



# DNA Center

Michel Peters

Technical Leader Engineering

[michelpe@cisco.com](mailto:michelpe@cisco.com)

# Objective

The key objective of the DNA series is to cover specific technologies making up the Digital Network Architecture solution aka Software Defined Access (SDA).

This session will go into how to setup the Appliance, setup DNA Center and deploy a small fabric

# Agenda

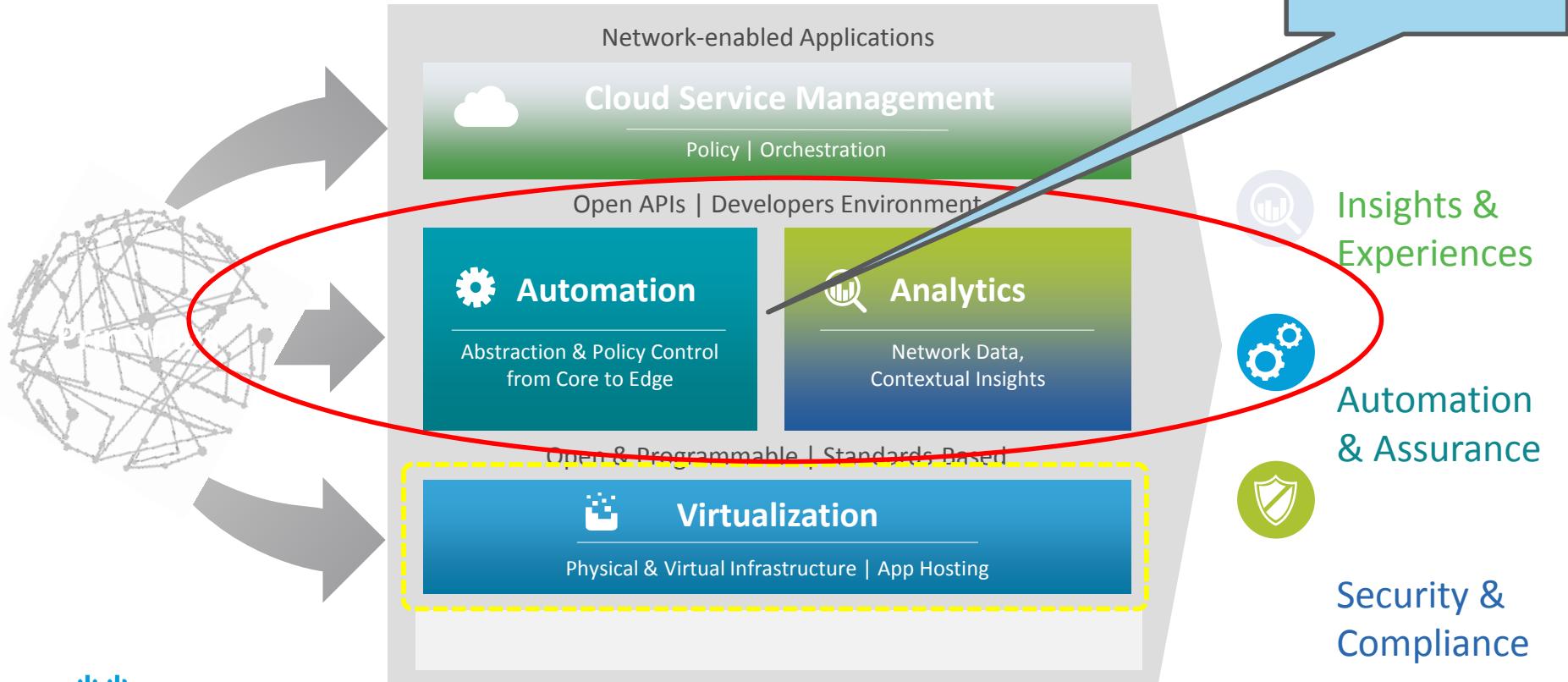
- DNA Center Appliance Installation
- Basic setup of DNA Center
- Deploying a fabric

