery and streaming is limited to registered devices within the UDN for wired and wireless devices such as MacBooks, iPhones, and iPads. For the Apple TV, if the AirPlay settings are left in their default state however, devices with Bluetooth enabled and within roughly 30 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 UDN is to optimize the user experience by displaying only those AirPlay devices within the UDN, it might be optimal for the organization deploying the solution to recommend that Apple TVs have Bluetooth disabled by their owners when installing them in their rooms. Unfortunately, there is no single button/setting to disable Bluetooth on the Apple TV and so the following procedure details how this is accomplished.

4. From the Apple TV home screen select **Settings**.



5. Select **AirPlay and HomeKit**.
6. Select **Allow Access** (Default is Everyone).
7. Change from **Everyone** to **Anyone on the Same Network**
8. An **Apple TV Options** box appears in which you need to change **Also Allow Nearby to AirPlay** to **Off**.



Feedback

For comments and suggestions about this guide and related guides, join the discussion on [Cisco Community](https://cs.co/en-cvds) at <https://cs.co/en-cvds>.