

From Zero to Hero with Catalyst Center

Adoption Insights from the Frontline

Martyn Rees
Customer Success Specialist

cisco Live !

Session ID: BRKOPS-2067

Cisco Webex App

Questions?

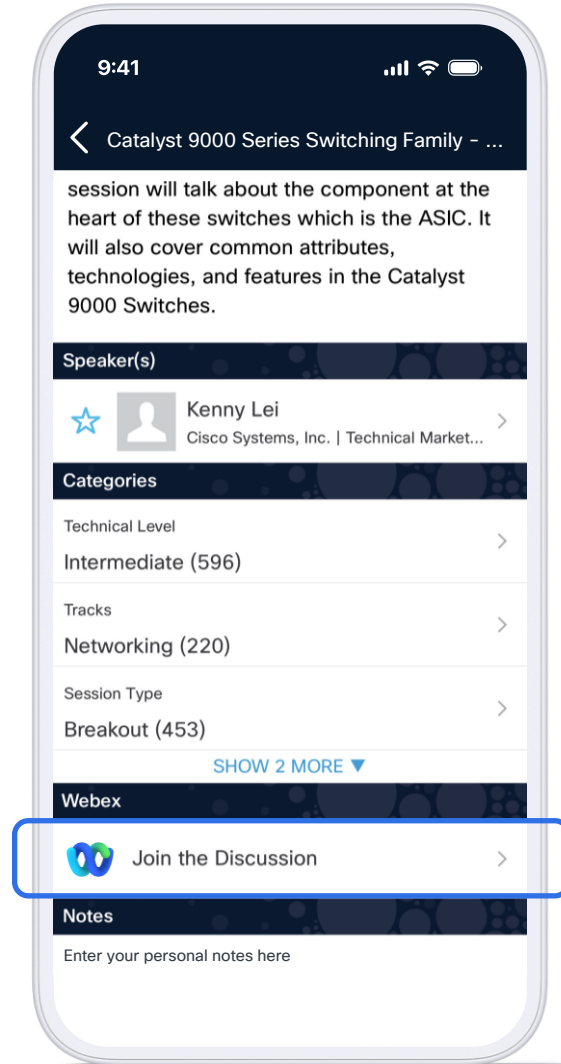
Use Cisco Webex App to chat with the speaker after the session



How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-2067>

Agenda

- 01 Introduction
- 02 A Checklist for Success
- 03 AI-RRM
- 04 Integrations
- 05 API's
- 06 Closing



About Me

Customer Success Specialist @ Cisco – Campus Networking

Joined Cisco in 2021

Adelaide Based





A Checklist for Success:

Things you should configure

Things you should configure: General Settings

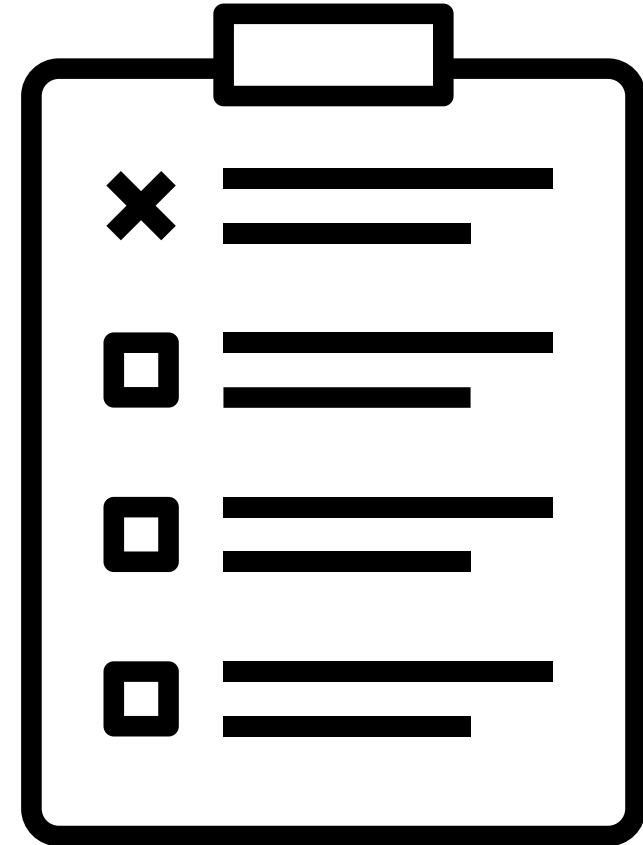
2.3.7.9

Common

- ☐ Revocation Check
- ☐ Wired Endpoint Data Collection
- ☐ Device Credentials
- ☐ Trusted Certificates
- ☐ Cisco.com Credentials
- ☐ Smart Account
- ☐ Smart Licensing
- ☐ SSM Connection Mode
- ☐ Device Controllability: enable autocorrect telemetry config
- ☐ Device EULA Acceptance
- ☐ Configuration Archive
- ☐ Cisco AI Analytics
- ☐ Building your Network Hierarchy

Appliance only

- ☐ System Health: CIMC Credentials

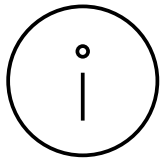


Revocation Check



For your
reference

Design > Network Settings > Security & Trust > Revocation - Check



This applies to the **self-signed** certificate or **your own** certificate.

The **self-signed** doesn't have a CRL so the recommended setting is "*Revocation - Check: None*".

Your own certificate may have a CRL.

Catalyst Center

Design / Network Settings

Servers Device Credentials IP Address Pools Wireless Telemetry **Security and Trust**

Find Hierarchy Search Help

Global

Australia

New Zealand

Certificate Revocation Check

If Device Controllability is enabled, the Controller Certificates device settings will be configured on the device when it is assigned to a site. This certificate revocation check requires access to the Certificate Authority that publishes the Certificate Revocation List (CRL). The default revocation-check is "crl none" which will check CRL first and then permit connection if not available. Select "none" to skip CRL check altogether.

Revocation Check CLI to configure on the device

Revocation - Check: CRL None

Revocation - Check: CRL None

Revocation - Check: None

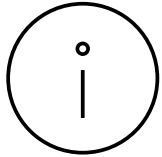
```
! Revocation - Check: CRL none
crypto pki trustpoint DNAC-CA
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check crl none
source interface Loopback0
hash sha256
```

```
! Revocation - Check: none
crypto pki trustpoint DNAC-CA
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check none
source interface Loopback0
hash sha256
```

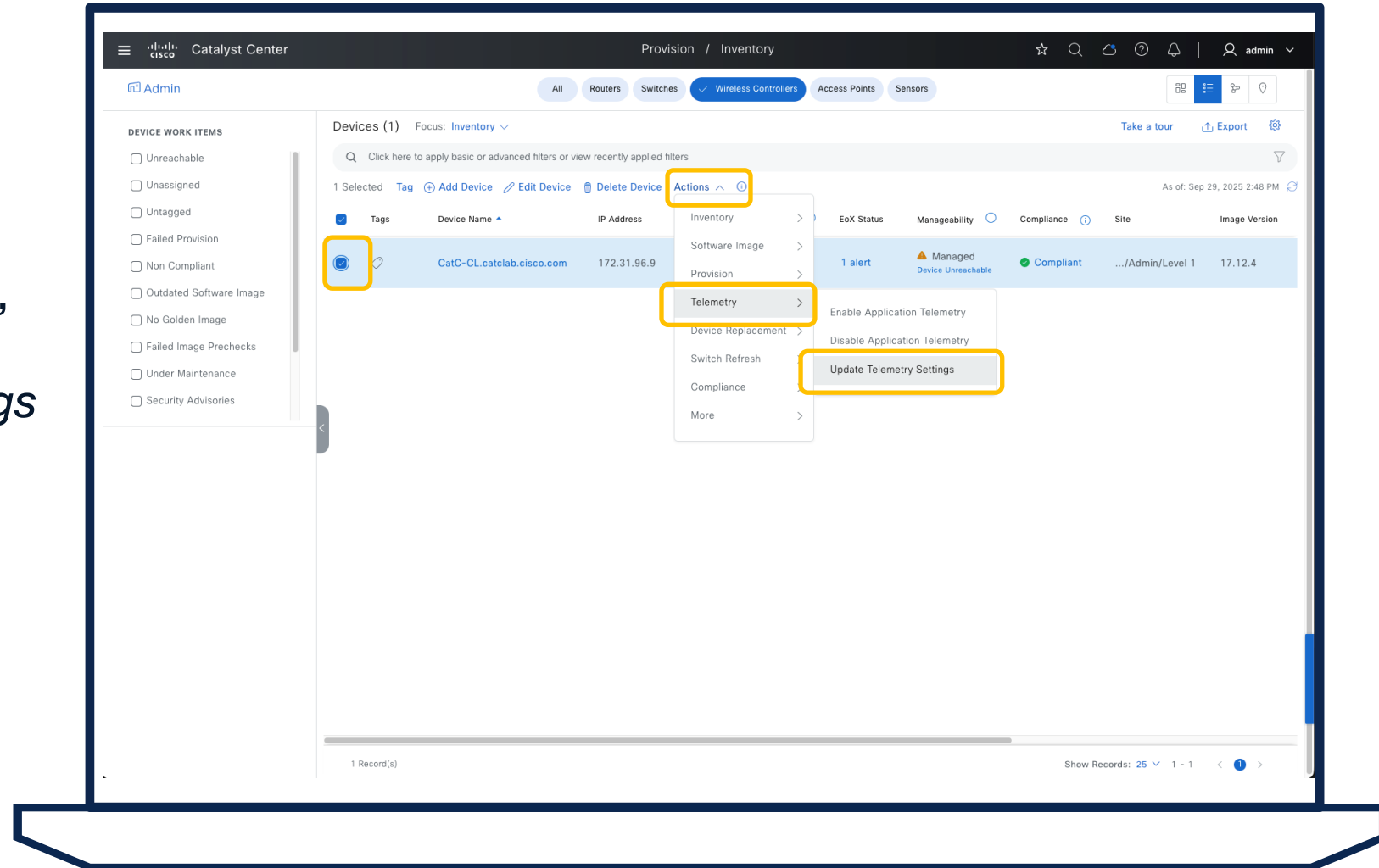
Save

Revocation Check

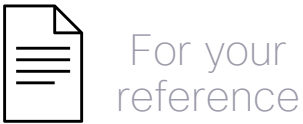
Design > Network Settings > Security & Trust > Revocation - Check



To apply this change to devices you can go to inventory, select devices, *Actions > Telemetry > Update Telemetry Settings*



Wired Endpoint Data Collection

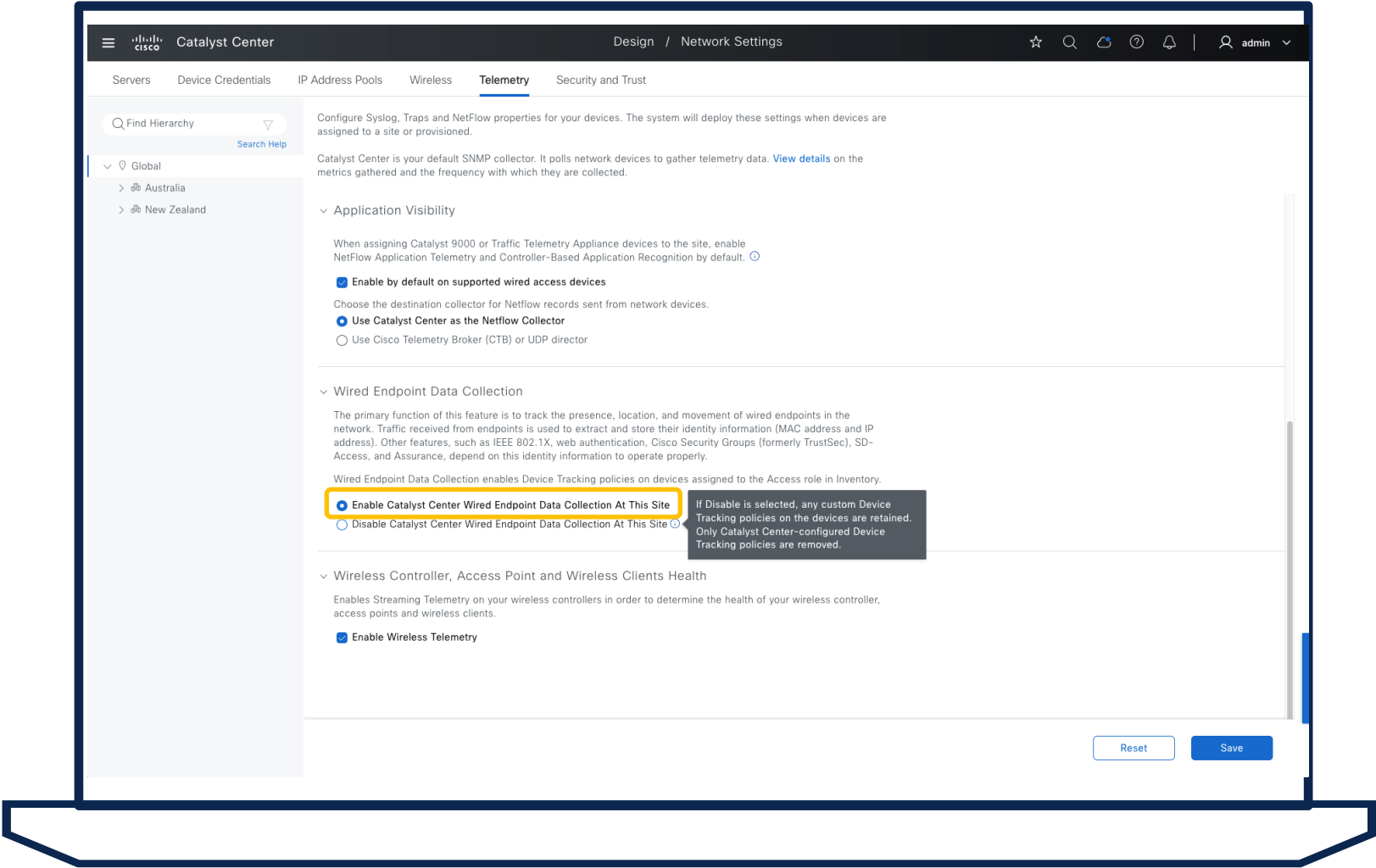


For your
reference

Design > Network Settings > Telemetry > Enable Catalyst Center Wired Endpoint Data Collection At This Site

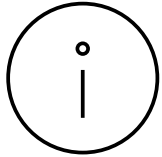


Applies to switching only!



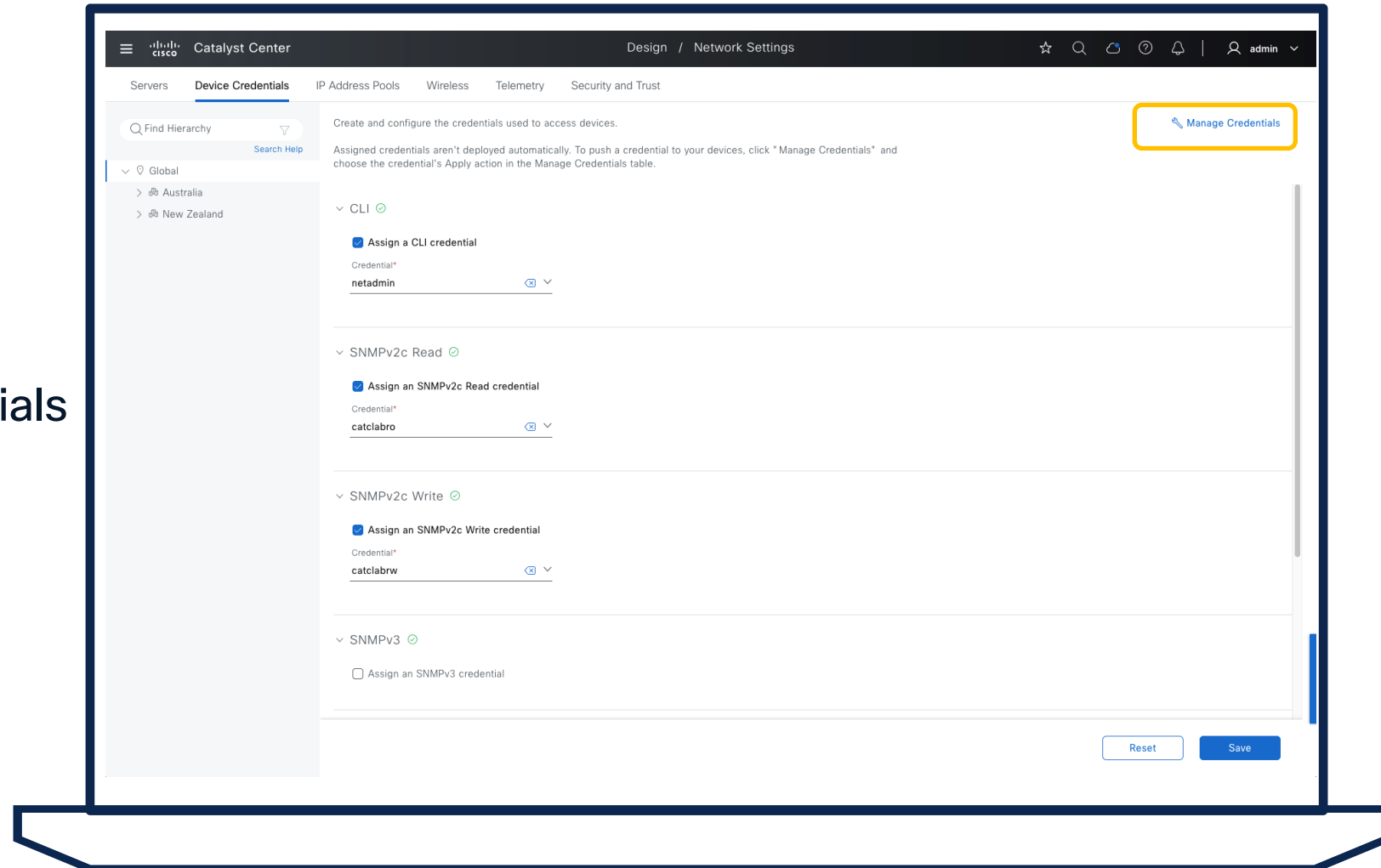
Device Credentials

Design > Network Settings > Device Credentials



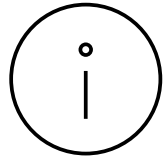
You can do it before a discovery or during the discovery.

If you do it during the discovery assign credentials to the global level.



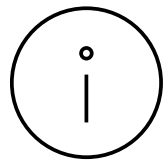
Device Credentials

Design > Network Settings > Device Credentials

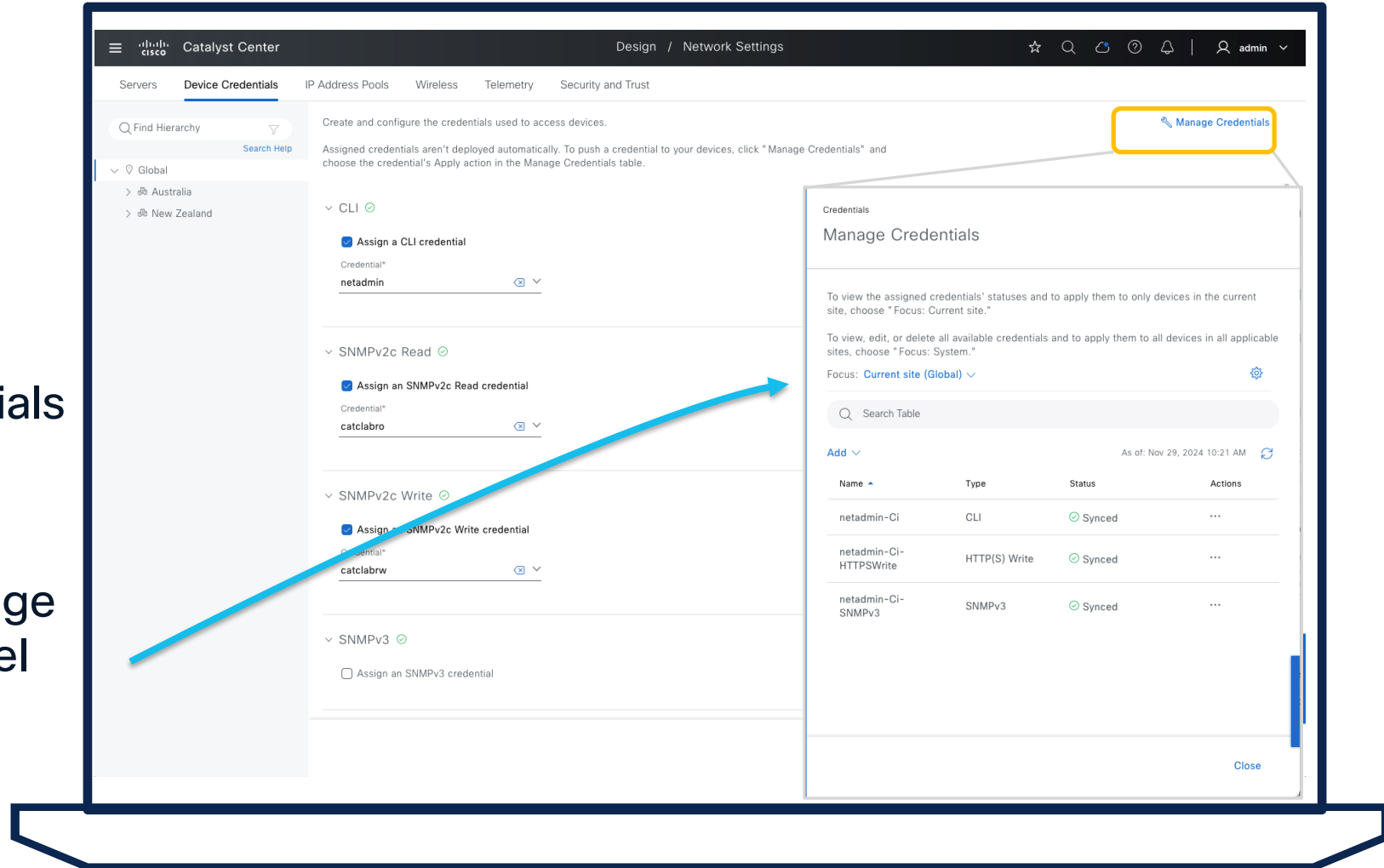


You can do it before a discovery or during the discovery.