# DNA Center Appliance



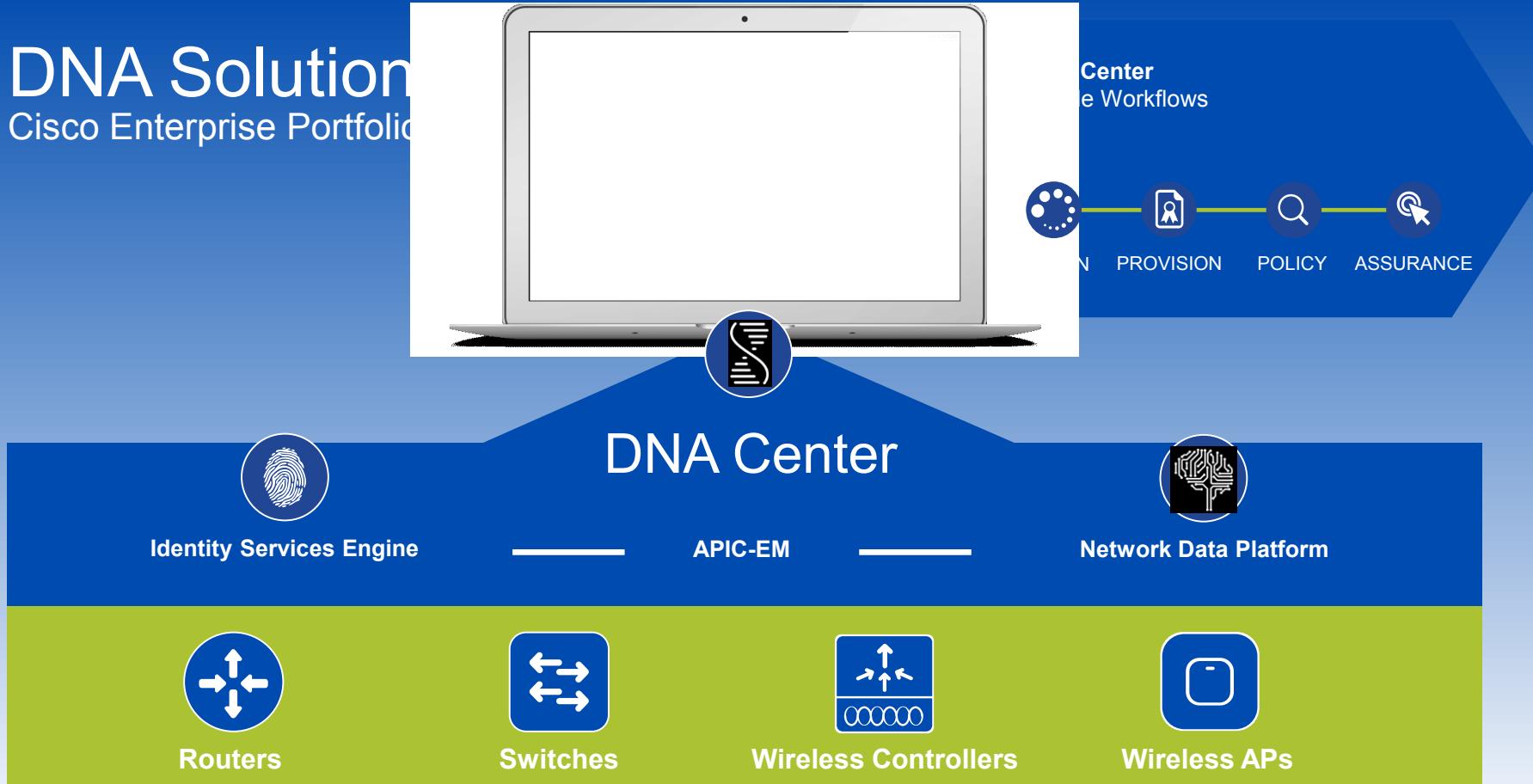
# Cisco Digital Network Architecture

## Overview



# DNA Solutions

Cisco Enterprise Portfolio



# DNA Center Appliance (DNA-HW-APL)

Drive Bays	Disk Type	Function
1-2	2x 480G	Master
3-4	2x 1.9TB	Automation
5-8	4x 1.9TB	Assurance

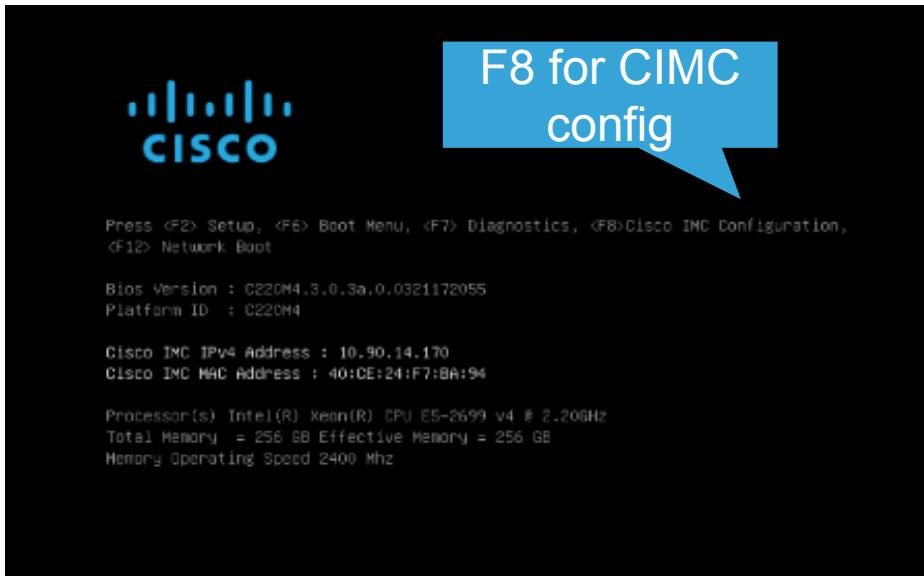


CIMC Management port

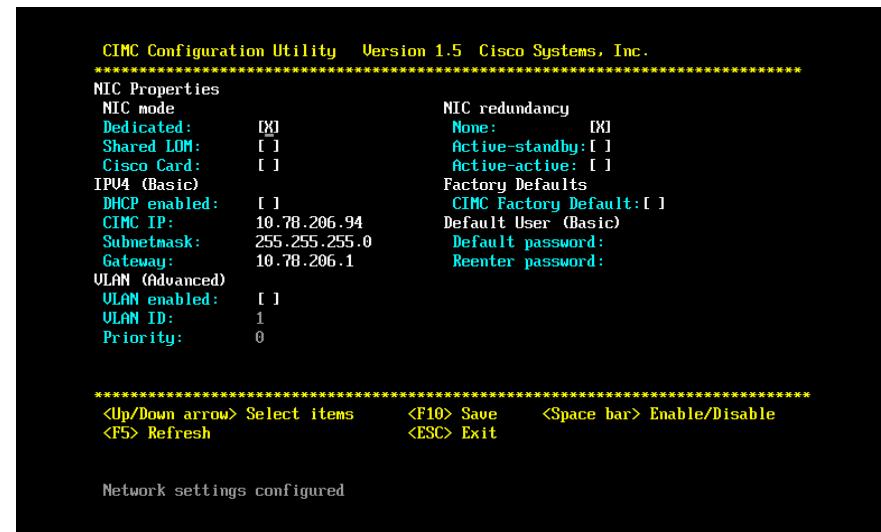
DNA Center interfaces

DNA Center only supported on the DNA Appliance.  
Currently no VM support

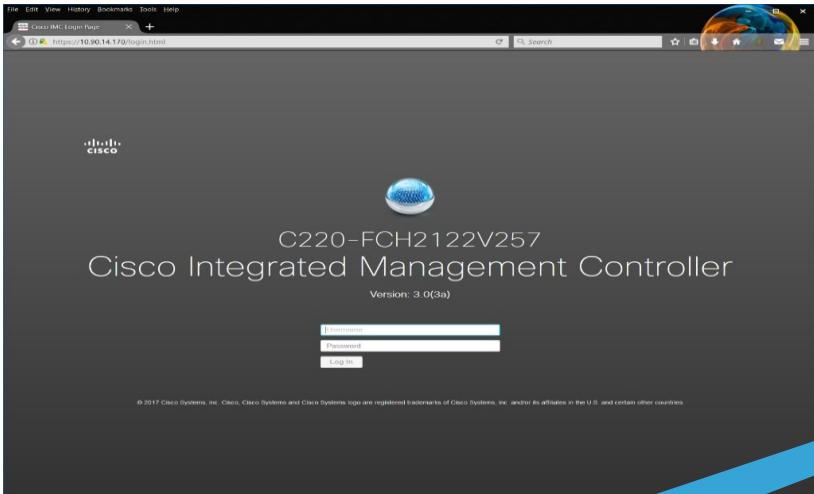
# Cisco Integrated Management Controller Setup