If you do it during the discovery assign credentials to the global level.



Focus allows you to change credentials at system level as well.

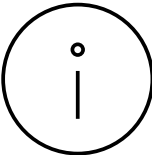


The screenshot displays the Cisco Catalyst Center interface for configuring Device Credentials. The main area shows a configuration page with a sidebar for finding hierarchies (Global, Australia, New Zealand) and a main section for creating and configuring credentials. A blue arrow points from the 'Global' level in the hierarchy to the 'Manage Credentials' modal. The modal shows a table of credentials with columns: Name, Type, Status, and Actions. The table lists three credentials: netadmin-CI (CLI, Synced), netadmin-CI-HTTPSWrite (HTTP(S) Write, Synced), and netadmin-CI-SNMPv3 (SNMPv3, Synced). A 'Manage Credentials' button is highlighted in the top right of the main area.

Name	Type	Status	Actions
netadmin-CI	CLI	Synced	...
netadmin-CI-HTTPSWrite	HTTP(S) Write	Synced	...
netadmin-CI-SNMPv3	SNMPv3	Synced	...

Device Credentials

Design > Network Settings > Device Credentials



Focus allows you to change credentials at system level as well.

Design / Network Settings

Servers

Device Credentials

IP Address Pools

Wireless

Telemetry

Security and Trust

Find Hierarchy

Search Help

Global

Australia

New Zealand

Create and configure the credentials used to access devices.

Assigned credentials aren't deployed automatically. To push a credential to your devices, click "Manage Credentials" and choose the credential's Apply action in the Manage Credentials table.

Manage Credentials

Credentials

Manage Credentials

To view the assigned credentials' statuses and to apply them to only devices in the current site, choose "Focus: Current site."

To view, edit, or delete all available credentials and to apply them to all devices in all applicable sites, choose "Focus: System."

Focus: System

Search Table

Add

As of: Nov 29, 2024 10:27 AM

Name	Type	Actions
netadmin-Ci	CLI	...
netadmin-Ci-HTTPSWrite	HTTP(S) Write	...
netadmin-Ci-SNMPv3	SNMPv3	...

Close

Credentials

Manage Credentials

To view the assigned credentials' statuses and to apply them to only devices in the current site, choose "Focus: Current site."

To view, edit, or delete all available credentials and to apply them to all devices in all applicable sites, choose "Focus: System."

Focus: Current site (Global)

Search Table

Add

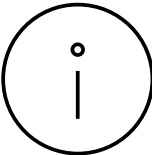
As of: Nov 29, 2024 10:21 AM

Name	Type	Status	Actions
netadmin-Ci	CLI	Synced	...
netadmin-Ci-HTTPSWrite	HTTP(S) Write	Synced	...
netadmin-Ci-SNMPv3	SNMPv3	Synced	...

Close

Trusted Certificates

Design > Network Settings > Trusted Certificates



Click on “*Update trusted certificates now*” to download the latest version.

Catalyst Center

System / Settings

Search

Certificates

Trusted Certificates

System Certificates

Certificate Authority

Device Certificates

Cisco Accounts

PnP Connect

Cisco.com Credentials

Smart Account

Smart Licensing

SSM Connection Mode

Device Settings

PnP AP Location

Image Distribution Servers

Device Controllability

Network Resync Interval

SNMP

ICMP Ping

PnP Device Authorization

Device EULA Acceptance

Device Prompts

Configuration Archive

External Services

Umbrella

Authentication and Policy Serv...

Integrity Verification

SD-Access Compatibility Matrix

Settings / Certificates

Trusted Certificates

Cisco Trusted External Root Bundle is available now. [Update trusted certificates now](#)

Cisco Catalyst Center supports the storage and update of the Cisco Trusted External Root Bundle([ios.p7b](#)) from the [Cisco PKI](#) web site. This Cisco Trusted External Root Bundle enables supported Cisco networking devices to authenticate the controller and its applications such as Network Plug and Play, upon the presentation of a valid third-party vendor device certificates. Cisco Catalyst Center already contains a pre-installed Cisco Trusted External Root Bundle.

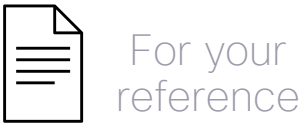
Trusted Certificates Status

All Expired Expiring

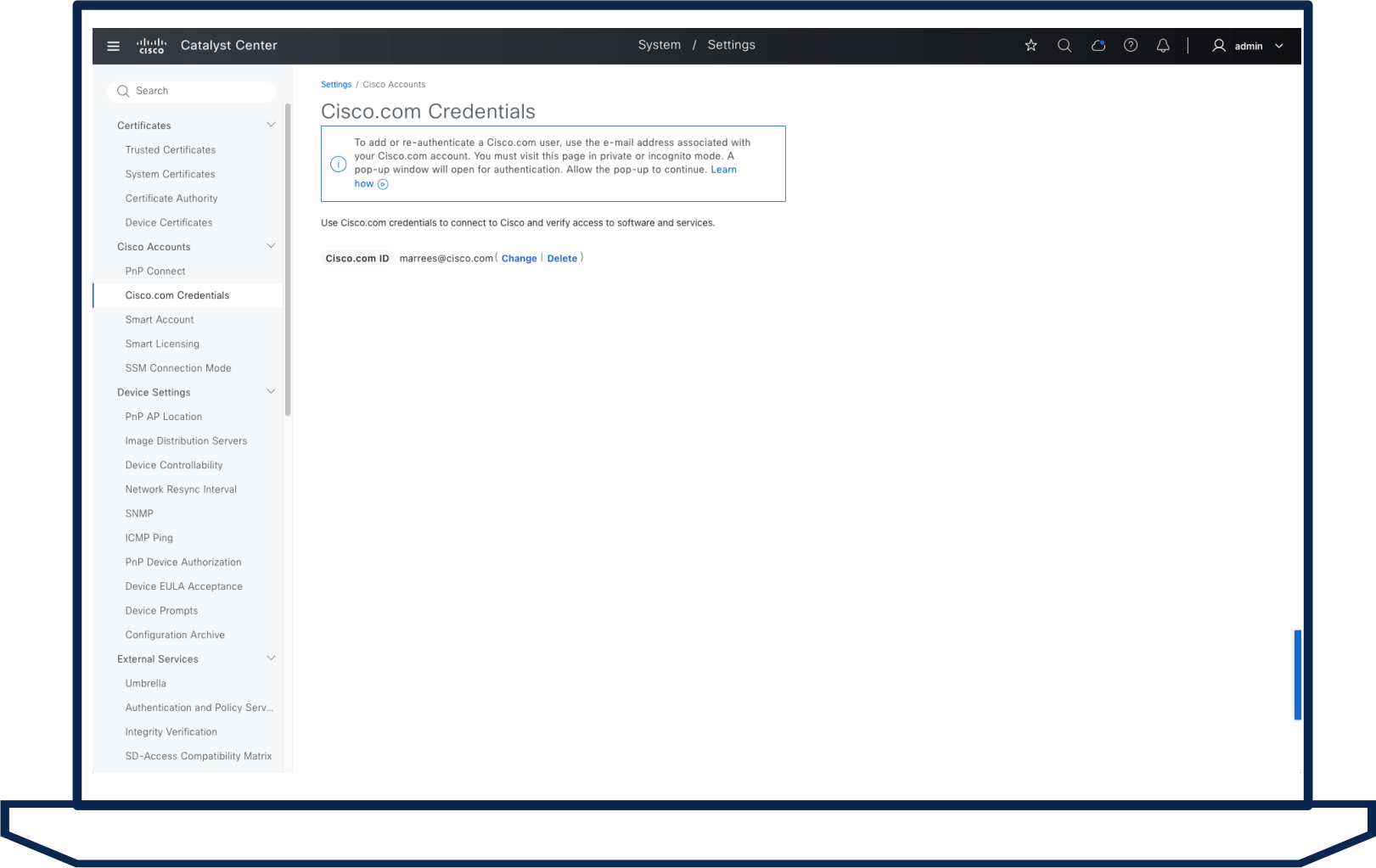
[Import](#) [Export](#) As of: Sep 29, 2025 2:15 PM

Issued To	Issued By	Used For	Certificate Serial Number	Time Left	Status	Valid From	Valid To	Action
OU=Security Communication RootCA1, O=SECOM Trust.net, C=JP	OU=Security Communication RootCA1, O=SECOM Trust.net, C=JP	Cisco Trusted	0	N/A	<div></div>	Sep 30, 2003 1:50 PM	Sep 30, 2023 1:50 PM	<div></div>
CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Cisco Trusted	...000b9	N/A	<div></div>	May 13, 2000 4:16 AM	May 13, 2025 9:29 AM	<div></div>
CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O=" Entrust, Inc.", C=US	CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O=" Entrust, Inc.", C=US	Cisco Trusted	...b5054	425 days	<div></div>	Nov 28, 2006 6:53 AM	Nov 28, 2026 7:23 AM	<div></div>
CN=Certigna, O=Dhimyotis, C=FR	CN=Certigna, O=Dhimyotis, C=FR	Cisco Trusted	...948ff	639 days	<div></div>	Jun 30, 2007 12:43 AM	Jun 30, 2027 12:43 AM	<div></div>
CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Cisco Trusted	...ac394	852 days	<div></div>	Sep 1, 1998 9:30 PM	Jan 28, 2028 10:30 PM	<div></div>
CN=NetLock Arany (Class Gold) Főtanúsítvány, OU=Tanúsítványkiadók (Certification Services), O=NetLock Kft., L=Budapest, C=HU	CN=NetLock Arany (Class Gold) Főtanúsítvány, OU=Tanúsítványkiadók (Certification Services), O=NetLock Kft., L=Budapest, C=HU	Cisco Trusted	...40010	1165 days	<div></div>	Dec 12, 2008 1:38 AM	Dec 7, 2028 1:38 AM	<div></div>
CN=AAA Certificate Services	CN=AAA Certificate Services							Iss: 1

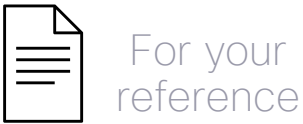
Cisco.com Credentials



System > Settings > Cisco.com Credentials

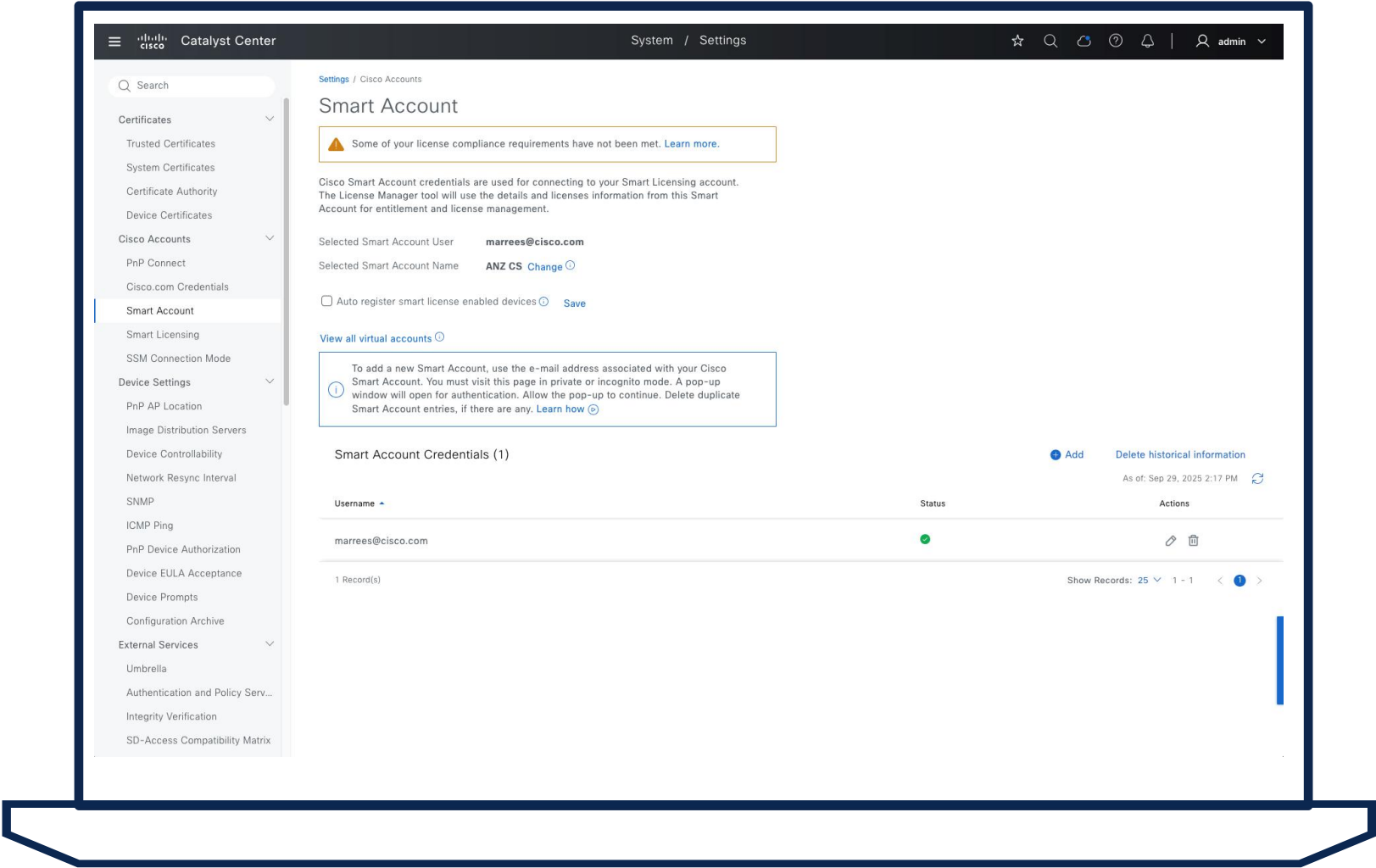


Smart Account



For your
reference

System > Settings > Smart Account

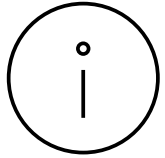


Smart Licensing



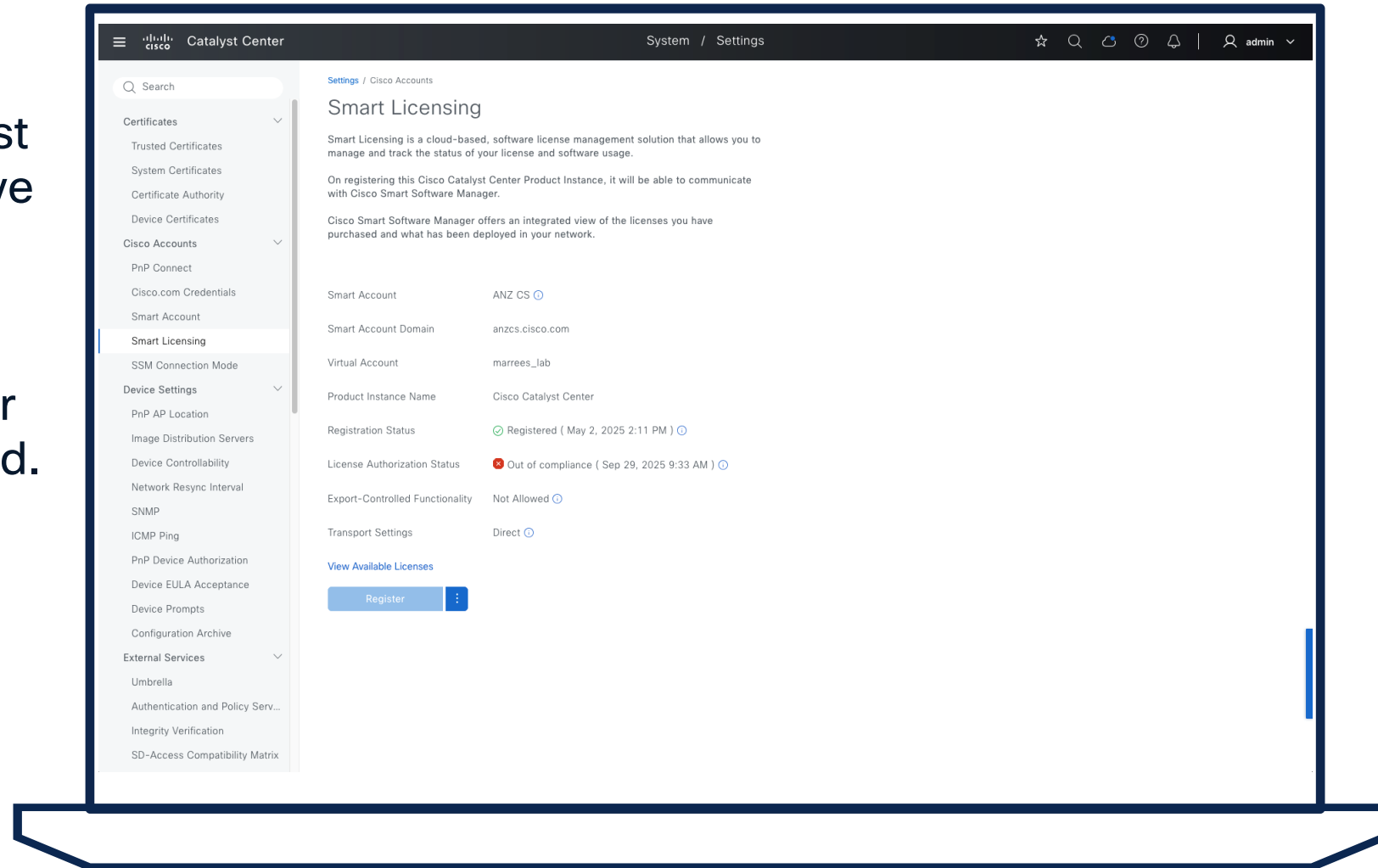
For your
reference

System > Settings > Smart Licensing



This is a license for Catalyst Center itself. It doesn't have a cost.

It is deposited in the smart account when a physical or virtual appliance is acquired.