CIMC needs an IP address either via DHCP or using a Keyboard/monitor



# Accessing CIMC KVM



KVM can be launched from CIMC

Server Properties

Product Name:	C220.FCH2122V257
Serial Number:	FCH2122V257
PID:	DN1-HW-APL
UUID:	00E94208-F200-4B5C-AC1D-59ABFD4BA105
BIOS Version:	C220M4.3.0.3a.0.0321172055
Description:	
Asset Tag:	Unknown

Server Utilization

Power State:	<input type="radio"/> Off
Overall Server Status:	<span style="color:red">✗</span> Moderate Fault
Temperature:	<span style="color:green">✓</span> Good
Overall DIMM Status:	<span style="color:green">✓</span> Good
Power Supplies:	<span style="color:red">✗</span> Fault
Fans:	<span style="color:green">✓</span> Good
Locator LED:	<input type="radio"/> Off
Overall Storage Status:	<span style="color:green">✓</span> Good

# DNA Center Initial setup

Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one or more options below to specify how you would like to configure this host:

[Start a DNA-C Cluster](#)

[Join a DNA-C cluster](#)

< exit >

Maglev Configuration Wizard 0.1.4

## STEP #4

The wizard has discovered 1 physical network adapter(s) installed on the appliance.

Enter the network settings for the 1st network adapter (00:50:56:a5:44:09 - ens160).

Select "Cluster Link" if used for cluster communication.

### NETWORK ADAPTER #1 (ens160)

Host IP Address:

Enter the IP address to use for this network adapter

De

DNS Servers:

Static Routes:

Cluster Link

Configure IPv6 address

<< back

< cancel >

done >>

next >>

Maglev Configuration Wizard 0.1.4



# DNA Center Initial setup

STEP #8

**NETWORK PROXY**

The controller appears to be behind a network proxy.  
Enter your network proxy configuration settings to enable cloud connectivity.

HTTPS Proxy:  
[ ] Enter the IP address and port number of the HTTPS proxy (example:  
HT http://192.168.1.100:3128).

DNA Center needs to reach the cloud to download updates

<< back      < cancel >      next >>

Maglev Configuration Wizard 0.1.4

STEP #11

**MAGLEV CLUSTER DETAILS**

Enter the connectivity details for your existing Maglev cluster

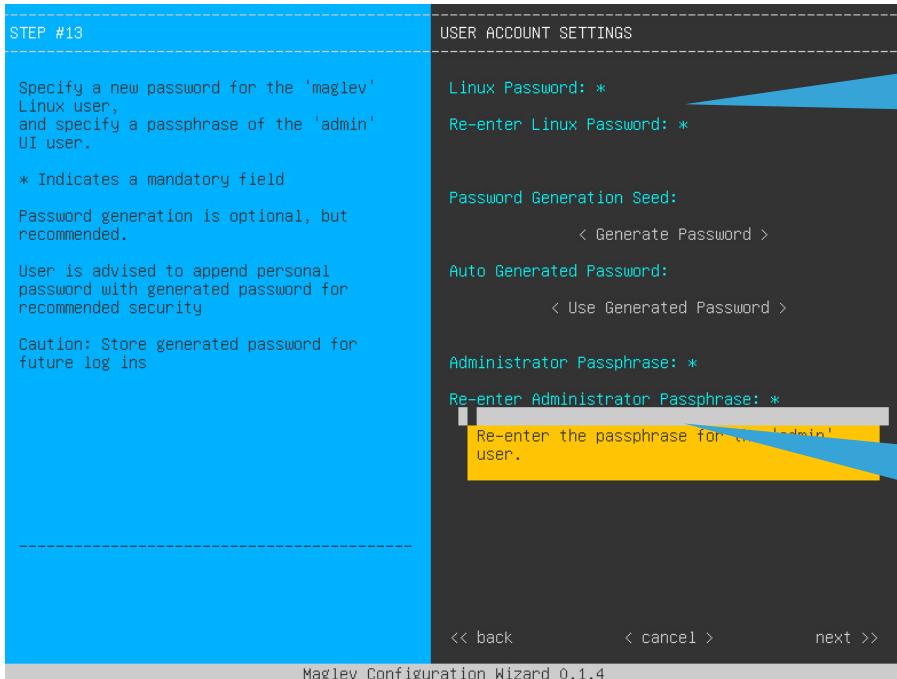
Cluster Virtual IP Address:  
[ ] (Optional) Enter the Virtual IP address to be used to reach the Cluster's Web Interface

Clustering coming in future versions of DNAC

<< back      < cancel >      next >>

Maglev Configuration Wizard 0.1.4

# DNA Center username setup



Local console access and ssh  
access using port 2222  
Username maglev

User for access to GUI ,  
username admin

# DNA Center additional networking settings

STEP #14

Enter the IP address of the NTP server that the controller will use.

It is recommended to specify 3 or more NTP servers to improve availability and time accuracy.

Please note that the NTP server(s) must be accessible in order for the APIC-EM configuration to succeed.

\* Indicates a mandatory field

NTP SERVER SETTINGS

NTP Servers: \*

Enter a single NTP server address or a space separated list of NTP server addresses.

It is recommended to specify 3 or more NTP servers to improve availability and time accuracy.

<< back      < cancel >      next >>

Maglev Configuration Wizard 0.1.4



Reachable NTP server

STEP #16

Enter the IP networks for cluster services network and api network to use. These network shouldn't overlap with the existing enterprise network.

The minimum recommended size of each network is 2048, i.e. /21 subnets.

\* Indicates a mandatory field

MAGLEV ADVANCED SETTINGS

Services Subnet: \*

Cluster Services Subnet: \*

Enter the Subnet to be used for the Cluster Services networking

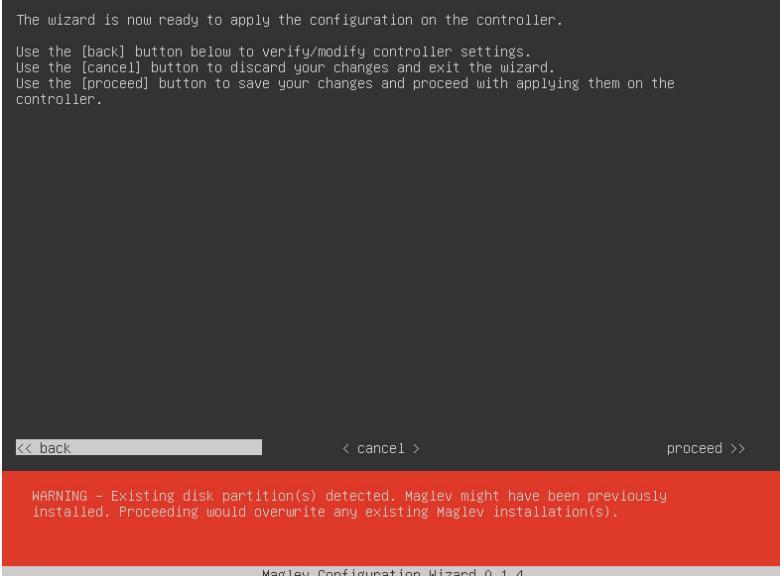
To avoid IP conflicts, this subnet must not be used elsewhere

<< back      < cancel >      next >>

Maglev Configuration Wizard 0.1.4

2 subnets (/21) for internal use.  
Not for external use:

# DNA Center Installation script

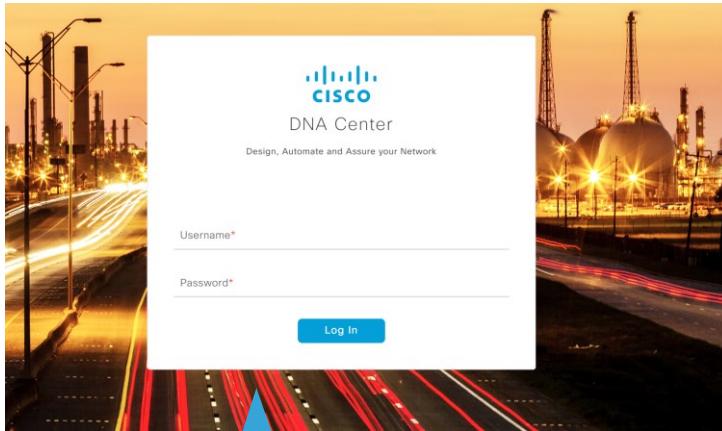


```
2017-12-08 07:40:50,844 | post_reboot : Collecting all addons APIs
2017-12-08 07:40:50,968 | post_reboot : set_fact
2017-12-08 07:40:51,012 | post_reboot : set_fact
2017-12-08 07:40:51,053 | post_reboot : Adding addons routes to API gateway
2017-12-08 07:40:55,663 | post_reboot : Configure request-termination plugin on api gateway for internal route
2017-12-08 07:40:55,951 | post_reboot : Creating Default Tenant on API gateway
2017-12-08 07:40:56,229 | post_reboot : Get passphrase from secret
2017-12-08 07:40:56,563 | post_reboot : set_fact
2017-12-08 07:40:56,605 | post_reboot : Creating Default Tenant secret on API gateway
2017-12-08 07:40:56,928 | post_reboot : Waiting for Identity Management service to be running
2017-12-08 07:43:12,432 | post_reboot : Creating Default Tenant on Identity Management
2017-12-08 07:43:14,936 | post_reboot : Adding default rbac resource
2017-12-08 07:43:19,846 | post_reboot : Adding rbac resource for user
2017-12-08 07:43:20,116 | post_reboot : Adding default rbac permissions for super admin
2017-12-08 07:43:26,540 | post_reboot : Adding default rbac permissions for network-admin and observer
2017-12-08 07:43:32,029 | post_reboot : Adding rbac url mappings
2017-12-08 07:43:37,929 | post_reboot : Adding rbac permission for superadmin, network-admin and observer to update login password
2017-12-08 07:43:38,319 | post_reboot : Adding rbac url mappings for user password update permission
2017-12-08 07:43:38,627 | post_reboot : Enabling JWT security on api gateway
2017-12-08 07:43:42,288 | post_reboot : include
2017-12-08 07:43:42,668 | post_reboot : Creating Maglev Catalog service
2017-12-08 07:43:45,732 | post_reboot : Waiting for Maglev Catalog service to be running
2017-12-08 07:43:56,571 | post_reboot : Get passphrase from secret
2017-12-08 07:43:56,899 | post_reboot : set_fact
2017-12-08 07:43:56,944 | post_reboot : Configuring maglev CLI
2017-12-08 07:44:00,656 | post_reboot : Syncing local service catalog with parent service catalog
2017-12-08 07:44:00,695 | post_reboot : Pulling latest version of maglev system Package from parent service catalog
2017-12-08 07:44:00,730 | post_reboot : Looking for default Libraries to deploy
2017-12-08 07:44:00,991 | post_reboot : Looking for default Packages to deploy
2017-12-08 07:44:01,181 | post_reboot : Pushing default Libraries
2017-12-08 07:44:22,068 | post_reboot : Pushing default Packages
```

Be patient, install can take few hours



# GUI access



HTTPs access to  
DNA Center



What can DNA Center do? Take a [Tour](#).