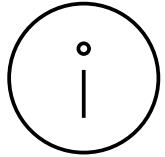


SSM Connection Mode

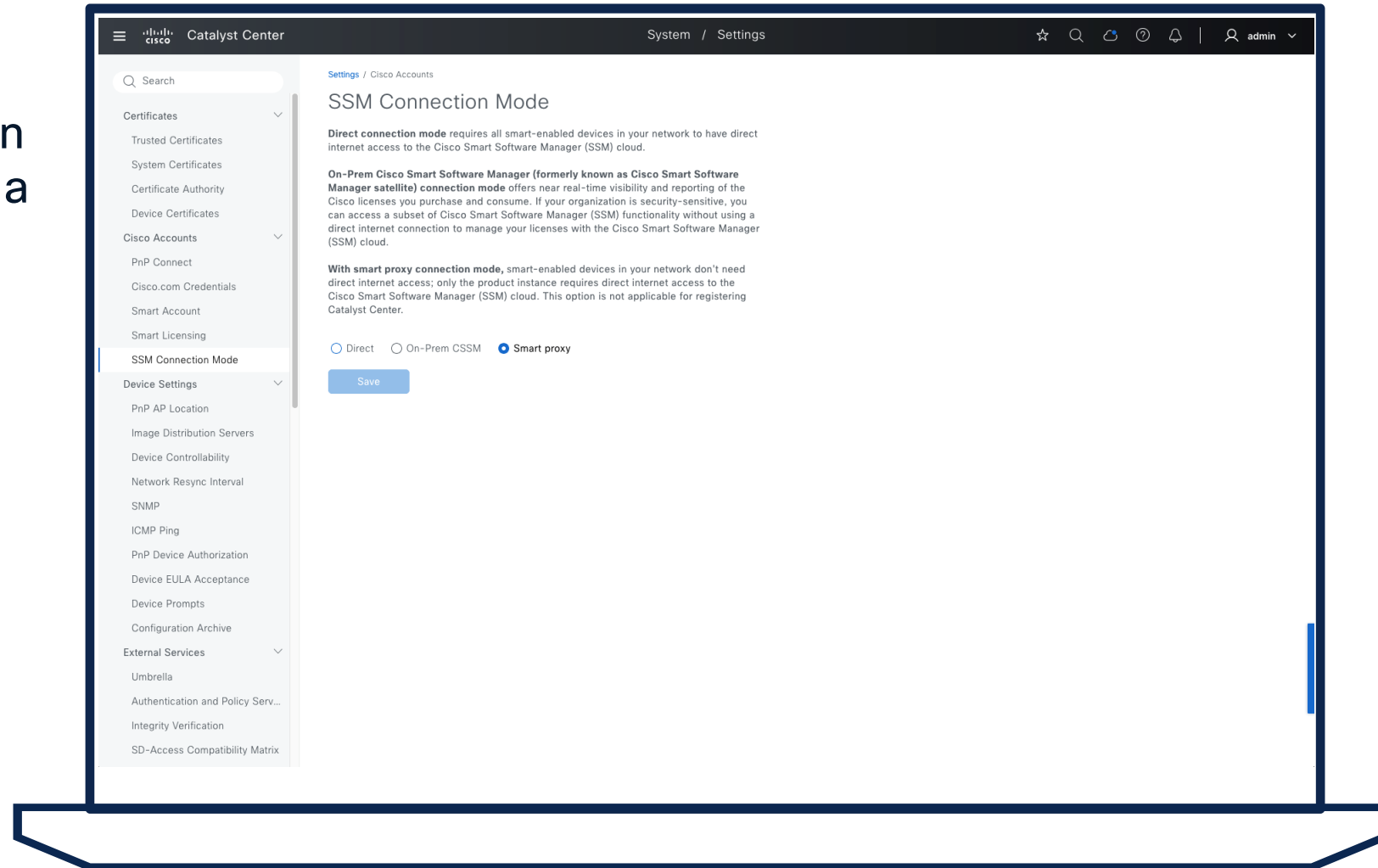


For your
reference

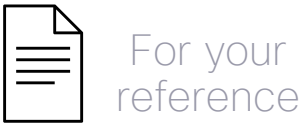
System > Settings > SSM Connection Mode



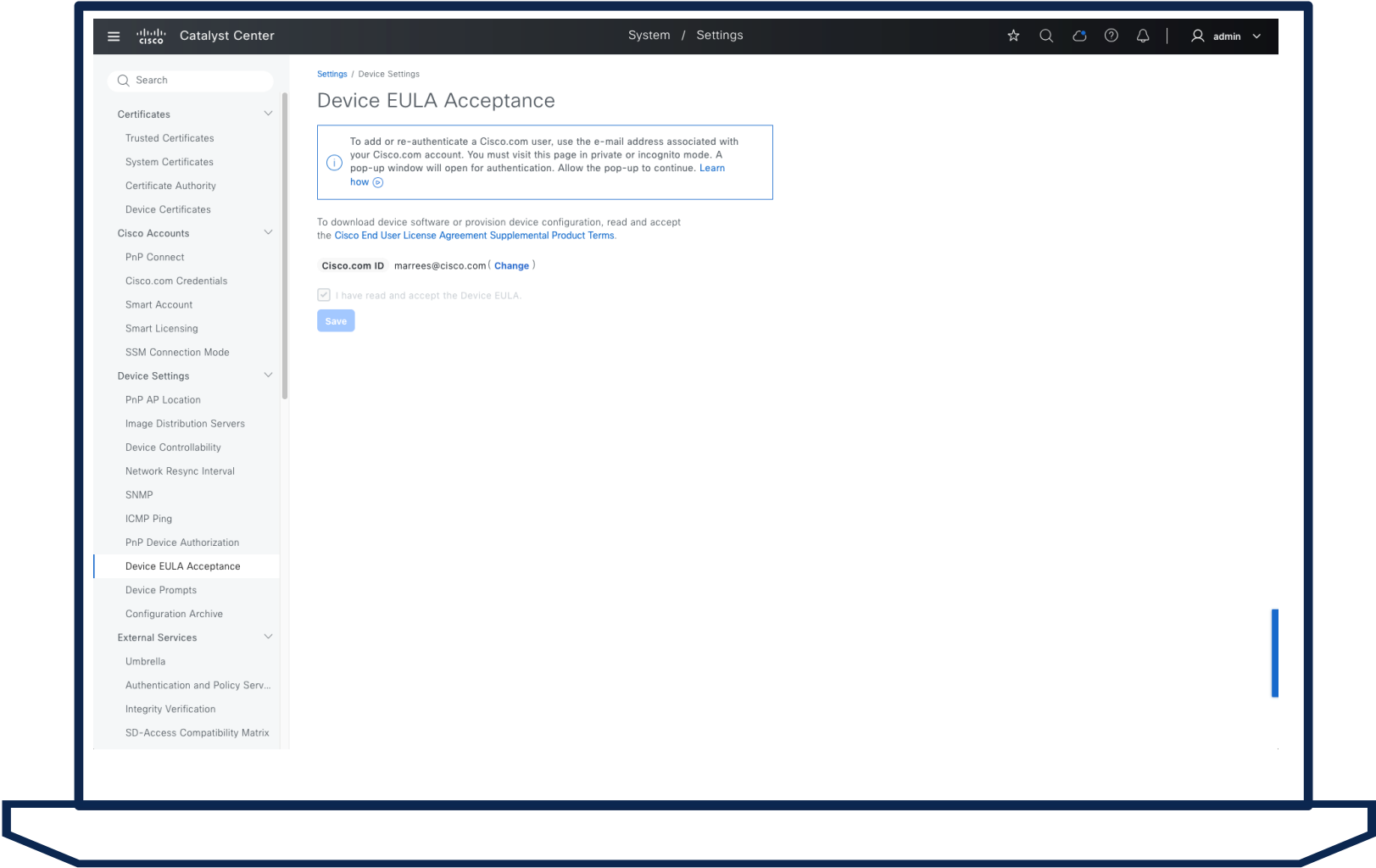
Mode selection depends on your setup. Smart proxy is a very convenient way.



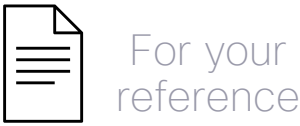
Device EULA Acceptance



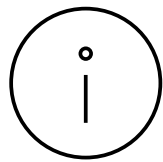
System > Settings > Device EULA Acceptance



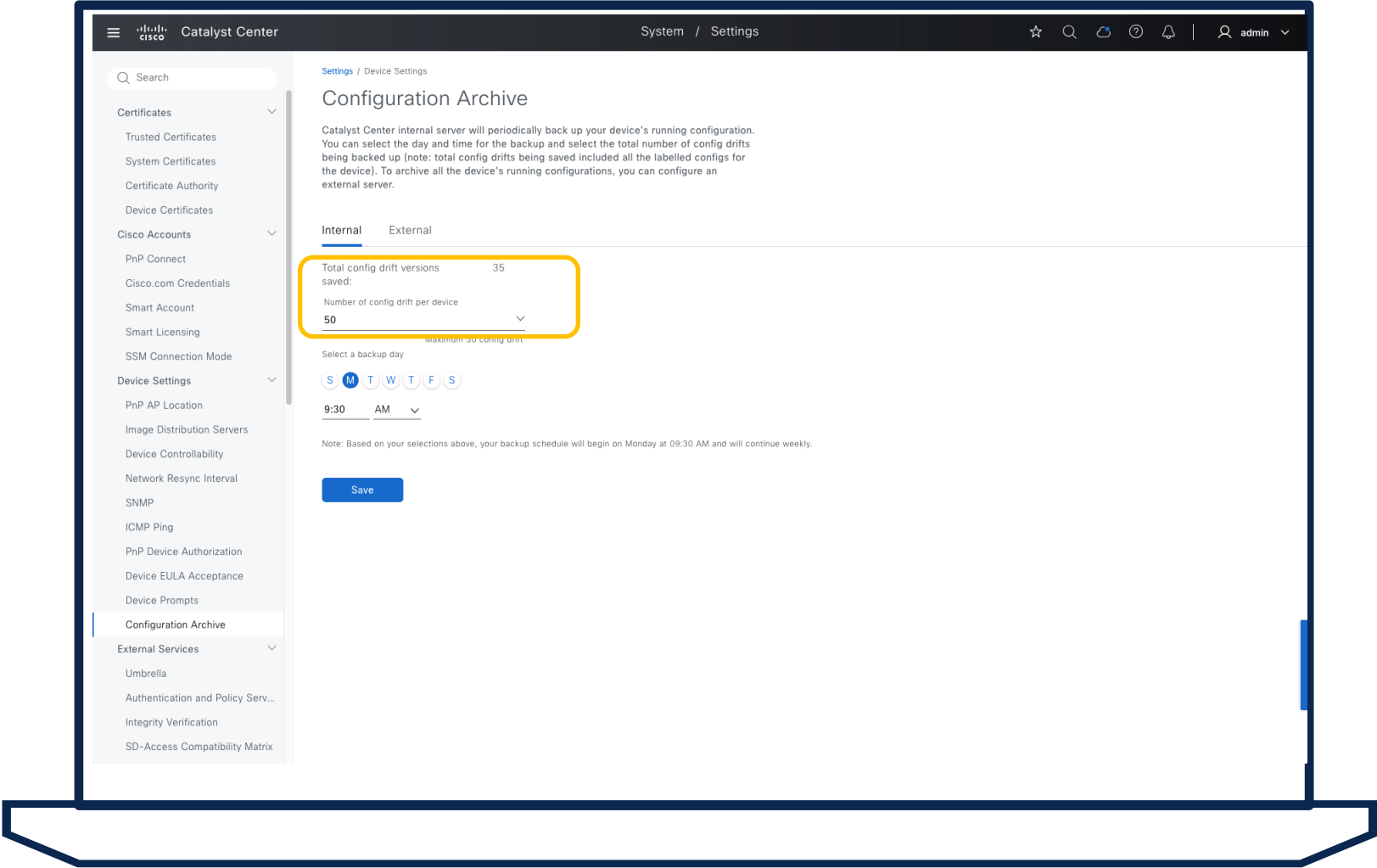
Configuration Archive



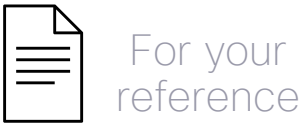
System > Settings > Configuration Archive



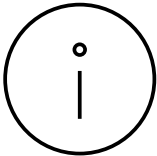
By default, it is 15.
50 is the maximum.



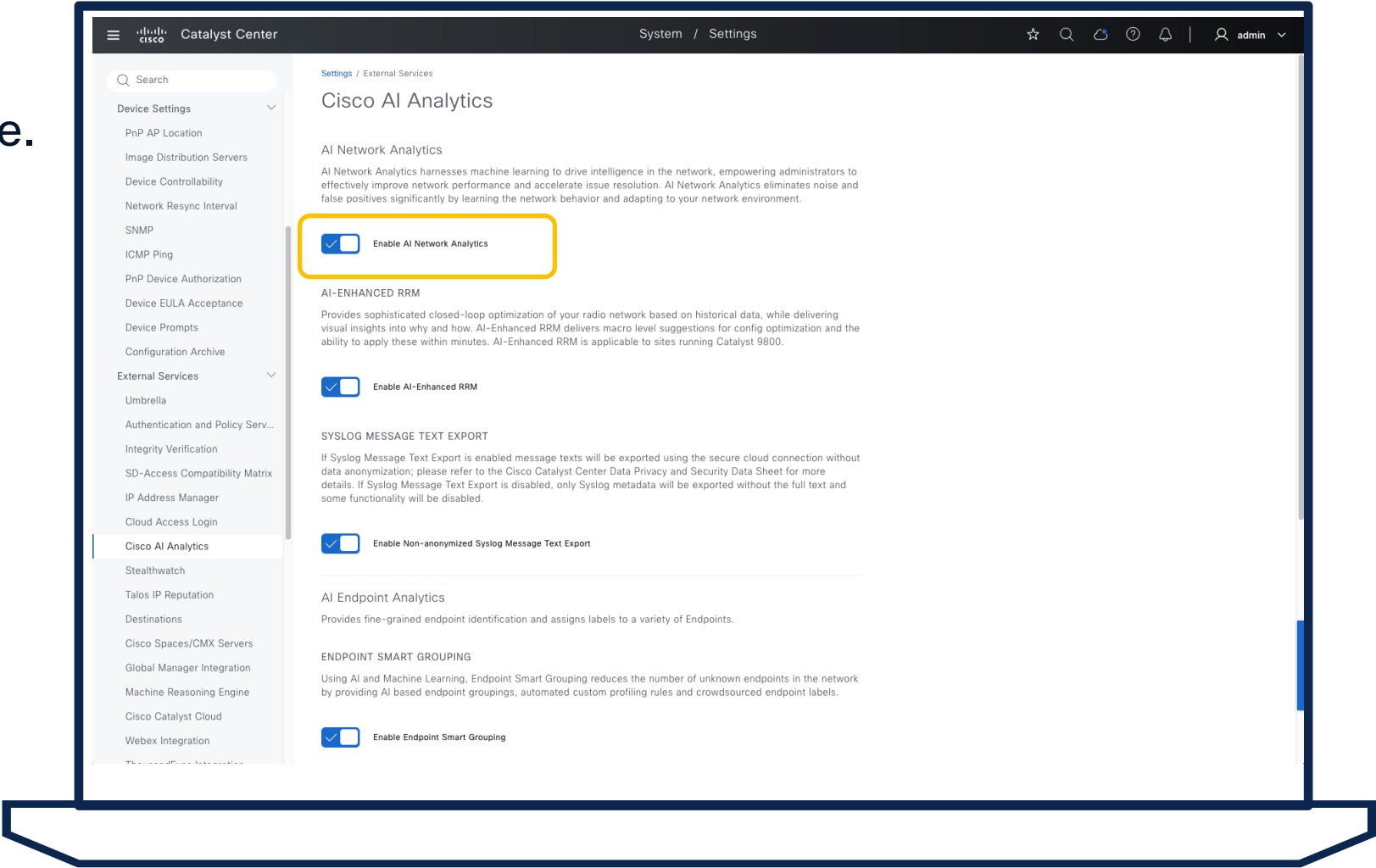
Cisco AI Analytics



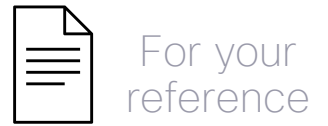
System > Settings > Cisco AI Analytics



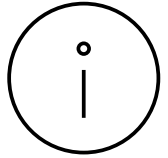
It requires DNA Advantage.