Need to add functionality to DNA Center? [Add applications](#)

Want to learn more about DNA Center? [Watch video](#)

## Design

Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.

- Add site locations on the network
- Designate golden images for device families
- Create wireless profiles of SSIDs

## Provision

Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.

- Discover and provision switches to defined sites
- Provision WLCs and APs to defined sites
- Set up Campus Fabric across switches

## Policy

Use policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.

- Segment your network as Virtual Networks
- Create scalable groups to describe your critical assets
- Define segmentation policies to meet your policy goals

## Assurance BETA

Use proactive monitoring and insights from the network data platform to predict problems and ensure that policy and configuration changes achieve the consistent, high-quality user experience you want.

- Assurance Health
- Assurance Issues

DNA Center home page

# App Management

System settings,  
app management

Assurance - Base	Running	1.0.5.471
Command Runner	Running	2.1.0.64153   <a href="#">Uninstall</a>
Network Controller Platform	Running	2.1.0.64153   <a href="#">Uninstall</a>
Automation - Sensor [EFT]	Not Installed	2.1.0.64153   <a href="#">Install</a>
NCP - Services	Running	2.1.0.64153
Infrastructure	Running	1.0.4.588
Automation - Device Onboarding	Running	2.1.0.64153   <a href="#">Uninstall</a>
Network Data Platform - Base Analytics	Running	1.0.6.332
Automation - SD Access	Not Installed	2.1.0.64153   <a href="#">Install</a>
Automation - Image Management	Running	2.1.0.64153
Assurance - Path Trace	Running	2.1.0.64153

Apps can be  
downloaded and  
installed from cloud

# DNA Center, Basic setup, ISE integration



# Adding ISE

POLICY PROVISION ASSURANCE

Settings Data Platform Users Backup & Restore

### Authentication and Policy Servers

Use this page to specify the servers that authenticate DNA Center users. ISE servers can also supply policy and user information.

IP Address	Protocol	Type
		No matching records found

Add AAA/ISE server

Server IP Address\*

Shared Secret\*  This field is required

Cisco ISE server

Username\*

Password\*

FQDN\*

Subscriber Name\*

SSH Key

View Advanced Settings

Username on ISE, for  
admin (UI) and  
console access (ssh)

FQDN of ISE  
Certificates(Gi0)

A username to be  
created on pxgrid



# ISE Successfully added

The screenshot shows the Cisco DNA Center interface. At the top, there are tabs for DESIGN, POLICY, PROVISION, and ASSURANCE. Below that, a navigation bar includes System 360, App Management, Settings (which is selected), Data Platform, Users, and Backup & Restore. A search bar is also present. On the left, a sidebar lists various management options like Certificate, Cisco Credentials, Debugging Logs, Device Controllability, IP Address Manager, Network Sync Interval, PKI Certificate Management, Proxy Certificate, SFTP, SNMP Properties, Telemetry Collection, and Trustpool. The main content area is titled "Authentication and Policy Servers" and contains a table with one row:

IP Address	Protocol	Type	Status
10.48.91.220	RADIUS	ISE	ACTIVE

At the bottom right of the main content area, there is a large blue callout box with the text "ISE Added and active".

The screenshot shows the Cisco DNA Center interface. At the top, there are tabs for DESIGN, POLICY, PROVISION, and ASSURANCE. Below that, a navigation bar includes System 360, App Management, Settings (selected), Data Platform, Users, and Backup & Restore. The main content area is divided into several sections:

- Hosts:** Shows a host entry for 10.48.91.204 with status "Deployed". A note indicates that enabling high availability requires installing a minimum of 3 hosts. It also links to the "Cisco DNA Center Appliance Installation Guide".
- External Network Services:** Shows two entries: "10.48.91.220 Identity Service Engine" and "PXGRID 10.48.91.220". Both are marked as "Available".
- IP Address Manager:** Shows a note that the IPAM server is not configured and provides a link to "Configure settings for IPAM".

A large blue callout box on the left side of this section contains the text "ISE reachable and pxgrid connection up".



# ISE Basic setup (ISE 2.3)

ISE Basic setup (ISE 2.3) - Node Configuration

Node Name: BRUSEENAC  
FQDN: BRUSEENAC.cisco40.com  
IP Address: 10.48.91.220  
Node Type: Identity Services Engine (ISE)

Role: STANDALONE **Make Primary**

Administration  
Monitoring (Primary)  
Other Monitoring Node

Policy Service

- Enable Session Services
- Include Node in Node Group: None
- Enable Profiling Service
- Enable Threat Centric NAC Service
- Enable SXP Service**
- Use Interface: GigabitEthernet 0
- Enable Device Admin Service
- Enable Passive Identity Service

pxGrid

Save Reset

Enable PxGrd

ISE Basic setup (ISE 2.3) - ERS Settings

Client Provisioning  
FIPS Mode  
Alarm Settings  
Posture  
Profiling  
Protocols  
Proxy  
SMTP Server  
SMS Gateway  
System Time  
ERS Settings

**ERS Settings**

General

External RESTful Services (Optional): REST API based on HTTPS over port 9060. This ERS service is disabled by default. An ISE Administrator with the "ISE-Admin" or "ERS-Operator" group assignment is required to use the API. For more information, please refer to the ERS SDK page at: <https://10.48.91.220:9060/doc/api/>

ERS Setting for Administration Node

- Enable ERS for ReadWrite** (selected)
- 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)** (selected)

Save Reset

Enable ERS

# ISE Basic setup (ISE 2.3)

Node: BRUSEENAC

Role: STANDALONE

Policy Service: Enable SXP Service

pxGrid: pxGrid

Enable PxGrd

ERS Settings

General: External RESTful Services (ERS) is enabled.

EERS Setting for Administration Node: Enable ERS for ReadWrite

CSRФ Check: USE CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)

Enable ERS



# Integration success

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

All Clients Web Clients Capabilities Live Log Settings Certificates

Total Pending Approval(0) ▾

<input type="checkbox"/> Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
<input type="checkbox"/> ise-mnt-bruisdnac		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate
<input type="checkbox"/> ise-admin-bruisdnac		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate
<input type="checkbox"/> ise-bridge-bruisdnac		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate
<input type="checkbox"/> ise-pubsub-bruisdnac		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Administrator	Certificate
<input type="checkbox"/> testuser123		Capabilities(0 Pub, 3 Sub)	Online (XMPP)	Session	Certificate
<input type="checkbox"/> iamdnac		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)	Session	Certificate
<input type="checkbox"/> testing123123		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)	Session	Certificate

Connected to pxGrid BRUISEDNAC.cisco.com

Test user created and online

Pxgrid up

# DNA Center, Basic setup



# Adding sites

A hierarchy of “sites”,  
“Buildings” and “floors”

The screenshot shows the Cisco DNA Center interface. At the top, there are tabs: DESIGN (highlighted in green), POLICY, PROVISION, and ASSURANCE. Below these are sub-tabs: Network Hierarchy (highlighted in green), Network Settings, Image Repository, Network Profiles, and Auth Template. On the left, a sidebar titled 'Global' shows 'No Children Found.' A search bar at the top left says 'Find Hierarchy'. In the center, a modal window titled 'Add Site' is open. It contains fields for 'Site Name\*' (with 'eg : San Jose' example) and 'Parent' (set to 'Global'). There are buttons for 'Cancel' and 'Add'. Below the modal is a link 'Or select a file' and options to 'Upload CSV' or 'Download Template'. To the right of the modal is a world map of the North Atlantic region, showing countries like Iceland, Norway, Sweden, Denmark, UK, Ireland, France, Spain, Portugal, Italy, and North Africa.



# Adding buildings

CISCO DNA CENTER

DESIGN POLICY PROVISION ASSURANCE

Network Hierarchy Network Settings Image Repository Network Profiles Auth Template

Find Hierarchy

Global No Children Found.

Add Site

Add Site

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

Site  Building

Building Name\* Pegasus

Parent Global

Address De Kleetlaan 7, Machelen, 1831 Vlaams E

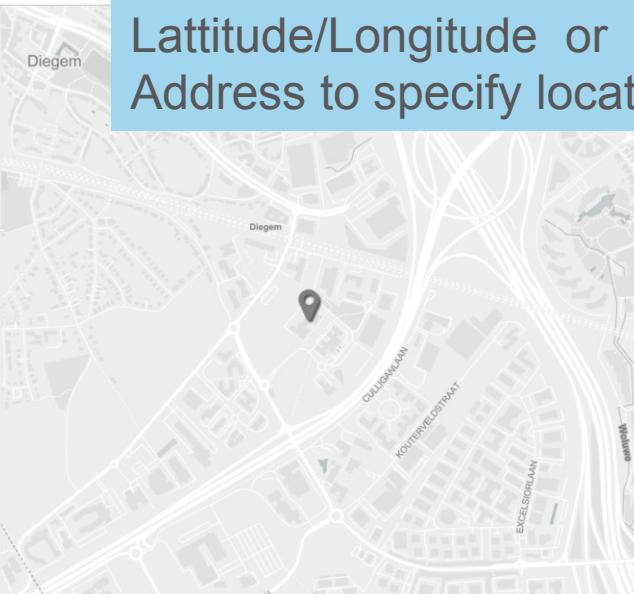
Latitude\* 50.887419 Longitude\* 4.447516

Cancel Add

Or select a file

Upload CSV Download Template

Lattitude/Longitude or Address to specify location



Diegem

Diegem

COLLEGELAAN

KOUTERVELSTRAAT

EXCELSIORLAAN

Willeme

# Defining network Servers

The screenshot shows the Cisco DNA Center interface for defining network servers. On the left, there's a sidebar with tabs for DESIGN, POLICY, PROVISION, and ASSURANCE. Under DESIGN, the Network Settings tab is selected, showing sections for DHCP Server, DNS Server, SYSLOG Server, and SNMP Server. A modal window titled "Add Servers" is open, containing checkboxes for AAA, Netflow Collector, and NTP, with "OK" and "Cancel" buttons. Below the sidebar, there's a main content area with tabs for DESIGN, POLICY, PROVISION, and ASSURANCE. The Network tab is selected, showing "Network Settings" and "Network Telemetry". A large blue callout box on the right states: "Under Network Settings/Network all servers for the Fabric devices are defined." The main content area also includes sections for Device Credentials, IP Address Pools, SP Profiles, and Wireless. It shows network properties like AAA, NTP, Syslog, Trap, and Netflow setup. There are tabs for "Network", "Client/Endpoint", and "Protocol". Under "Network", it shows "Servers" (ISE selected), "Protocol" (RADIUS selected), and "IP Address (Primary)" (10.48.91.220). Under "Client/Endpoint", it shows "Servers" (ISE selected), "Protocol" (RADIUS selected), and "IP Address (Primary)" (10.48.91.220). At the bottom, there are "Reset" and "Save" buttons.

Under Network Settings/Network all servers for the Fabric devices are defined.



# Device credentials

Network Settings    Image Repository    Network Profiles    Auth Template

Network    Device Credentials    IP Address Pools    SP Profiles    Wireless

**CLI Credentials**

Name / Description	Username	Password	Enable Password	Actions
No data to display				

**SNMP Credentials**

Name / Description	Read Community	Actions
No data to display		

**HTTP(S) Credentials**

Name / Description	Username	Password	Port	Reset	Save
HTTP(S) Read   <a href="#">HTTP(S) Write</a>					

Needs at least CLI credentials and snmp read community

# IP Pools

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes the Cisco DNA CENTER logo, DESIGN (selected), POLICY, and PROVISION tabs. Below the navigation is a search bar and a grid icon. The main left sidebar has 'Network Hierarchy' and 'Find Hierarchy' sections, followed by a 'Global' section with 'No Children Found.' A central panel displays 'IP Address Pools' with a table header 'Name'. A modal dialog box titled 'Add IP Pool' is open in the center. It contains fields for 'IP Pool Name \*' (with a red asterisk), 'IP Subnet \*' (with a red asterisk), 'CIDR Prefix' dropdown set to '/8 (255.0.0.0)', 'Gateway IP Address \*', 'DHCP Server(s)', and 'DNS Server(s)'. There is also an unchecked checkbox for 'Overlapping'. At the bottom of the dialog are 'Cancel' and 'Save' buttons. To the right of the dialog, there is a summary table with columns 'Free Count', 'Overlapping', and 'Actions', and a large blue 'Add IP Pool' button. A callout box in the bottom right corner states: 'IP Pools can be defined for Voice, Data Traffic, AP's. Or internal use in the fabric'.