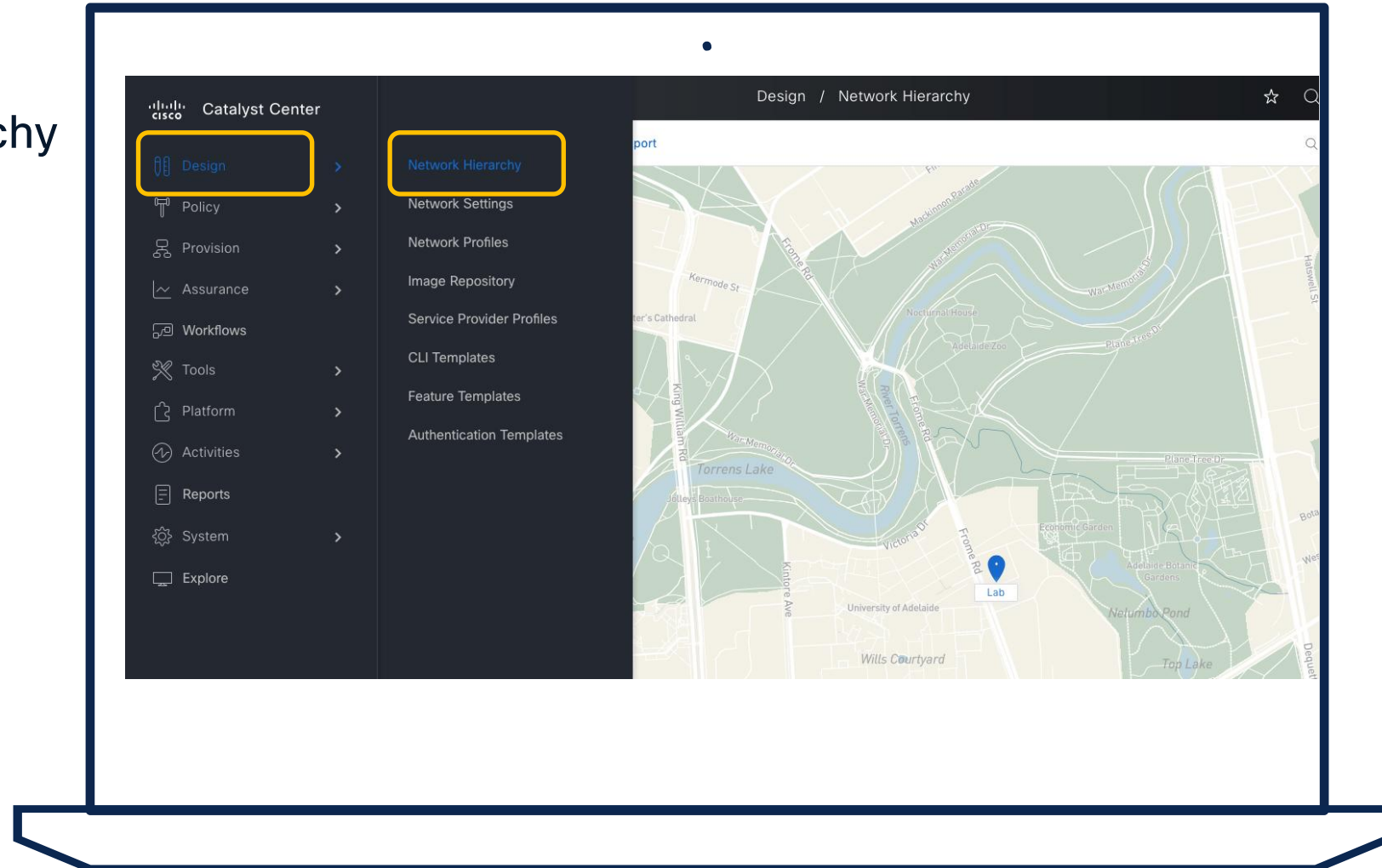
Building your Network Hierarchy



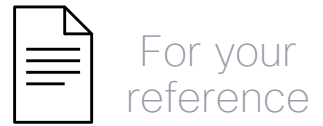
Design > Network Hierarchy



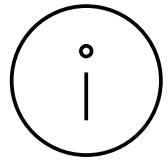
You can create the Hierarchy manually



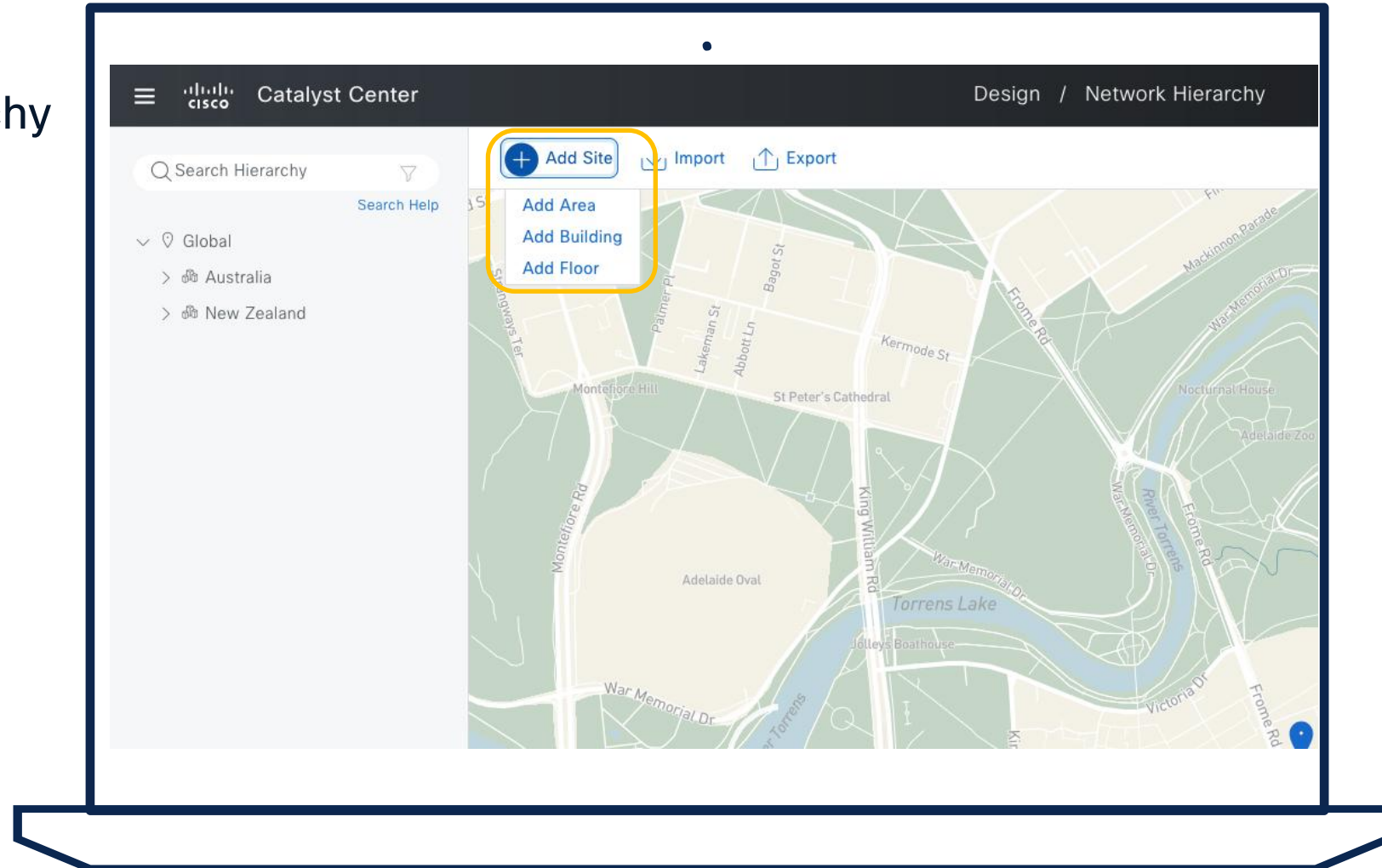
Building your Network Hierarchy



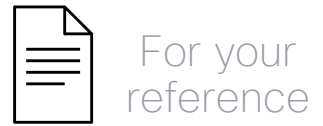
Design > Network Hierarchy



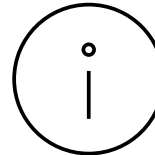
You can create the Hierarchy manually

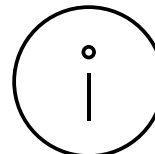


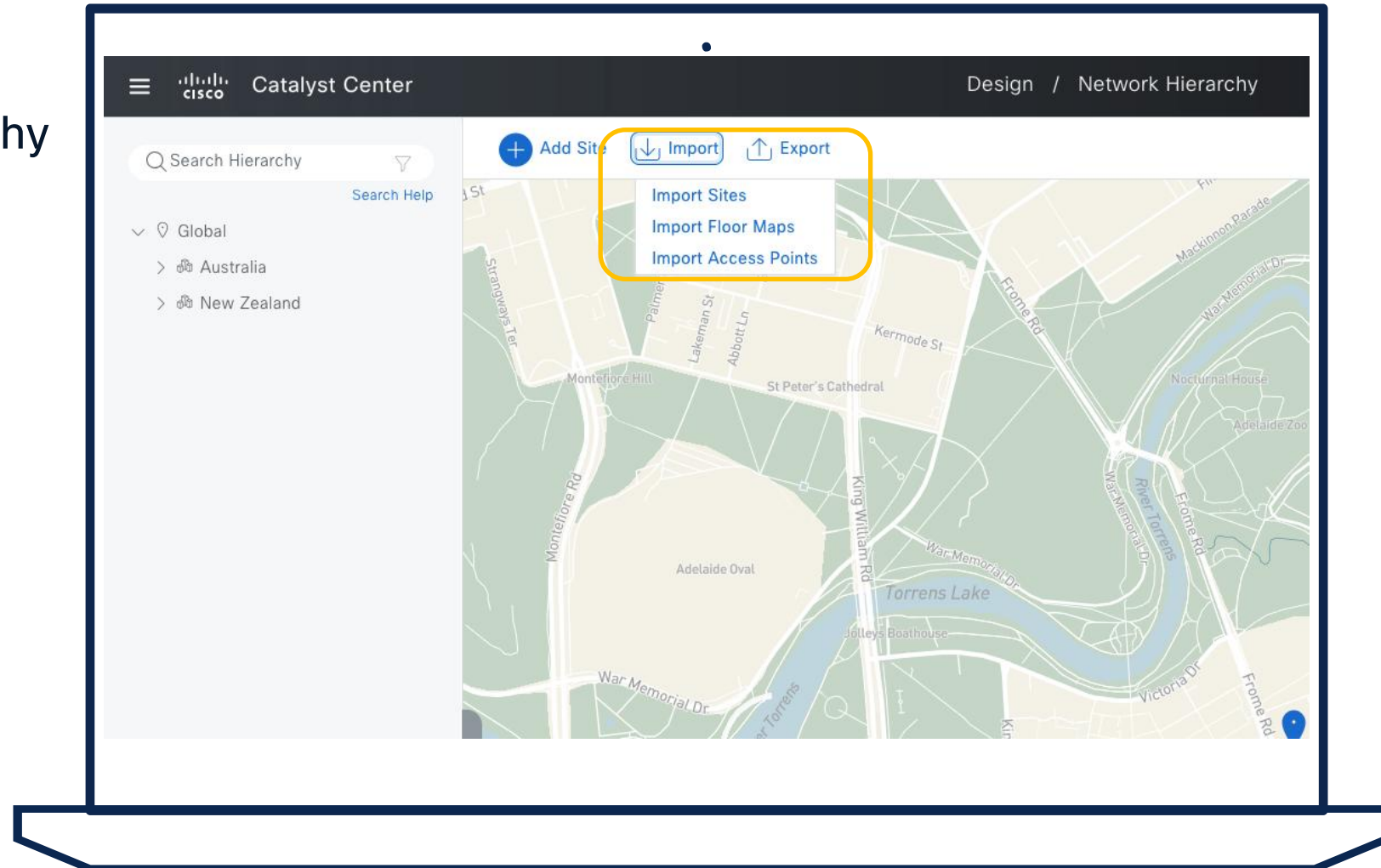
Building your Network Hierarchy



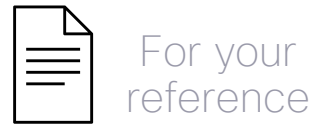
Design > Network Hierarchy

 You can create the Hierarchy manually

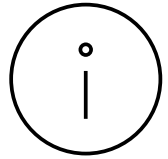
 You can import data (e.g. from Prime Infrastructure, CSV, Ekahau)



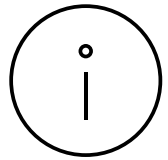
Building your Network Hierarchy



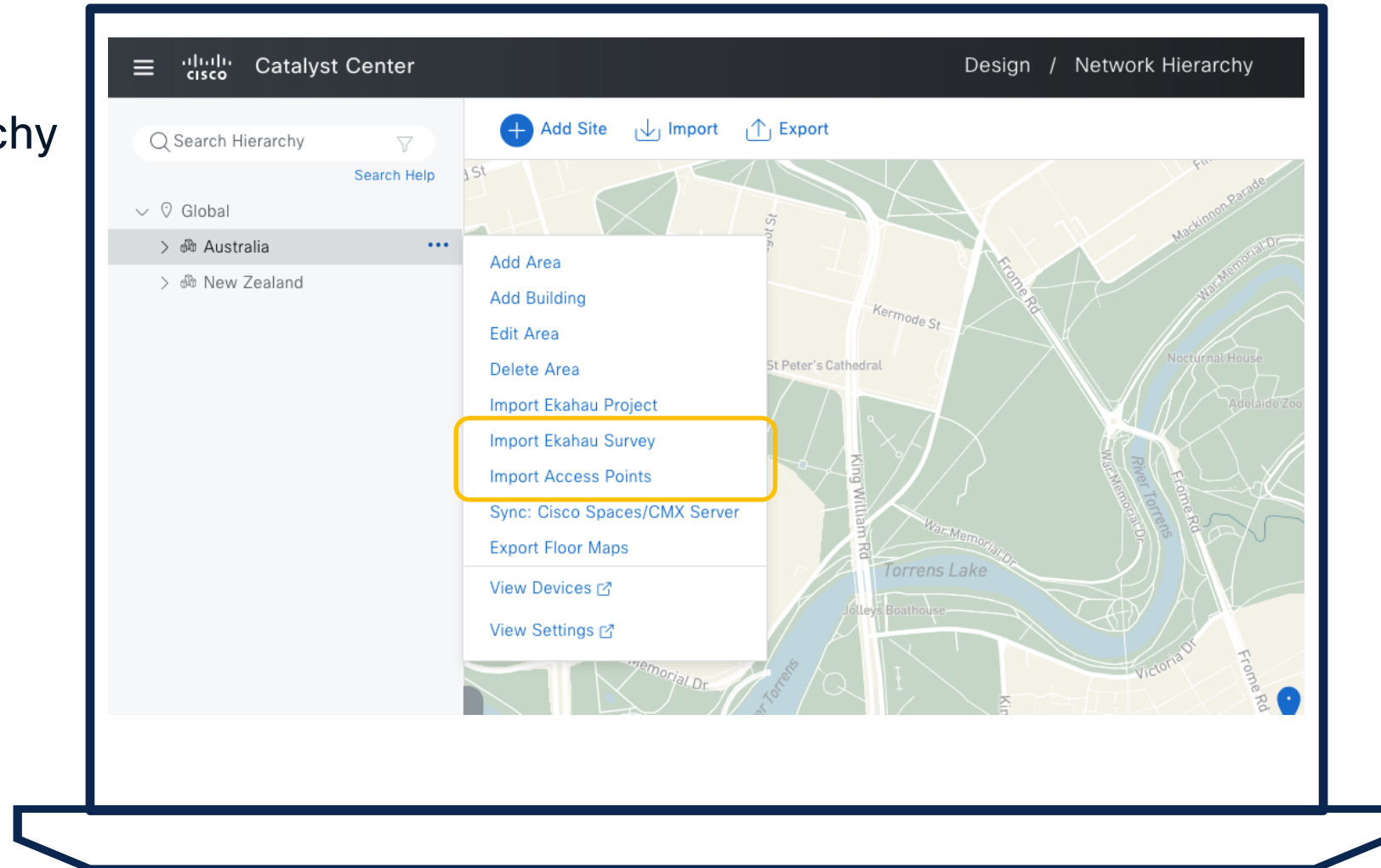
Design > Network Hierarchy



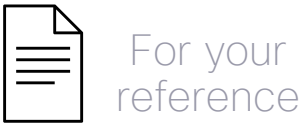
You can create the Hierarchy manually



You can import data (e.g. from Prime Infrastructure, CSV, Ekahau)

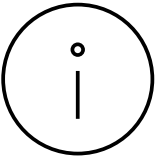


Appliance only – System health

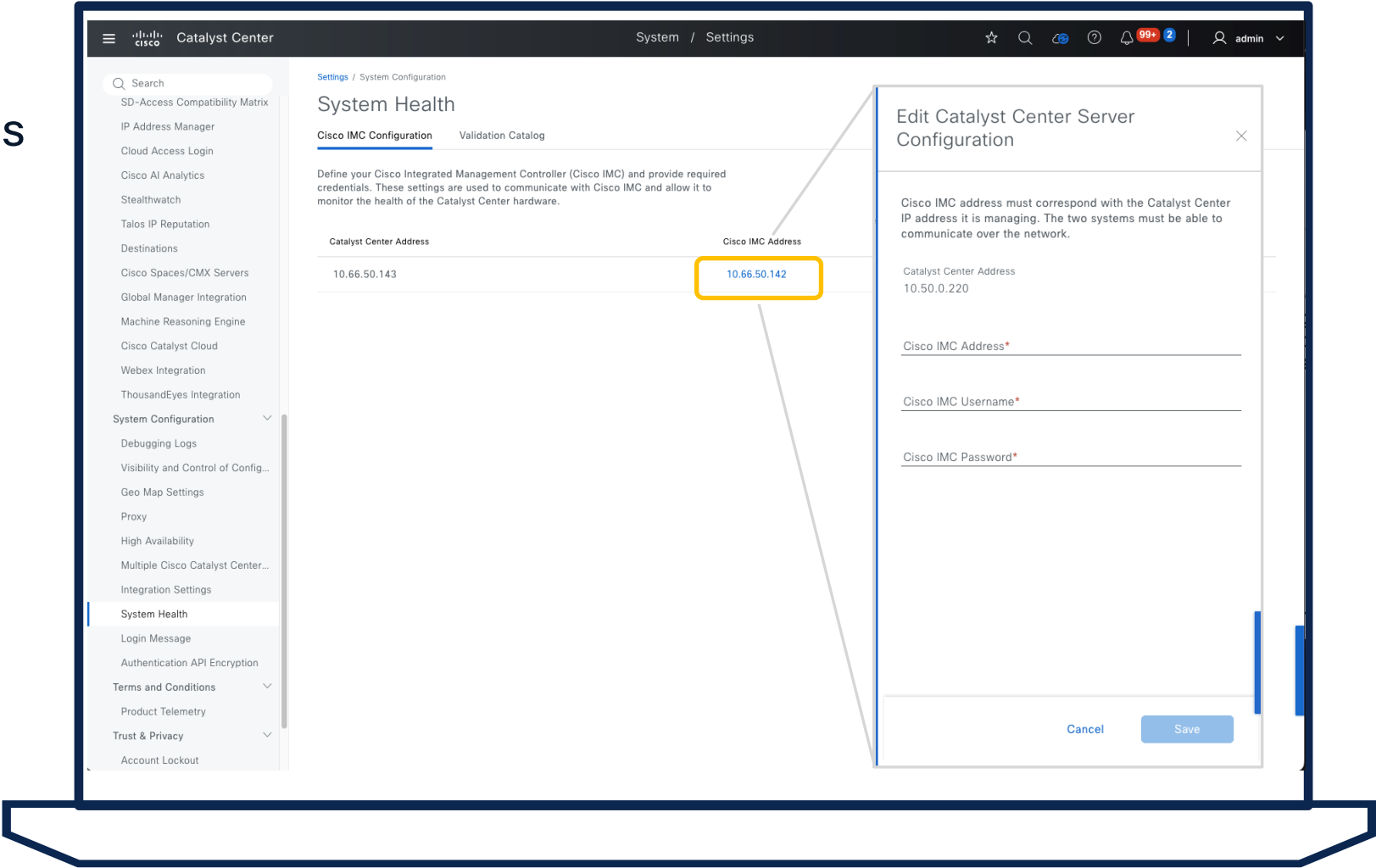


For your
reference

System > Settings > System Health



Enter the CIMC credentials
to get information on the
appliance health within
System 360.



Things you should configure: Firewall(s)



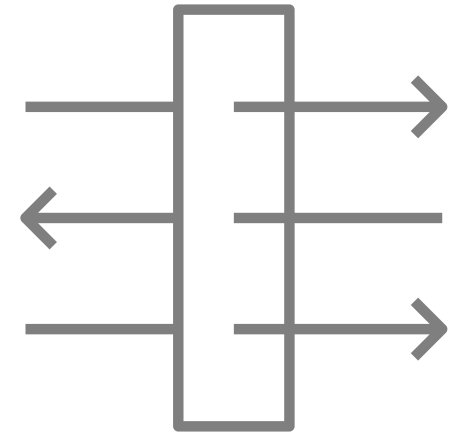
Don't forget about the firewall!

- Within your network:

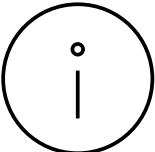
[Cisco Catalyst Center Security Best Practices Guide](#) section
[Secure Your Catalyst Center Deployment](#)

- Internet access:

[Cisco Catalyst Center Third-Generation Appliance Installation Guide, Release 2.3.7.x](#) section [Required Internet URLs and Fully Qualified Domain Names](#)



Things you should configure: Firewall(s)



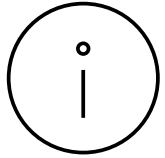
Catalyst Center requires internet access for SW updates, SWIM downloads, external integrations etc. This list is updated inline with each release of Catalyst Center and should be reviewed as part of upgrades.

In order to...	...Catalyst Center must access these URLs and FQDNs
Download updates for system software and application packages, and submit user feedback to the product team.	Recommended: *.ciscoconnectdna.com:443 ¹ To avoid wildcards, specify these URLs instead: <ul style="list-style-type: none">https://www.ciscoconnectdna.comhttps://cdn.ciscoconnectdna.comhttps://registry.ciscoconnectdna.comhttps://registry-cdn.ciscoconnectdna.com
Catalyst Center update package.	<ul style="list-style-type: none">https://*.ciscoconnectdna.com/*.cloudfront.net*.tesseractcloud.com
Smart Account and SWIM software downloads.	<ul style="list-style-type: none">https://apx.cisco.comhttps://cloudsso.cisco.com/as/token.oauth2https://*.cisco.com/https://download-ssc.cisco.com/
Authenticate with the cloud domain.	https://dnaservices.cisco.com
Integrate with ThousandEyes.	<ul style="list-style-type: none">*.awsglobalaccelerator.comapi.thousandeyes.com

List Continues

Things you should configure: Syslog & SNMP Extra Servers

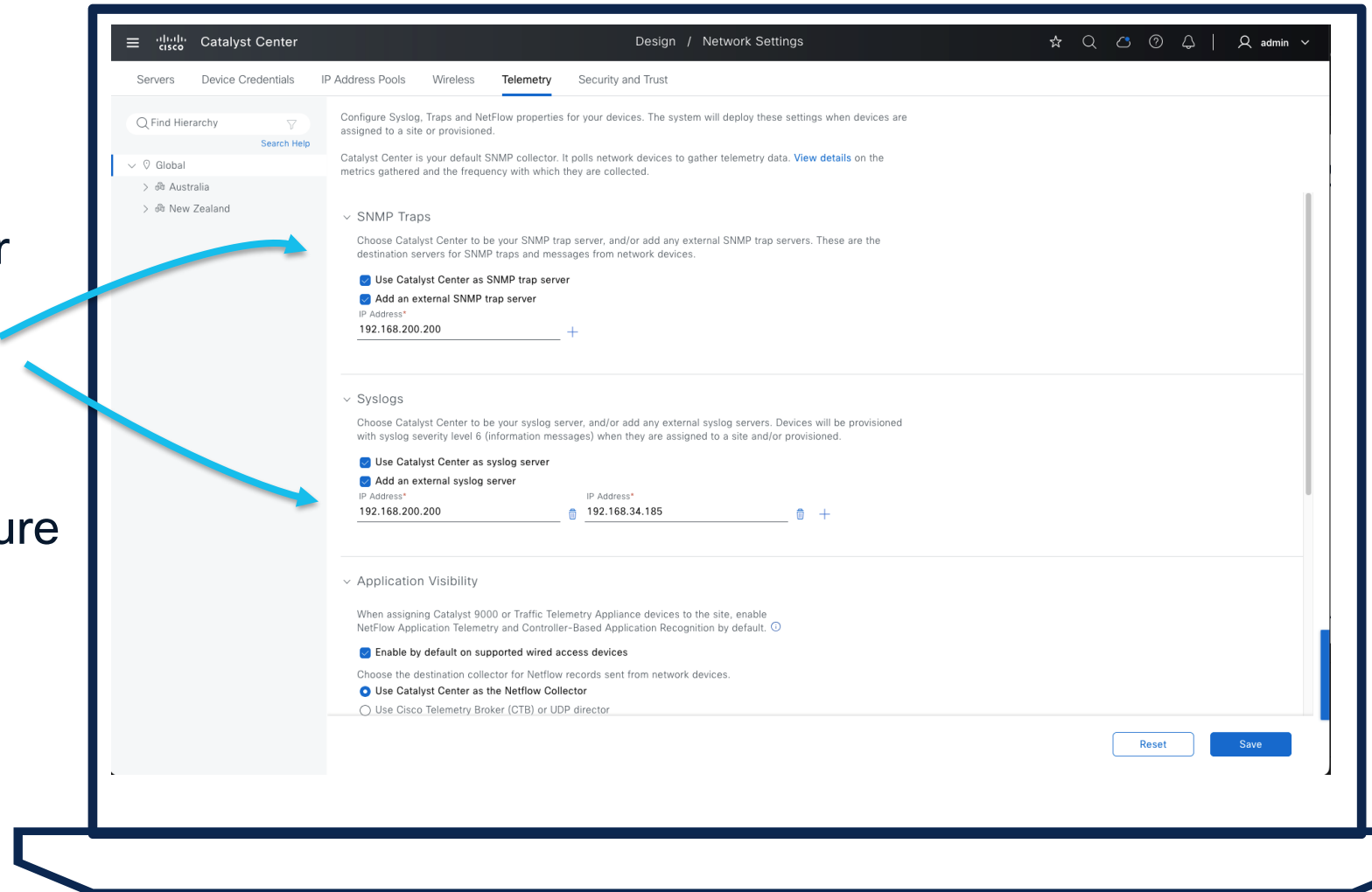
Design > Network Settings > Telemetry



Catalyst Center is a SNMP Trap & Syslog receiver.

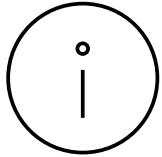
If you have Splunk or other 3rd party monitoring apps then these don't have to miss out!

Configure extra Trap & syslog destinations to ensure continuity of telemetry to other platforms

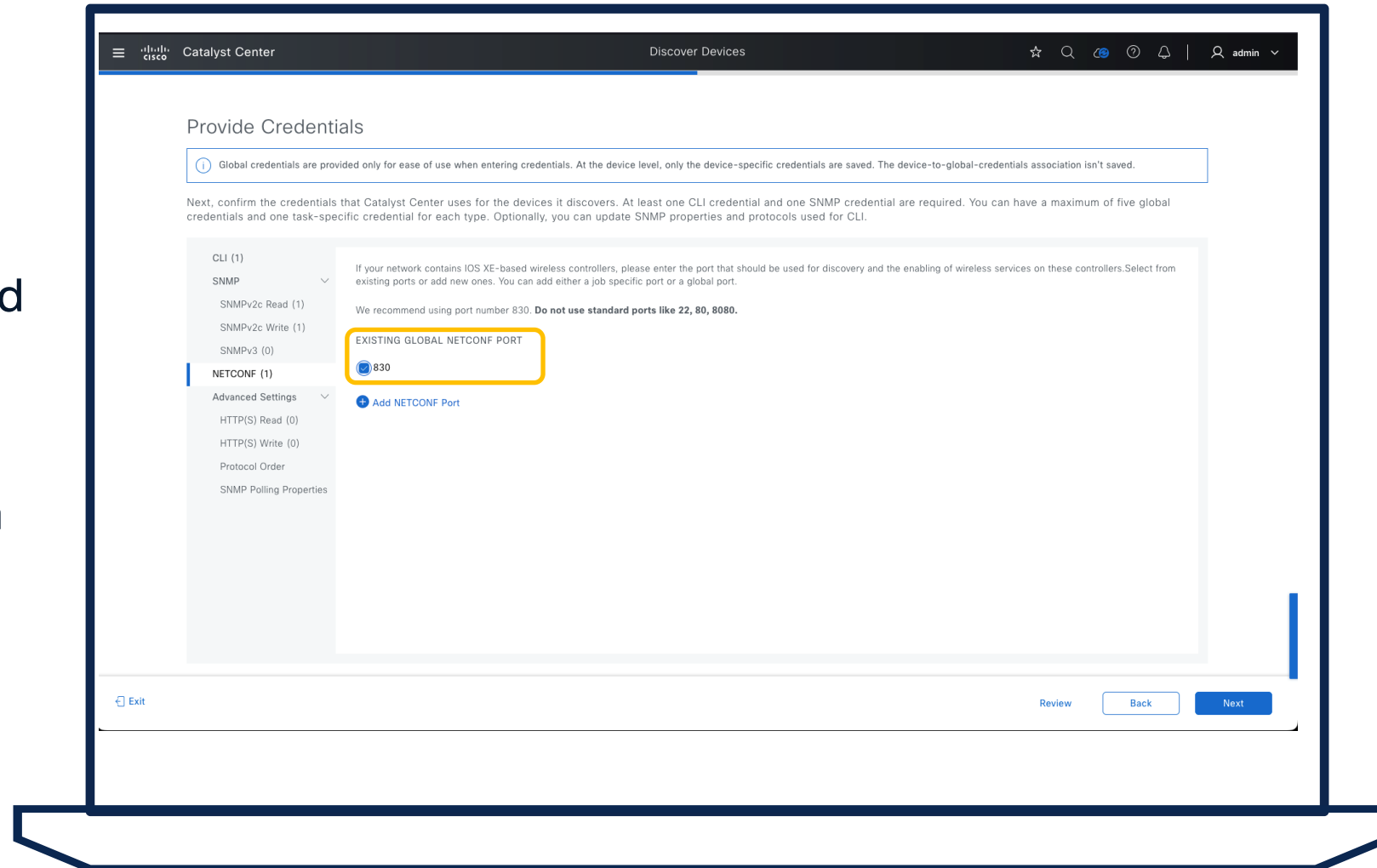


Things you should configure: Netconf

Tools > Discovery

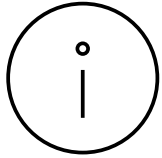


Netconf discovery is mandatory for wireless controllers. Switches should also be discovered with Netconf enabled as well for features such as PoE analytics, Sustainability and system telemetry.