IP Pools can be defined for Voice, Data Traffic, AP's. Or internal use in the fabric

# IP Pools

Network Settings

Image Repository

Network Profiles

Auth Template

Network

Device Credentials

IP Address Pools

SP Profiles

Wireless

und.

## IP Address Pools

 Add IP Pool

Name	IP Subnet Mask	Gateway	DHCP Server	DNS Server	Free Count	Overlapping	Actions
Data	192.168.1.0/24	192.168.1.254	10.254.255.58	10.48.91.202	256 of 256	No	<a href="#">Edit</a>   <a href="#">Delete</a>
NetPool	172.16.250.0/24	172.16.250.254			256 of 256	No	<a href="#">Edit</a>   <a href="#">Delete</a>
Voice	192.168.100.0/24	192.168.100.1	10.254.255.58	10.48.91.202	256 of 256	No	<a href="#">Edit</a>   <a href="#">Delete</a>

3 Pools defined, Data, Voice and Network pool.  
Other pools could be for Multicast, AP's

# Authentication Templates

The image shows the Cisco DNA Center interface. At the top, there are tabs for DESIGN, POLICY, PROVISION, and ASSURANCE. Below that, a navigation bar includes Network Hierarchy, Network Settings, Image Repository, Network Profiles, and Auth Template, with Auth Template being the active tab. A large blue banner in the center says "Templates can be ‘tuned’". On the left, a table lists authentication methods:

Name	Type
<a href="#">Open Authentication</a>	Open Authentication
<a href="#">No Authentication</a>	No Authentication
<a href="#">Closed Authentication</a>	Closed Authentication
<a href="#">Easy Connect</a>	Easy Connect
<a href="#">Wireless Authentication</a>	Wireless Authentication

At the bottom left, it says "show 10 entries" and "Showing 1 - 5 of 5". On the right, there is a configuration panel for "Easy Connect" with the following settings:

- First Authentication Order:
  - 802.1x followed by MAB
  - 802.1x
  - MAC Auth Bypass(MAB)
- 802.1x to MABFallback:  Second(s)
- Wake on LAN:  No
- Number of Hosts:  Count
- Downstream Flex AP / Switch

Below these settings are two expandable sections:

- Url Redirect Setting
- ISE Server Failure Setting

A "Close" button is at the bottom right.

**CISCO** and © 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential are located at the bottom.

# Discovery

The screenshot shows the Cisco DNA Center 'Discovery' interface. On the left, there's a sidebar with 'Discoveries' and a search bar. The main area is titled 'New Discovery' with a 'Discovery Name' field. Below it, under 'IP ADDRESS/RANGE', there are fields for 'Type' (set to 'CDP'), 'IP Address', 'Subnet Filters', 'CDP Level' (set to 16), and 'Preferred Management IP'. Under 'CREDENTIALS', there are sections for 'Add Credentials' (CLI, SNMPv2C READ, SNMPv2C WRITE, SNMP V3) and a note that says 'No credentials to display'. A 'GLOBAL' and 'JOB SPECIFIC' checkbox is also present.

Discovery based on  
IP range or using  
CDP

The screenshot shows a running discovery job named 'test' with a status of 'Complete' (12 devices). It includes sections for 'DISCOVERY DETAILS', 'CREDENTIALS', and 'HISTORY'. The history table shows one run completed today at 3:55 PM with a duration of 00:02:02.

Devices discovered and  
reachable

The screenshot shows a list of discovered devices. The columns include IP Address, Device Name, Status, ICMP, SNMP, CLI, HTTPS, and Netconf. Devices listed include FE2039.cisco.co.m, FE2037.cisco.co.m, FE2051.lab.cisco.com, FE2052.lab.cisco.com, FE2053.lab.cisco.com, FE2054.lab.cisco.com, FE2055.lab.cisco.com, FE2056.lab.cisco.com, Dist\_cat01.cisco.com, Dist\_cat02.cisco.com, Dist\_cat03.cisco.com, and 3650\_XS.cisco.com. Most devices show a green checkmark in all columns, indicating they are successfully discovered and reachable.

# Defining a Virtual Network

DNA CENTER DESIGN POLICY PROVISION ASSURANCE

Dashboard Virtual Network Policy Administration Contracts Registry

Find Virtual Network +

Create or Modify Virtual Network by selecting Available Scalable Groups.

New Virtual Network

DEFAULT\_VN (16)

INFRA\_VN (0)