Things you should configure: Netconf

On the device

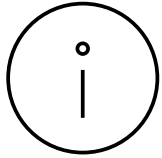


Enabling Netconf is important, but securing it is even more important...

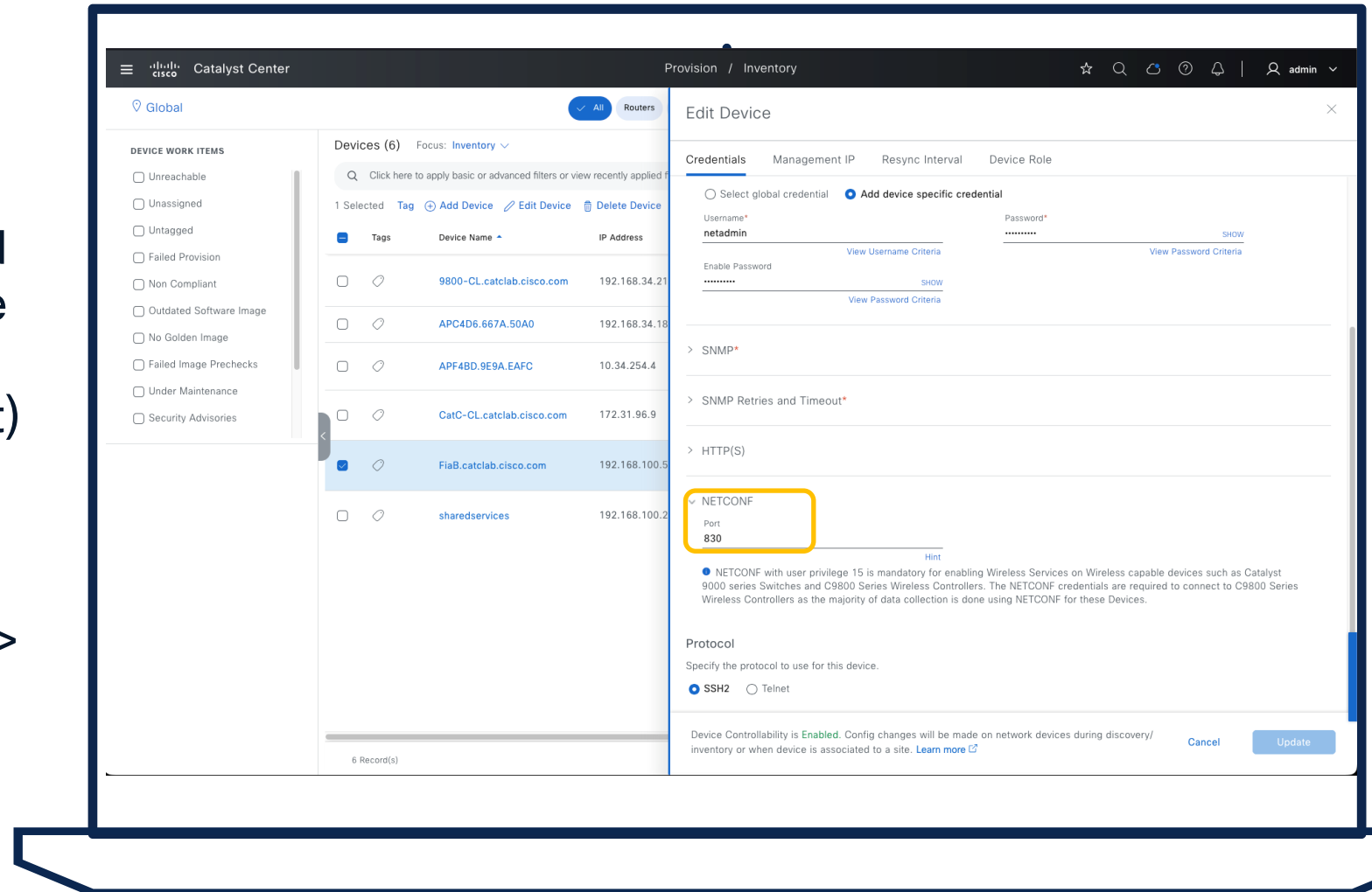
```
netconf-yang
aaa new-model
aaa authentication login default local
aaa authorization exec default local
ip access-list standard NETCONF_ACL
  permit <host-address> <wildcard-mask>
  deny any
exit
netconf-yang ssh ipv4 access-list name NETCONF_ACL
end
```

Things you should configure: Netconf

Inventory – Select Device –> Edit Device

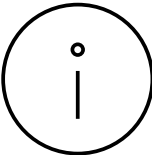


If switches have been discovered without Netconf, there is no need to rediscover. The device can be edited and the Netconf port (830 default) added at a later stage. Be sure to update telemetry once complete (select device > Actions > Telemetry > Update Telemetry)



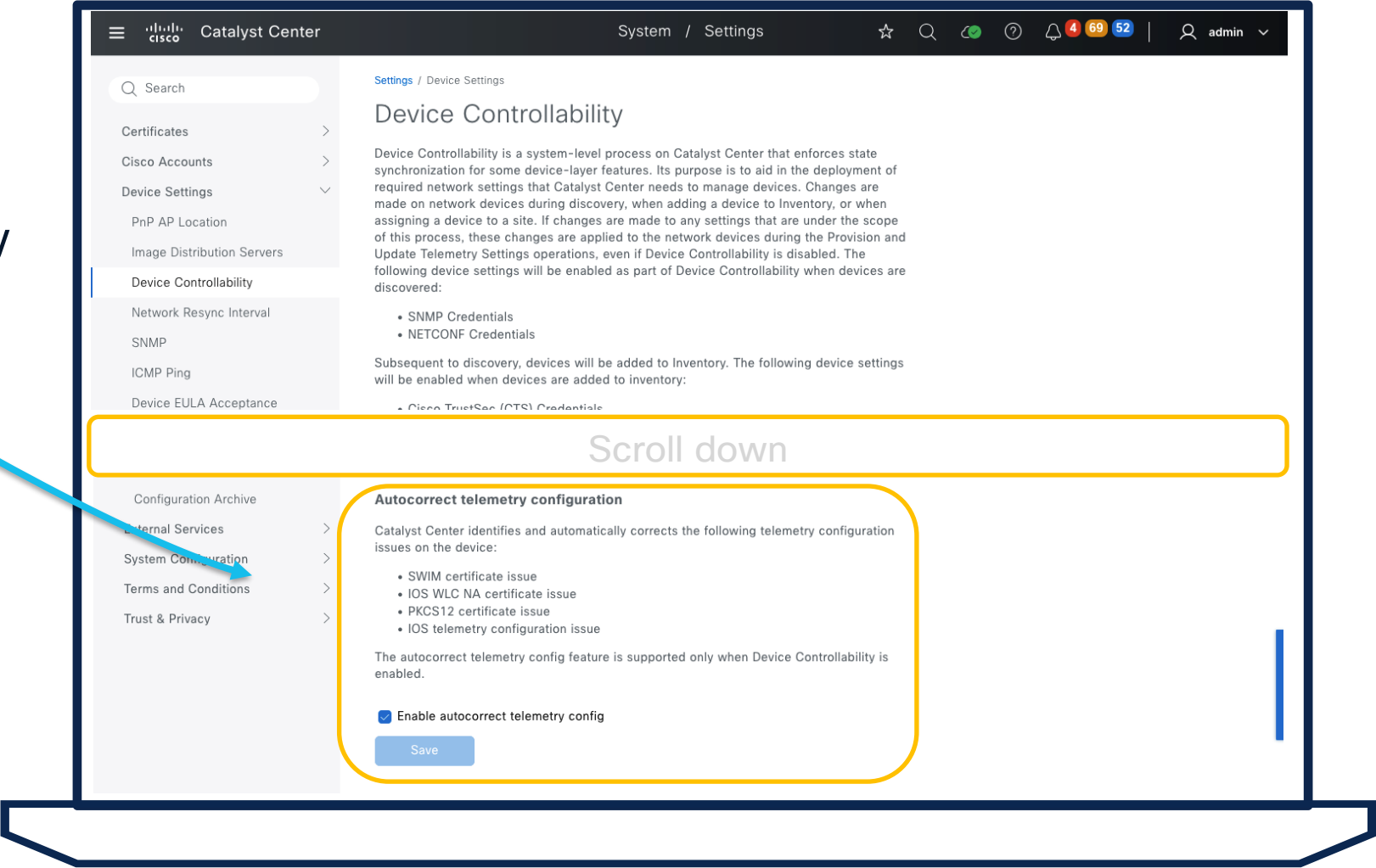
Things you should configure: Auto Correct Telemetry

System > Settings > Device Controllability



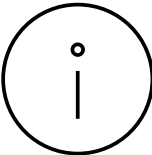
New feature (2.3.7.x) that allows Catalyst Center to automatically fix telemetry configurations.

Off by default.

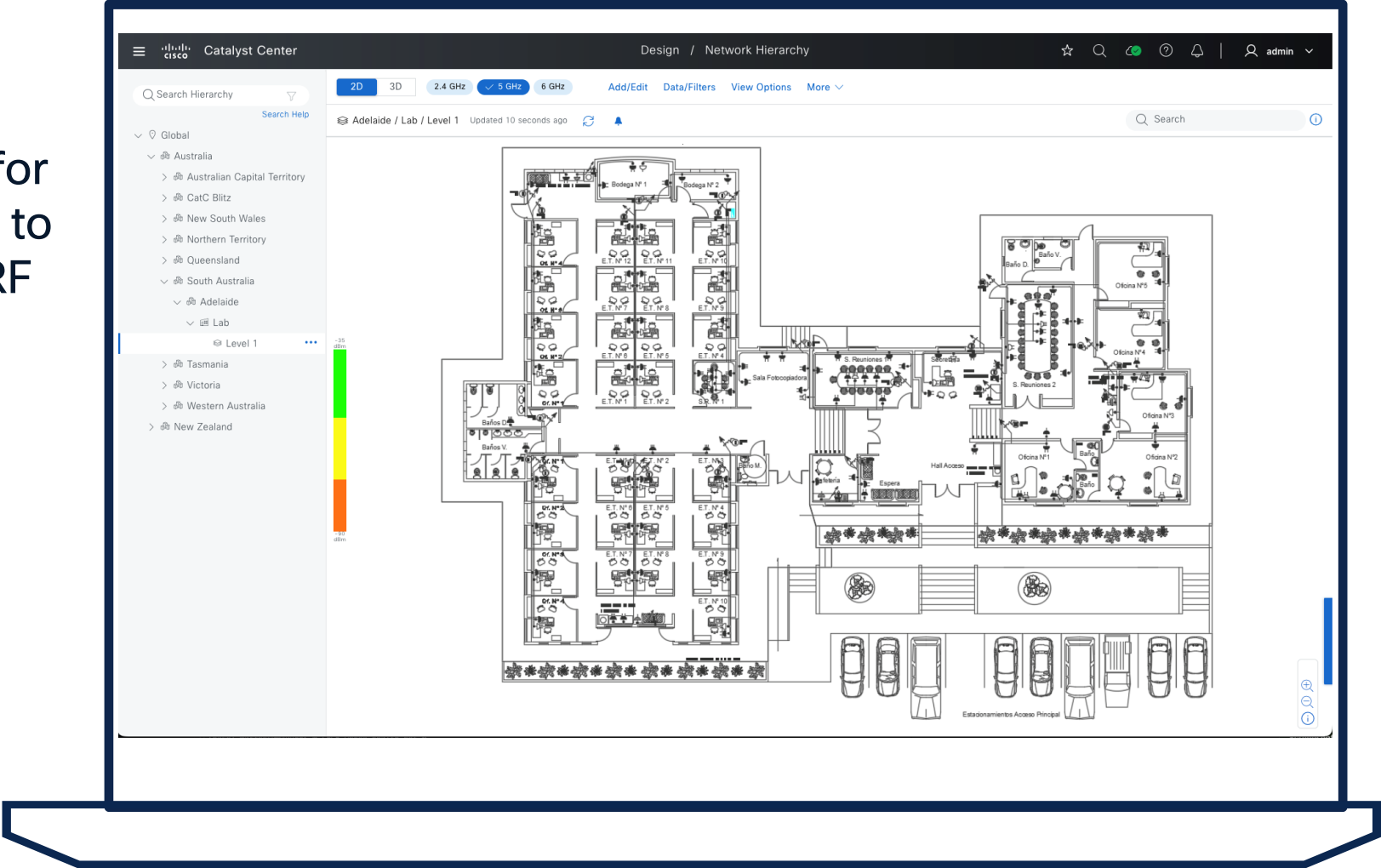


Things you should configure: Walls

Design > Network Hierachy

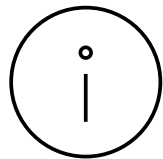


Walls and correct attenuation are important for Catalyst Center to be able to give you a guide on your RF coverage.

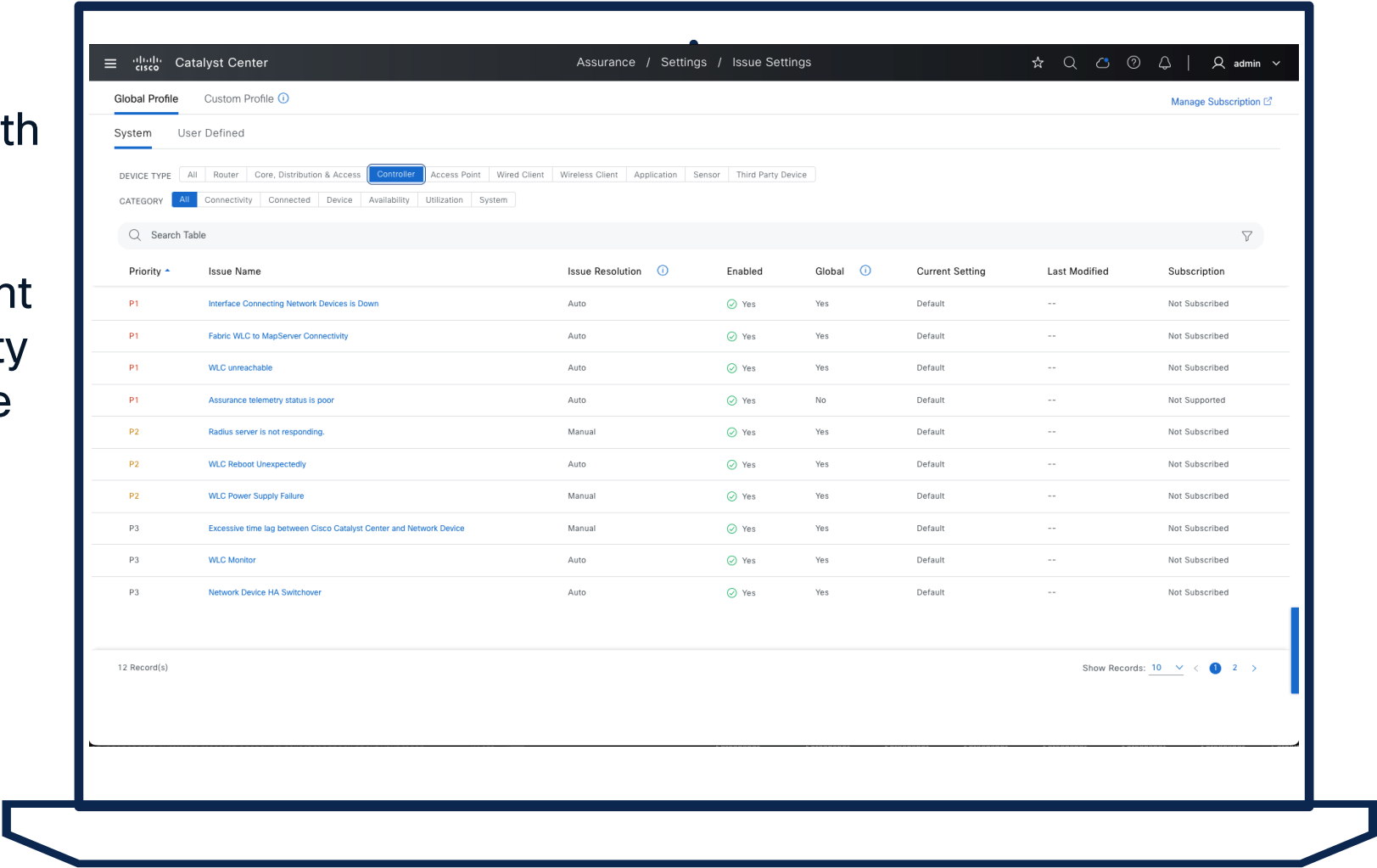


Things you should configure: Issues & Alerts

Assurance > Issue Settings

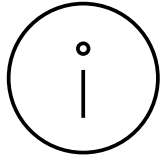


269 Pre-defined alerts with KPI's, thresholds and Priorities.
Globally subscribe to event notifications, adjust priority levels, and fine tune some KPI's.



Things you should configure: Issues – User Defined Events

Assurance > Issue Settings > User Defined



Match against device generated syslog for custom issue & alerting. Custom issues based on syslog severity, severity and message pattern matching.

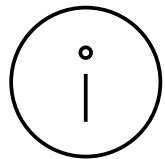
The screenshot displays the 'Create an Issue' configuration page in the Cisco Catalyst Center interface. The page is titled 'Create an Issue' and shows the following fields and options:

- Issue Name*:** PSU
- Description*:** PSU
- Syslog Detail:**
 - Severity*:** 1 - Alert
 - Facility*:** ENV_MON
 - Mnemonic*:** PS_ABSENT

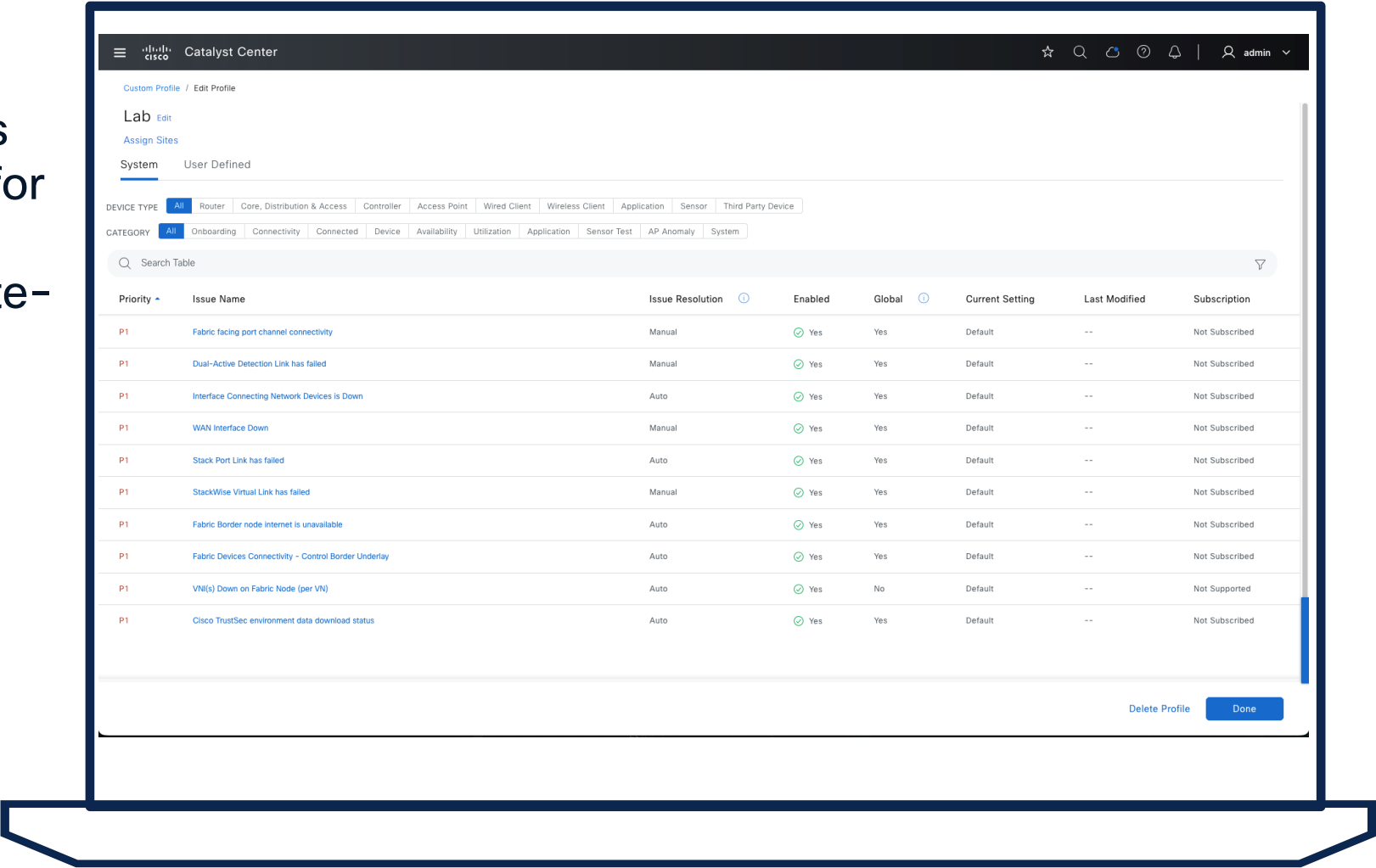
At the bottom right of the main content area, there is a red circle highlighting the 'Create an Issue' button. The page also includes a 'Next' button and a 'Cancel' button at the bottom right.

Things you should configure: Assurance Profiles

Design > Network Profiles > Assurance Profile

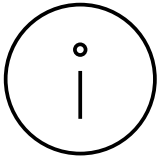


Custom Assurance Profiles to provide more flexibility for the wide range of environments, including site-based priority, KPI and notification adjustments.

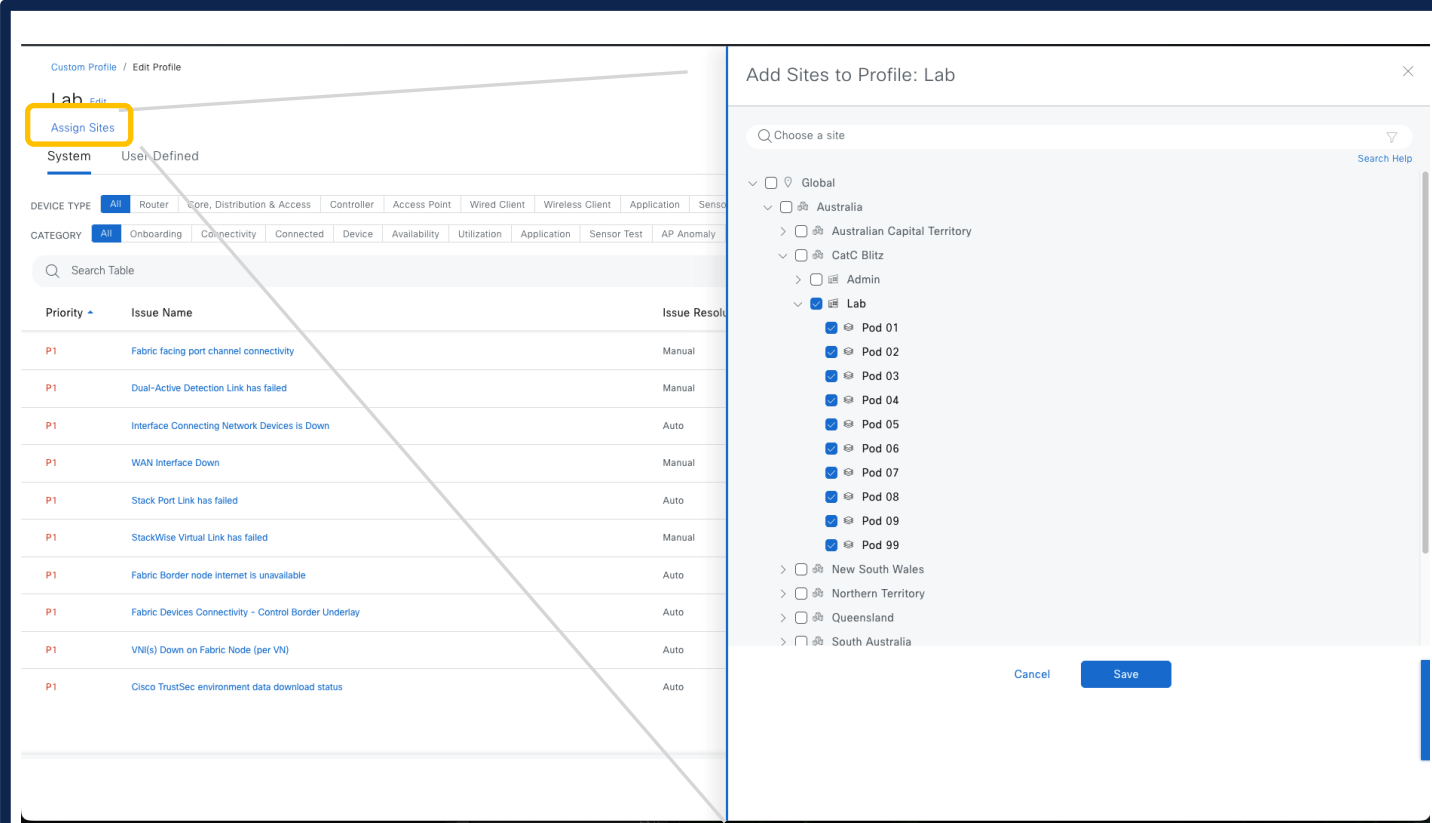


Things you should configure: Assurance Profiles

Design > Network Profiles > Assurance Profile

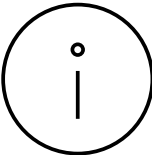


Custom Assurance Profiles to provide more flexibility for the wide range of environments, including site-based priority, KPI and notification adjustments.

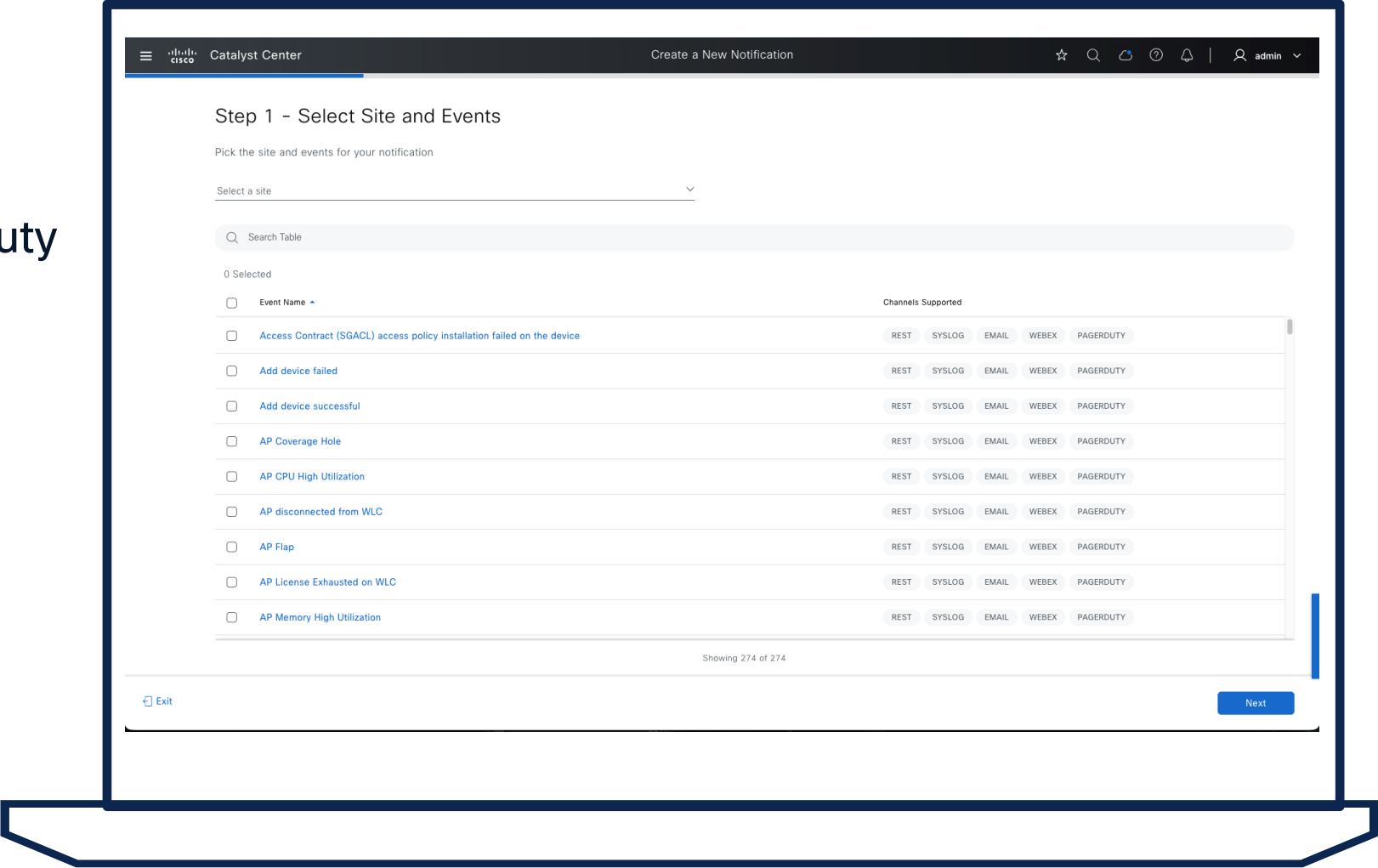


Things you should configure: Issues & Alerts

Platform > Developer Toolkit > Event Notifications

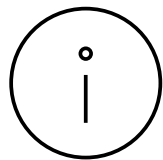


Notification channels for REST (webhook), syslog, Email, Webex, or Pager duty built in.



Things you should configure: Health Score Settings

Assurance > Health Score Settings



Remove or adjust certain KPI's from health score calculation relevant to your environment. Device, client & application health can all be fine tuned.

Catalyst Center

Assurance / Settings / Health Score Settings

☆

🔍

🔄

🔔

👤 admin

Device HealthApplication Health

Health Score

The health score can be customized based on device type. The network device's health score is the lowest score of all included KPIs. To disable a KPI from impacting the overall device health, you can exclude it from the health score calculation.

Note: Health score setting is not applicable for Third Party Devices.

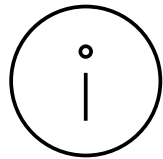
RouterCore, Distribution & AccessWireless ControllerAccess PointWireless ClientWired Client

🔍 Search Table

KPI Name	KPI Health Score		Included for Health Score	Current Setting	Last Modified
<div>Air Quality 2.4 GHz</div> <div>AP health indicated by Air Quality of 2.4 GHz band.</div>	POOR	GOOD	✔ Yes	Default	--
<div>Air Quality 5 GHz</div> <div>AP health indicated by Air Quality of 5 GHz band.</div>	POOR	GOOD	✔ Yes	Default	--
<div>Air Quality 6 GHz</div> <div>AP health indicated by Air Quality of 6 GHz band.</div>	POOR	GOOD	✔ Yes	Default	--
<div>CPU Utilization</div> <div>Device health indicated by CPU Utilization.</div>	POOR	GOOD	✔ Yes	Default	--
<div>Interference 2.4 GHz</div> <div>AP health indicated by Radio frequency Interference in 2.4 GHz band.</div>	POOR	GOOD	✔ Yes	Default	--
<div>Interference 5 GHz</div> <div>AP health indicated by Radio frequency Interference in 5 GHz band.</div>	POOR	GOOD	✔ Yes	Default	--
<div>Interference 6 GHz</div> <div>AP health indicated by Radio frequency Interference in 6 GHz band.</div>	POOR	GOOD	✔ Yes	Default	--
<div>Link Error</div>	POOR	GOOD	✔ Yes	Default	--

Things you should configure: Health Score Settings

Assurance > Health Score Settings



Remove or adjust certain KPI's from health score calculation relevant to your environment. Device, client & application health can all be fine tuned.

Assurance / Settings / Health Score Settings

Device Health Application Health

Health Score

The health score can be customized based on device type. The network device's health score is the lowest score of all included KPIs. To disable a KPI from impacting the overall health score, you can exclude it from the health score calculation. Note: Health score setting is not applicable for Third Party Devices.

Router Core, Distribution & Access Wireless Controller Access Point Wireless Client Wired Client

Search Table

KPI Name	KPI Health Score		Included for Health Score
Air Quality 2.4 GHz AP health indicated by Air Quality of 2.4 GHz band.	POOR < 60%	GOOD ≥ 60%	Yes
Air Quality 5 GHz AP health indicated by Air Quality of 5 GHz band.	POOR < 75%	GOOD ≥ 75%	Yes
Air Quality 6 GHz AP health indicated by Air Quality of 6 GHz band.	POOR < 75%	GOOD ≥ 75%	Yes
CPU Utilization Device health indicated by CPU Utilization.	POOR > 90%	GOOD ≤ 90%	Yes
Interference 2.4 GHz AP health indicated by Radio frequency Interference in 2.4 GHz band.	POOR > 50%	GOOD ≤ 50%	Yes
Interference 5 GHz AP health indicated by Radio frequency Interference in 5 GHz band.	POOR > 20%	GOOD ≤ 20%	Yes
Interference 6 GHz AP health indicated by Radio frequency Interference in 6 GHz band.	POOR > 20%	GOOD ≤ 20%	Yes
Link Error	POOR	GOOD	Yes

Air Quality 2.4 GHz

AP health indicated by Air Quality of 2.4 GHz band.

KPI HEALTH SCORE	
POOR	GOOD
< 60%	≥ 60%

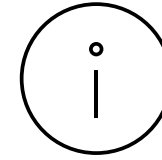
☒ Included in Device health Score

Last Modified: --
[View Default Setting](#)

Cancel Apply

Things you should UPDATE: Telemetry Updates

Provision > Inventory



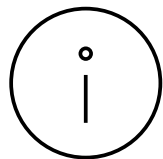
Post Upgrade telemetry endpoint updates are required to ensure full functionality with the new version of Catalyst Center.



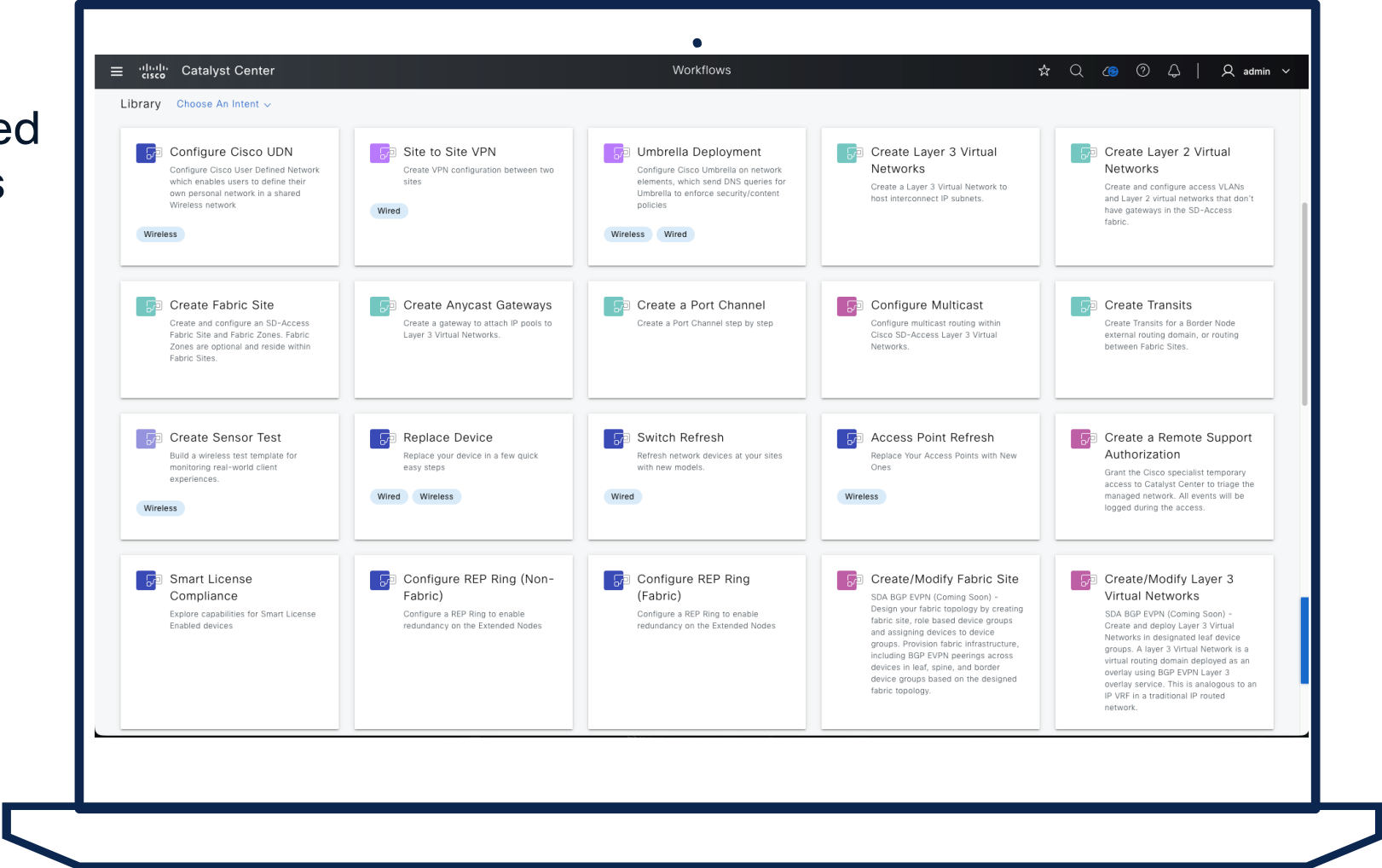
We have detected **IOS-XE device(s)** in your network where new telemetry subscriptions for assurance data need to be enabled and some of the existing subscriptions may need to be optimized for performance. [Apply Fix](#)
To provision subscriptions on **devices that have not been discovered with NETCONF**, rediscover the devices with NETCONF, and update the Telemetry Settings with the ☒ Force Configuration Push option.

Things you should USE: Workflows

Workflows



Workflows provided guided steps to automate various tasks via Catalyst Center



A Checklist for Success:

AI-RRM

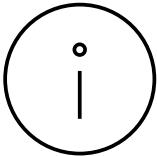
If you want to learn more about AI-RRM...



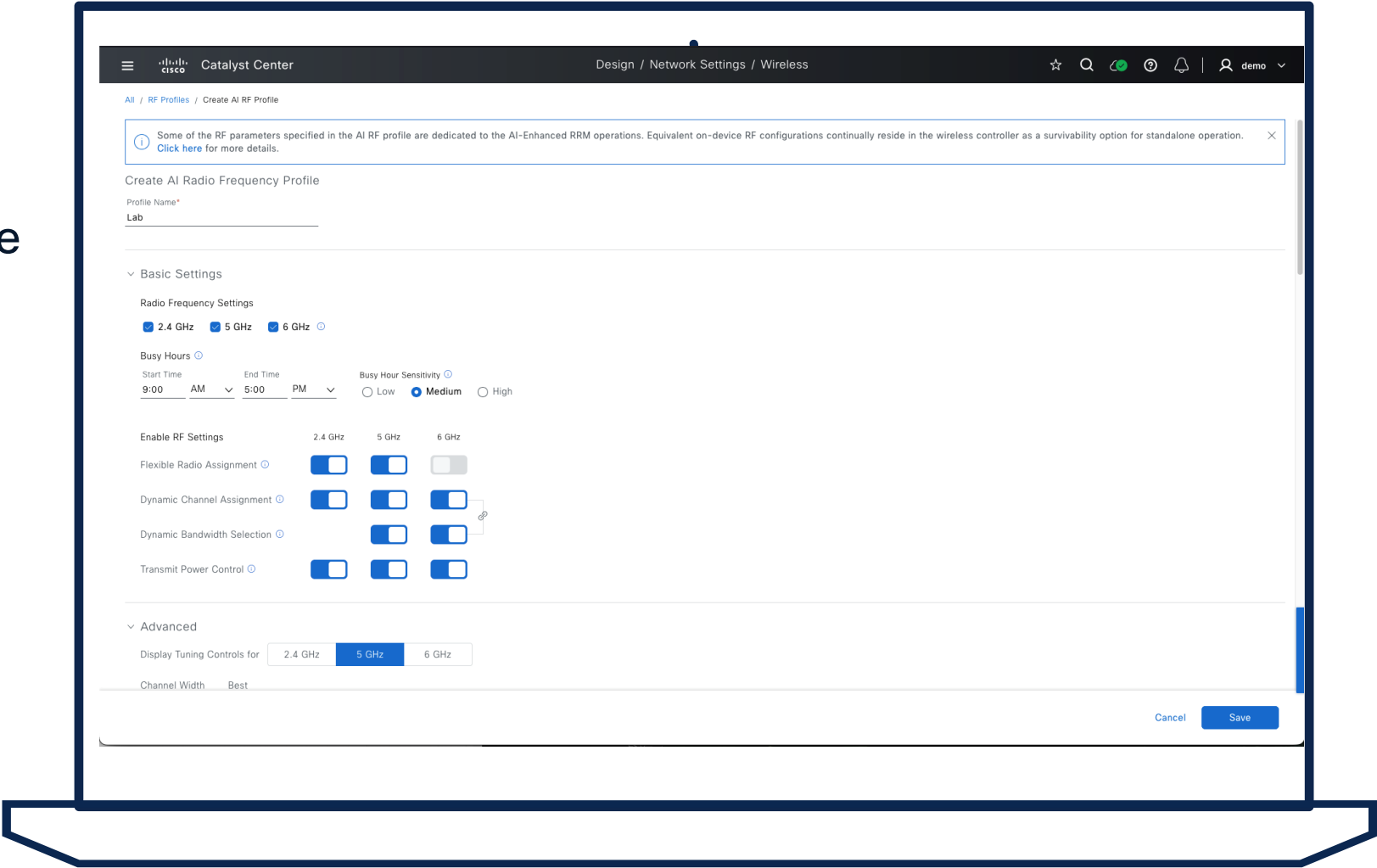
Advanced RF Tuning in Cisco Wireless - Become an Expert
While Getting a little Help from Cisco AI
BRKEWN-3413

AI-RRM: RF Profiles

Design > Network Settings > Wireless > RF Profile (AI RF Profile)



Give AI-RRM your constraints. Configure to match your existing profile and environment.

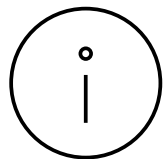


AI-RRM: Time Zones (they matter!)

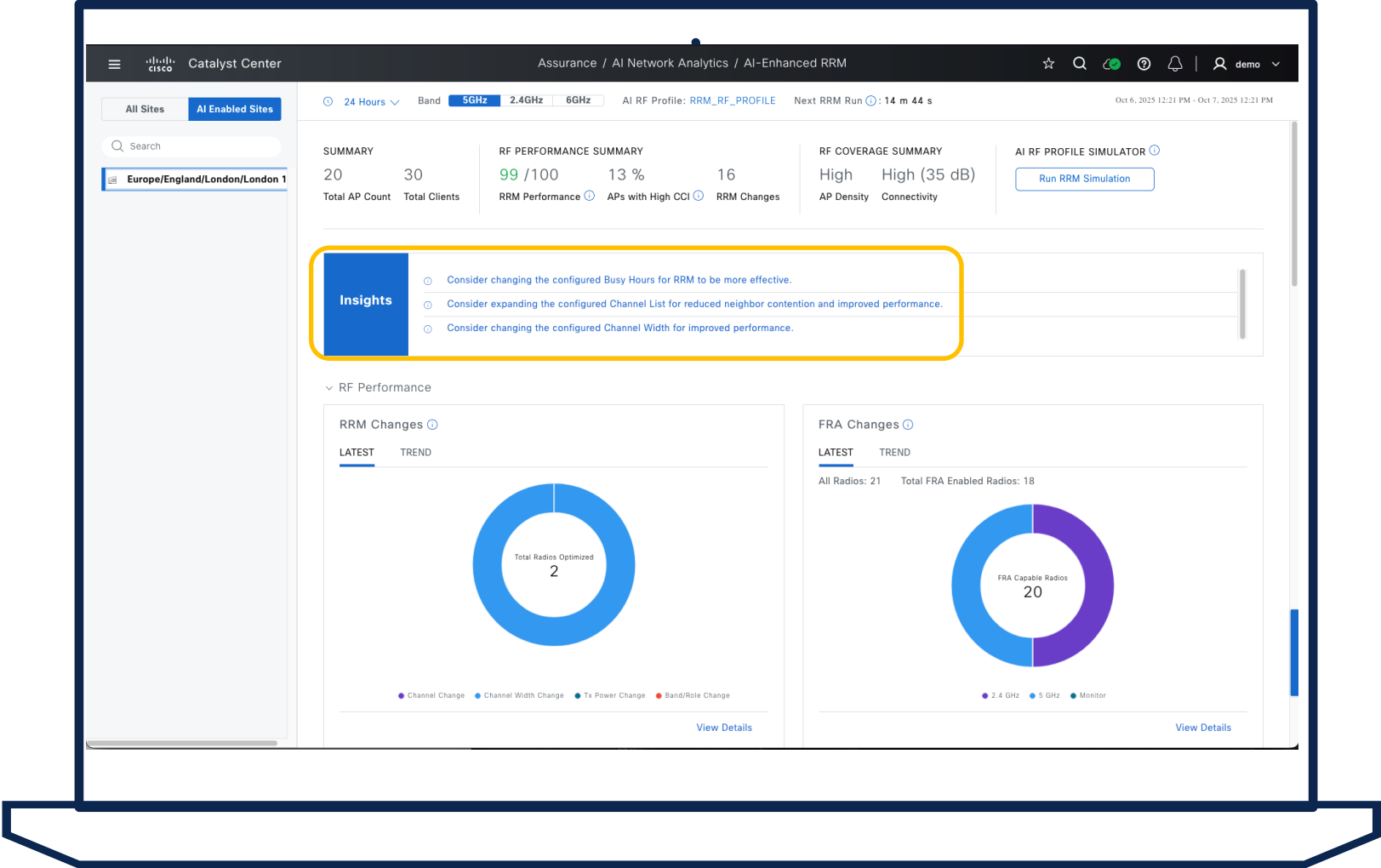


AI-RRM: Review Review Review (and simulate)

Assurance > AI-RRM

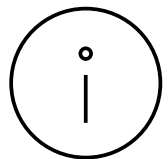


Per building RF scores & Insights to help drive visibility and continual improvement.

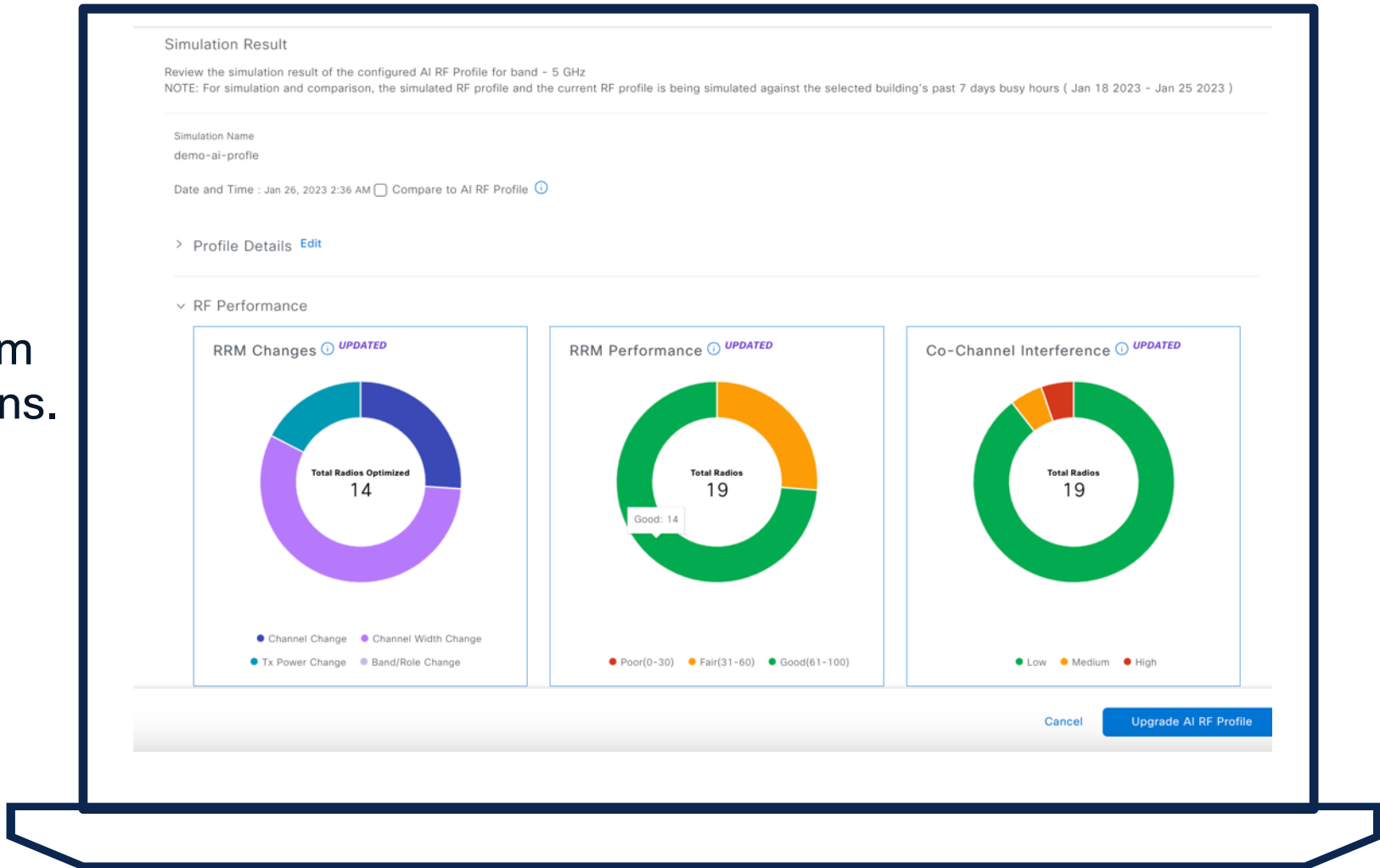


AI-RRM: Review Review Review (and simulate)

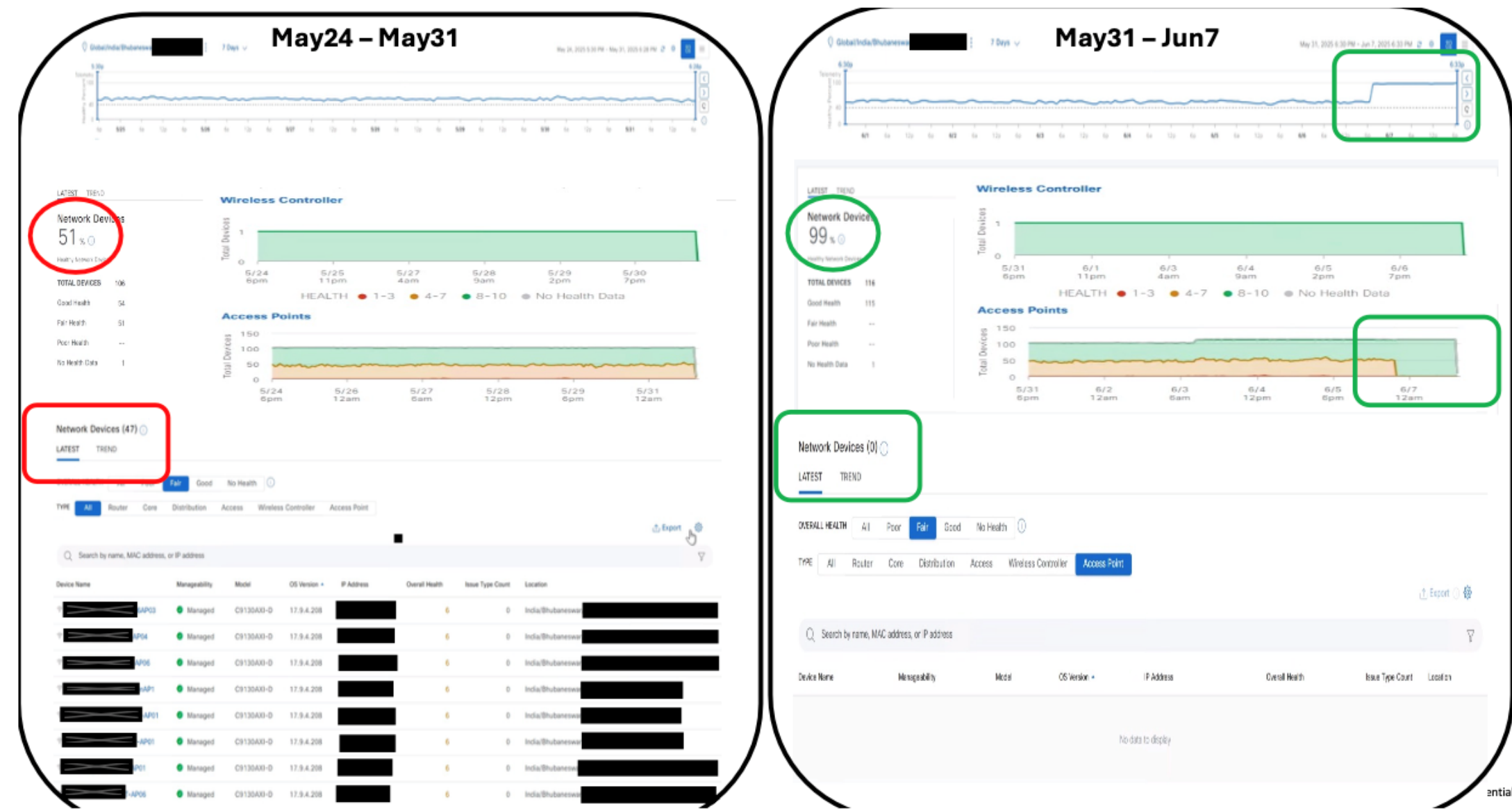
Assurance > AI-RRM



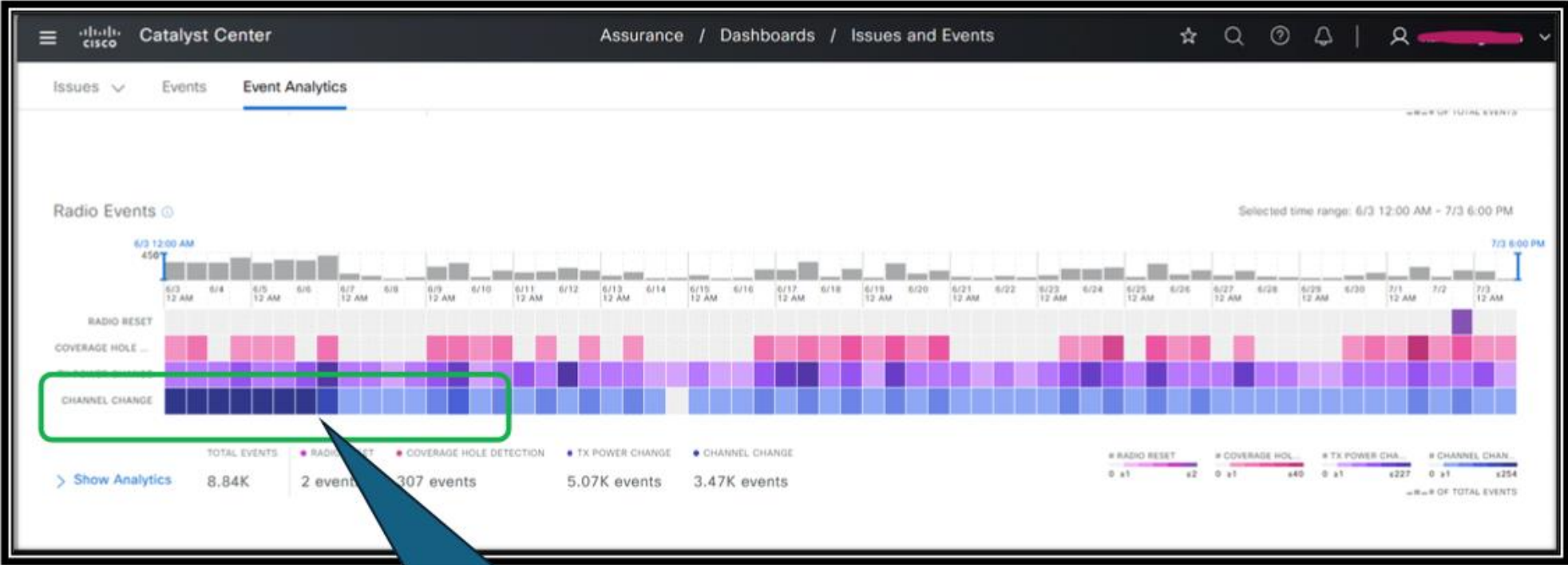
Simulate the impact of changes to the RF profile before applying to understand potential improvements gained from adopting recommendations.



AI-RRM: A real world result



AI-RRM: A real world result



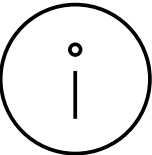
The darker the color more the changes in wireless network

A Checklist for Success:

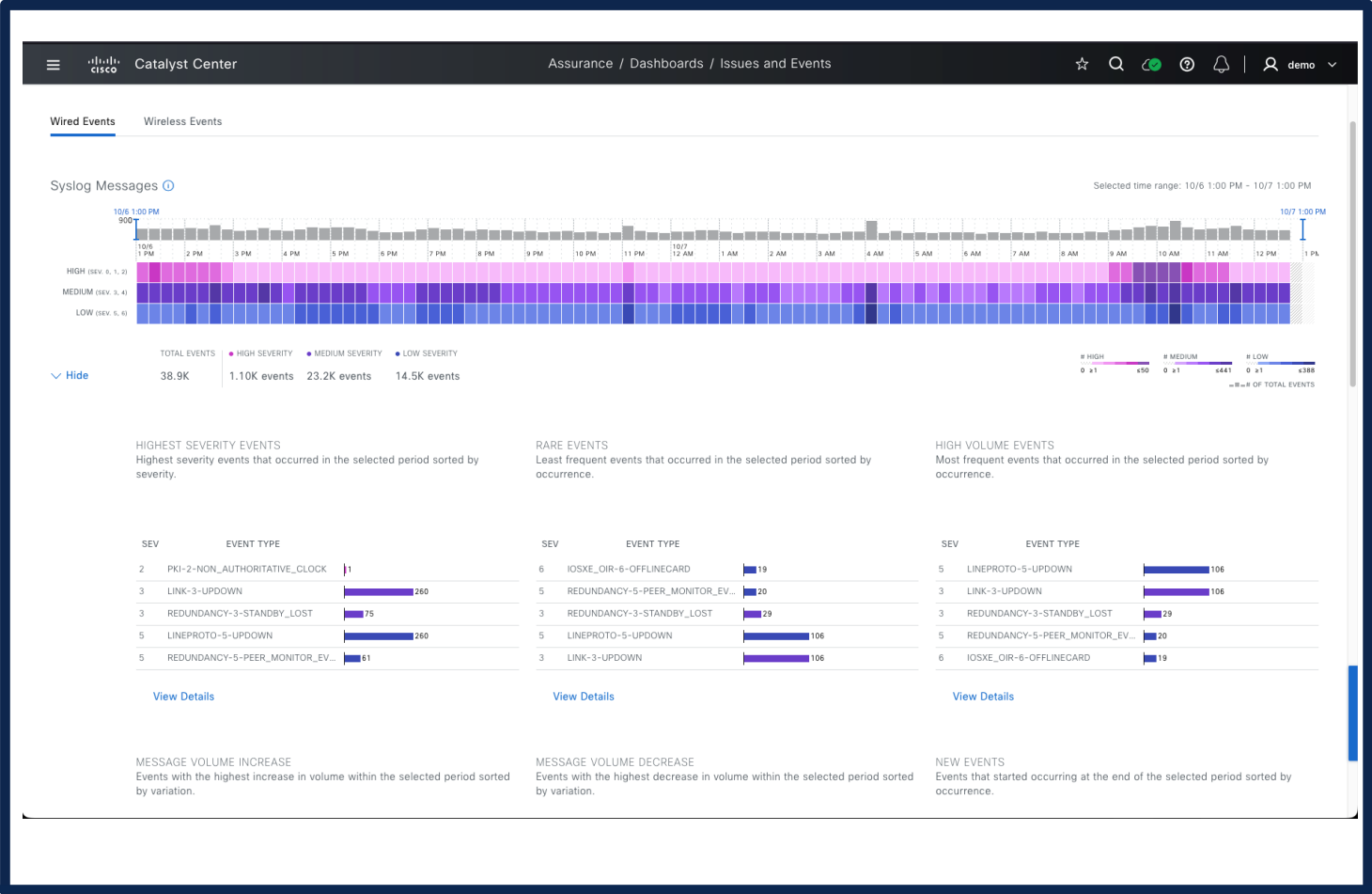
AI Event Analytics

Event Analytics: Uncover what you can't see

Assurance > Issues & Events > Event Analytics

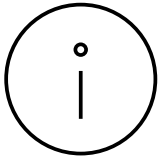


Understand trends and anomalies that you might not know are occurring in your environment, discovering insights into that annoying issue that has been plaguing you for a long time.

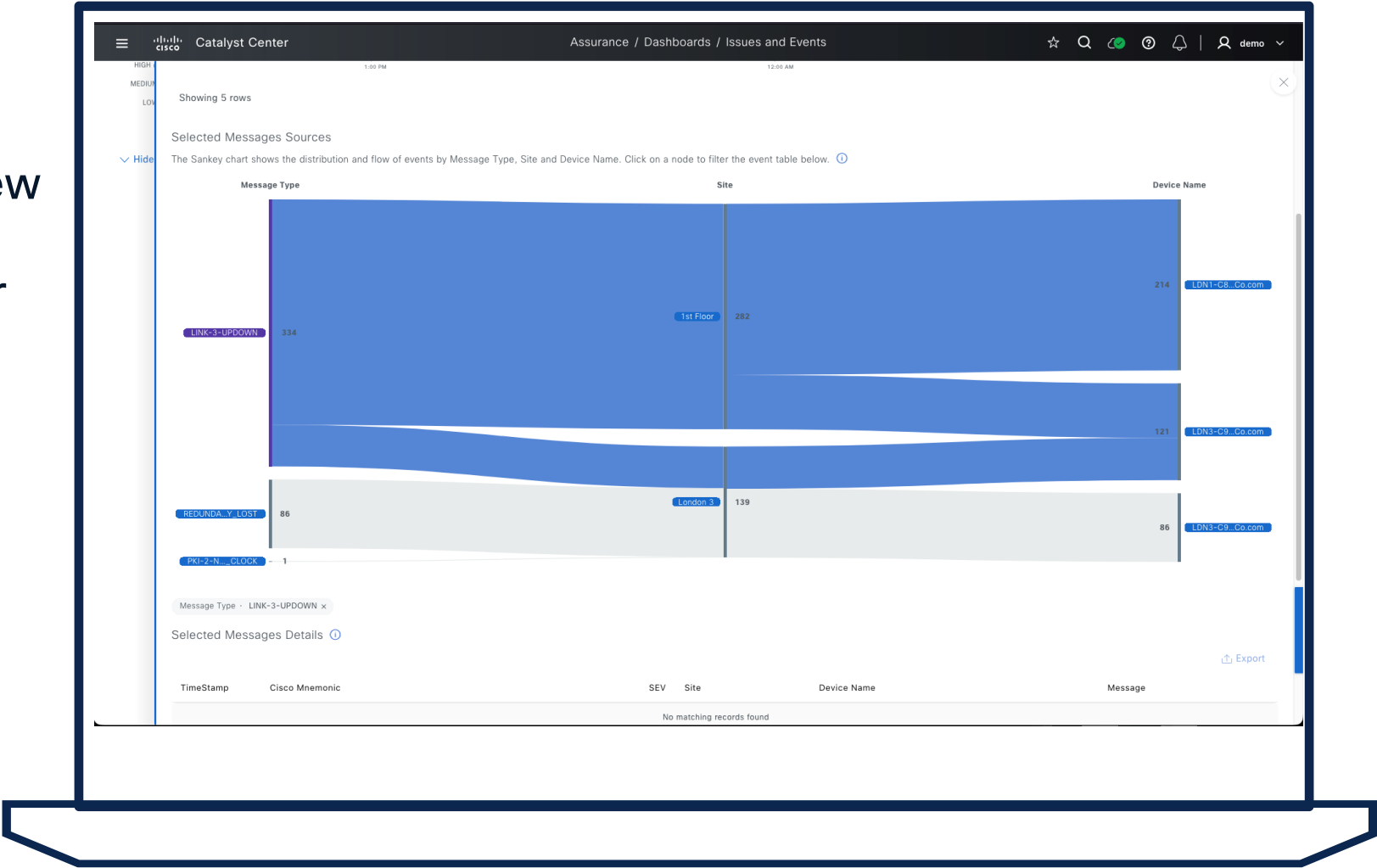


Event Analytics: Wired Superpowers

Assurance > Issues & Events > Event Analytics



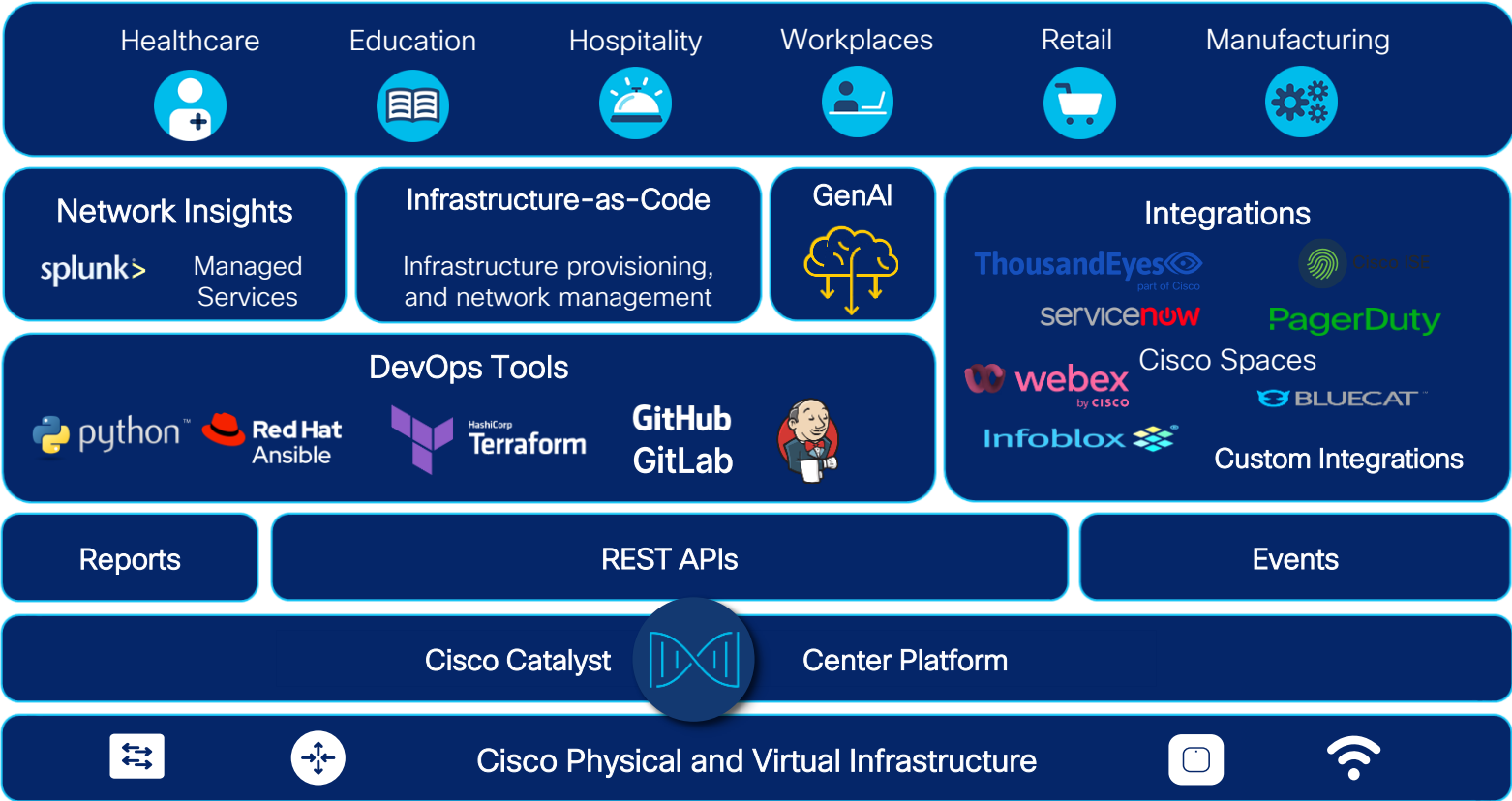
Investigate High severity, Rare, High Volume, and New events with data driven insights to help drive faster time to resolution.



A Checklist for Success:

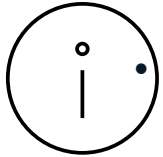
Integrations

Integrations: The Ecosystem

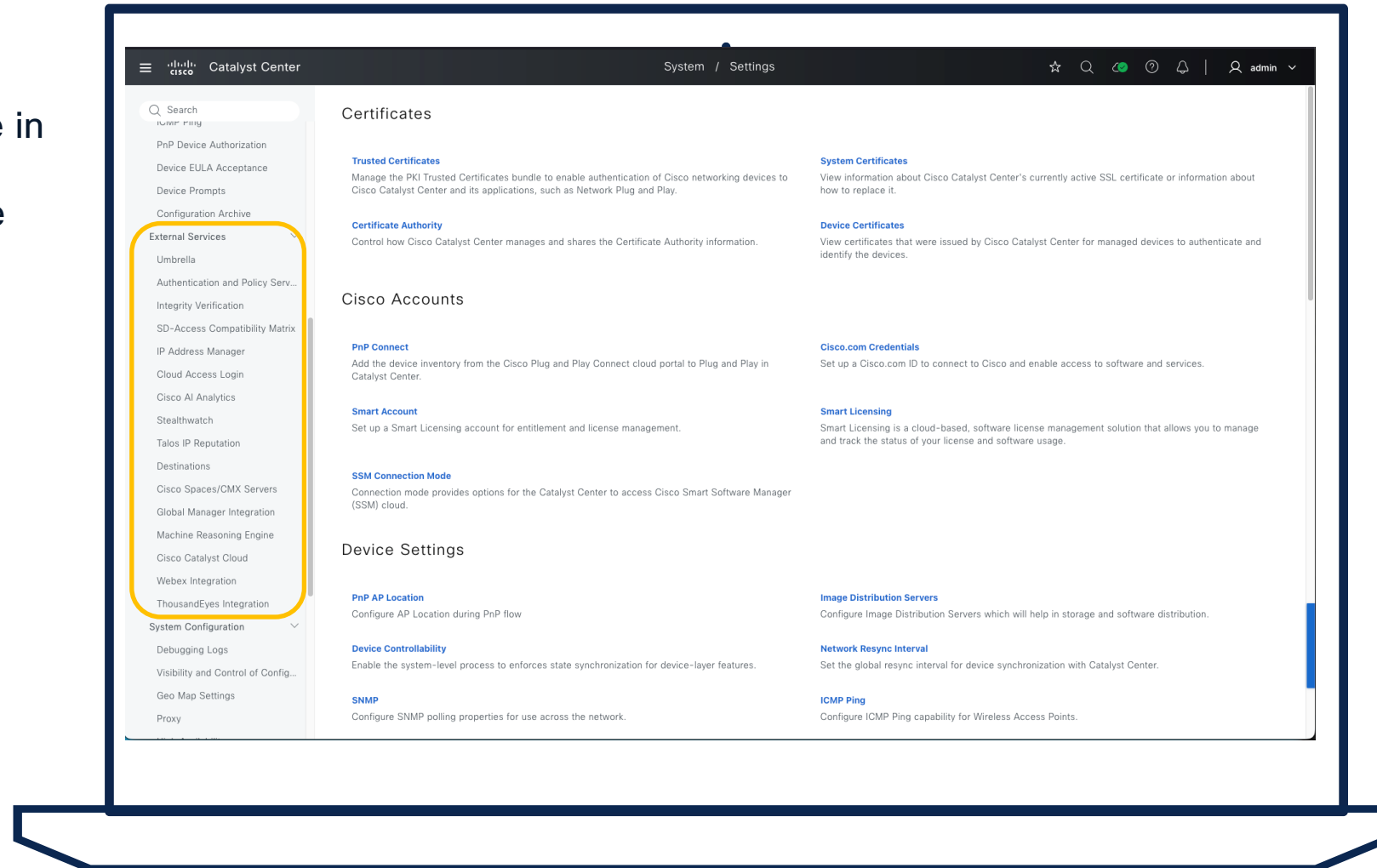


Integrations: External Services

System > Settings

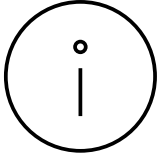


External integrations bring value in to Catalyst Center, extend it's capabilities and provide a single view to multiple sources of information to assist in troubleshooting.



Integrations: Getting Data Out – Splunk

Platform > Developer Toolkit



- Integration using the Cisco Catalyst Apps or the Cisco EN Integration Apps
- Webhook notifications to Splunk HTTP Event Collectors
- Run Python scripts hosted by Splunk – trigger reports runs and import data file
- Syslog notifications (Configured in Network Settings)

The screenshot shows the Splunk Enterprise web interface. The top navigation bar includes the Splunk logo, 'enterprise' label, 'Apps' dropdown, and a user profile for 'DEVTEST:GZAPODEA@CISCO.COM'. The main content area is titled 'Data inputs' and provides instructions on setting up data inputs. Below this, a section titled 'Local inputs' contains a table with the following data:

Type	Inputs	Actions
Files & Directories Index a local file or monitor an entire directory.	13	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	3	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	1	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	2	+ Add new
Scripts Run custom scripts to collect or generate more data.	25	+ Add new
cisco_dnac_clienthealth Go to the add-on's configuration UI and configure modular inputs under the Inputs menu.	2	+ Add new
cisco_dnac_compliance Go to the add-on's configuration UI and configure modular inputs under the Inputs menu.	2	+ Add new

A Checklist for Success:

API's & Automation



**WHO LIKES DOING THE
SAME THING OVER
AND OVER?**



**WHO THINKS
AUTOMATING A
TASK WILL LEAVE
THEM OUT OF
A JOB?**

**WHO ISN'T
COMFORTABLE WRITING CODE,
AS THAT'S FOR THE SW DEVS?**

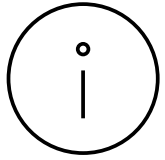


**WHAT IF YOU
COULD START SMALL
AND AUTOMATE LITTLE
PARTS TO FREE YOU UP
FOR MORE FUN THINGS**



API's: Ever Growing

Platform > Developer Toolkit



Accelerating release of new APIs:

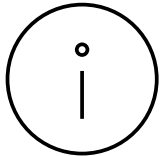
- Version 2.3.5.3 – 476 APIs
- Version 2.3.7.5 – 520 APIs
- Version 2.3.7.6 – 876 APIs
- Version 2.3.7.9 – 1132 API's
- Version 3.1.x – 1137 API's

The screenshot shows the Cisco Catalyst Center Developer Toolkit interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and the path 'Platform / Developer Toolkit'. Below this, there are tabs for 'APIs', 'Integration Flows', and 'Event Notifications'. A left sidebar contains a search bar and a list of categories: Appliance, Authentication, Cisco DNA Center System, Connectivity, Fabric Wireless, SDA, Wired (selected), Wireless, Ecosystem Integrations, Event Management, Integrations, Know Your Network, Operational Tasks, Policy, Site Management, System, and System Settings. The main content area is titled 'Wired' and displays a table of APIs. The table has columns for Method, Name, Description, URL, and Actions. The APIs listed are for creating, updating, and retrieving configurations for wired devices and features.

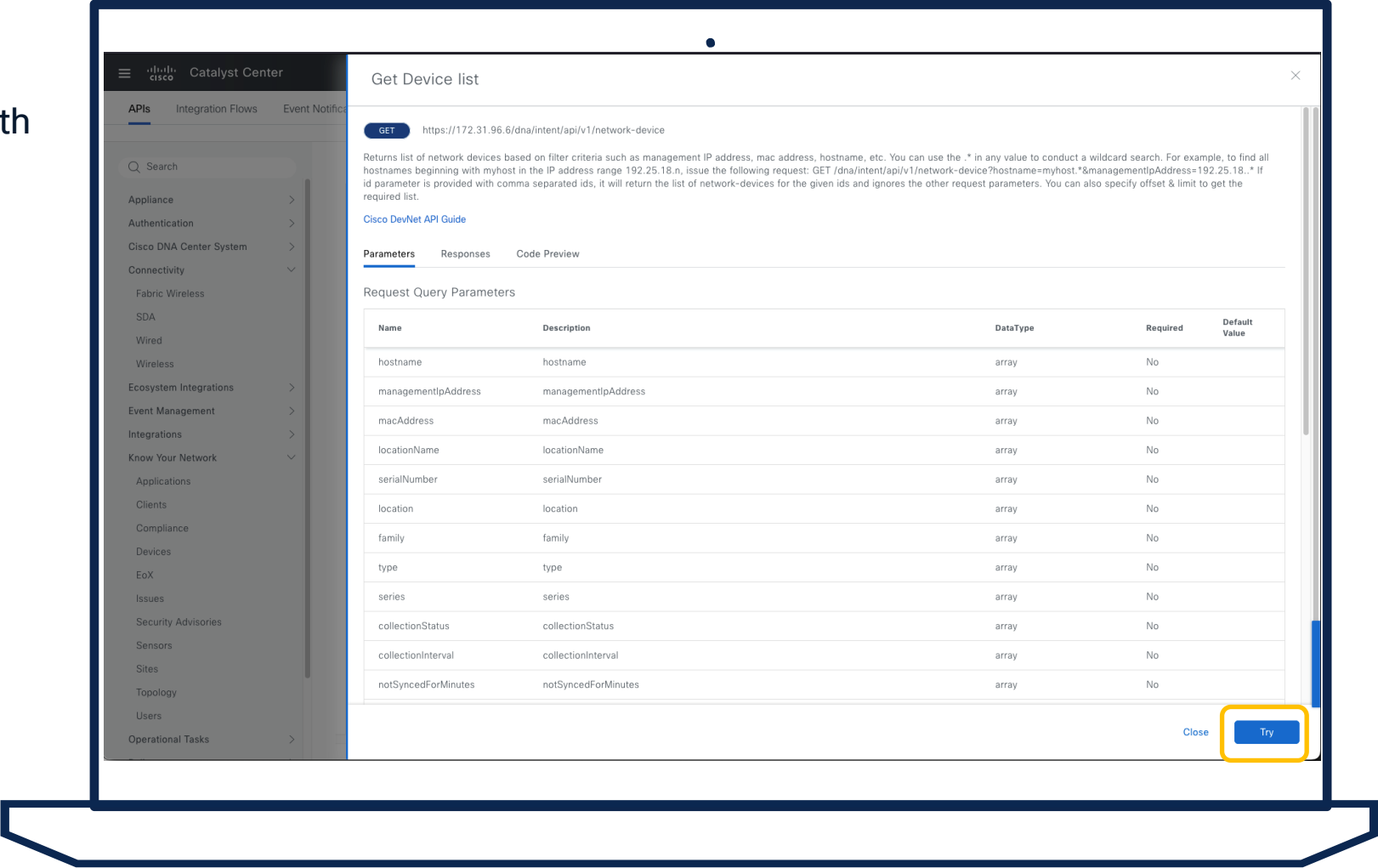
Method	Name	Description	URL	Actions
POST	Create a configuration model for the intended configs for a device.	Create a configuration model for the intended configs for a device. This is a pre-requisite to preview the generated device config for the provisioning...	/dna/intent/api/v1/wired/networkDevices/{networkDeviceId}/configFeatures/intended/configurationModels	...
PUT	Update configurations for an intended layer 2 feature on a wired device.	This API updates the configurations for an intended feature on a wired device. Only the feature configurations to be changed need to be added to the intended...	/dna/intent/api/v1/wired/networkDevices/{deviceId}/configFeatures/intended/layer2/{feature}	...
GET	Get configurations for a deployed layer 2 feature on a wired device.	The API returns configurations for a deployed layer 2 feature on a wired device.	/dna/intent/api/v1/wired/networkDevices/{deviceId}/configFeatures/deployed/layer2/{feature}	...
GET	Get number of configurations for a deployed layer 2 feature on a device.	The API returns the number of configurations for a deployed layer 2 feature on a device.	/dna/intent/api/v1/wired/networkDevices/{deviceId}/configFeatures/deployed/layer2/{feature}/count	...
POST	Deploy the intended configuration features on a wired device.	Deploy the intended configuration features on a wired device. This can be used only if the provisioning settings do not require Preview or ITSM Approval...	/dna/intent/api/v1/wired/networkDevices/{networkDeviceId}/configFeatures/intended/deploy	...
PUT	Update configurations for intended layer 2 features on a wired device.	This API updates the configurations for the intended features on a wired device. Only the feature configurations to be changed need to be added to the...	/dna/intent/api/v1/wired/networkDevices/{deviceId}/configFeatures/intended/layer2	...
GET	Get service deployment status.	Returns service deployment status based on filter criteria.	/dna/intent/api/v1/wired/networkDevices/{networkDeviceId}/configFeatures/intended/serviceDeployments	...
GET	Get the supported layer 2 features on a wired device.	The API returns the supported layer 2 features on a wired device.	/dna/intent/api/v1/wired/networkDevices/{deviceId}/configFeatures/supported/layer2	...
GET	Get configurations for an intended layer 2 feature on a wired device.	This API returns the configurations for an intended layer 2 feature on a wired device. Even after the intended configurations are deployed using the API...	/dna/intent/api/v1/wired/networkDevices/{deviceId}/configFeatures/intended/layer2/{feature}	...

API's: Ever Growing

Platform > Developer Toolkit

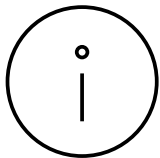


Explore API's, get comfortable with what you can do, and not have to write any code



API's: Ever Growing

Platform > Developer Toolkit



Try an API, see the results, and then take that data from there. For more details check out the developer portal.



Documentation

All

Catalyst Center

Cisco Catalyst Center API 2.3.7.9

Search docs

BETA

DELETE

Delete image

GET

Get software image details

GET

Returns count of software images

POST

Import local software image

POST

Add image distribution server

GET

Retrieve image distribution servers

PUT

Update the list of sites for the network device product name assigned to the software image

DELETE

Unassign network device product name from the given software image

GET

Returns network device product names for a site

POST

Tagging golden image

POST

Initiates sync of software images from Cisco.com

PUT

Update remote image distribution server

DELETE

Remove image distribution server

GET

Retrieve specific image distribution server

GET

Get Device Family Identifiers

GET

Retrieve network device product name

POST

Tag as Golden Image

GET

Returns the image summary for the given site

GET

Get network device

Software Image Management (SWIM)

Tag as Golden Image

Operation Id: tagAsGoldenImage

Description: Golden Tag image. Set sitelid as -1 for Global site.

POST

/dna/intent/api/v1/image/importation/golden

Request Parameters

Header

Accept | string

MIME type / MIME subtype Consumed

default = "application/json"

Content-Type | string

MIME type / MIME subtype Produced

default = "application/json"

Request body

request

Schema Definition

Example Body

TagAsGoldenImageRequest

Swim Golden Tag DTO

deviceFamilyIdentifier: string Device Family Identifier e.g. : 277696480-283933147,

Configuration

Parameters

Code Snippets

Curl

Python

Nodejs

```
curl -L --request POST \
--url /dna/intent/api/v1/image/importation/golden \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--data '{}'
```

Copy

API's: Examples – Copilots & LLM's are your friend

- Scaffold automation (VLAN/SVI generators, ACL templates)
- API starters (Catalyst Center, vManage, etc) and pagination handling
- IaC – Ansible & Terraform
- dnacentersdk for ease of implementation in python scripting
- Build & resolve issues with Jinja & Velocity templates
- Data parsing utilities for “show” outputs
- Quick one-offs: curl, regex, bash utilities



API's: Examples – Webhook Receiver



- Structure: role + context + constraints + examples + ask
- Weak: “Make a webhook server”
- Strong: “Flask app receiving Catalyst Center webhooks, verifying HMAC, forwarding to Teams Incoming Webhook, with health check and retries; provide README and sample payload”
- Tips:
 - Ground with file paths and API versions
 - State inputs/outputs and validation rules
 - Ask for tests and edge cases
 - Prefer smaller, iterative prompts for refactorings
- <https://github.blog/ai-and-ml/github-copilot/5-tips-for-writing-better-custom-instructions-for-copilot/>

API's: Examples – Daily Health Checks



Device Health Breakdown

Health Category	Count	Percentage
Poor Health (≤3)	16	27.1%
Fair Health (4-7)	4	6.8%
Good Health (>7)	39	66.1%

Critical & High Priority Issues

Issue Type	Count
Critical Issues (P1)	3
High Priority Issues (P2)	0

Client Health Summary

Connection Type	Total	Poor Health	Fair Health	Good Health
Wired Clients	1	1	0	0
Wireless Clients	0	0	0	0
All Clients	1	1	0	0

System Health Summary

System Component	Status
ISE Integration	2/2 Available
System Services	0/141 Running
System Backups	3/3 Successful

Wrapping up



Build Foundations

Baseline core settings for security, stability, and full feature enablement.



Customise Metrics

Tailor alerts, profiles & health scores to your needs.



Leverage AI insights

Optimize RF & detect hidden issues with AI-RRM & Event Analytics.



Integrate & Automate

Connect to tools & APIs to streamline network operations.

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