Virtual Network Name\* BrusselsLab

Available Scalable Groups

Find Scalable Group Show Unselected ▾

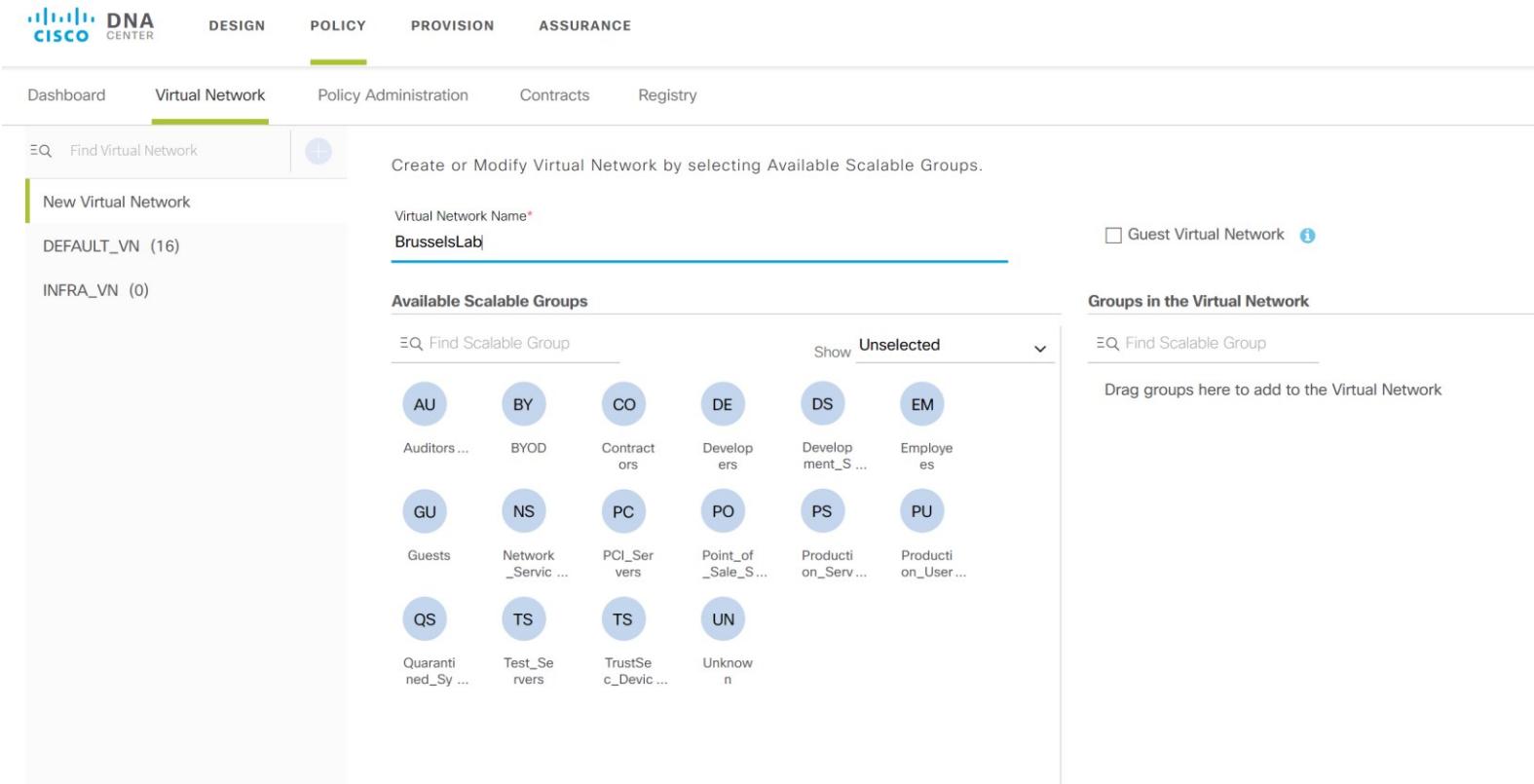
AU	BY	CO	DE	DS	EM
Auditors ...	BYOD	Contract ors	Develop ers	Develop ment_S ...	Employe es
GU	NS	PC	PO	PS	PU
Guests	Network _Servic ...	PCI_Ser vers	Point_of _Sale_S ...	Producti on_Serv ...	Producti on_User ...
QS	TS	TS	UN		
Quaranti ned_Sy ...	Test_Se rvers	TrustSe c_Devic ...	Unknown		

Guest Virtual Network ⓘ

Groups in the Virtual Network

Find Scalable Group

Drag groups here to add to the Virtual Network



# Assigning Groups to the VN

Dashboard   Virtual Network   Policy Administration   Contracts   Registry

Find Virtual Network  

Create or Modify Virtual Network by selecting Available Scalable Groups.

DEFAULT\_VN (12)

INFRA\_VN (0)

BrusselsLab (4)

Virtual Network Name\*  
BrusselsLab

Guest Virtual Network i

**Available Scalable Groups**

Find Scalable Group

Show **Unselected**

AU	BY	CO	DS	GU	NS
Auditors ...	BYOD	Contract ors	Development_S ...	Guests	Network _Servic ...
PC	PO	QS	TS	TS	UN
PCI_Ser vers	Point_of _Sale_S ...	Quaranti ned_Sy ...	Test_Se rvers	TrustSe c_Devic ...	Unknown

**Groups in the Virtual Network**

Find Scalable Group

DE	EM	PS	PU
Develop ers	Employe es	Producti on_Serv ...	Producti on_User ...

Scalable groups are coming from ISE Integration

# Defining Contracts

Dashboard   Virtual Network   Policy Administration   Contracts   Registry

Policy Administration

Group-Based Access Control (Fabric)   IP-Based Access Control (Non-Fabric)   Traffic Copy Policies

Create Policy by selecting Source, Destination, and applying a Contract

Policy Name\*  
E2D      Description (Optional)

Contract\*  
deny      Add Contract

Enable Policy    Enable Bi-directional i

Available Scalable Groups

Find

Source Scalable Groups	Destination Scalable Groups
EM Employees	DE Developers
AU Auditors ...	BY BYOD
CO Contractors	PO Point_of_Sale_S...
DS Development_S...	PS Production_Serv...
GU Guests	PC PCI_Servers
NS Network_Servic...	PU Producti_on_User...
QS Quarantine_Sy...	TS Test_Servers
TS TrustSe_c_Devic...	UN Unknown

Source Scalable Groups

EM  
Employees

Destination Scalable Groups

DE  
Developers

Who can talk to who and who not

# Contract pushed to ISE

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, Work Centers, Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, PassivelD, Overview, Components, TrustSec Policy, Policy Sets, SXP, Troubleshoot, Reports, and Settings.

The main content area displays a "Production Matrix" titled "Egress Policy". The matrix has "Source" and "Destination" columns. The sources listed are Auditors (9/0009), BYOD (15/000F), Contractors (5/0005), Developers (8/0008), Development\_Ser... (12/000C), Employees (4/0004), Guests (6/0006), Network\_Service... (3/0003), PCI Servers (14/000E), and Point\_of\_Sale\_S... (10/000A). The destinations listed are the same as the sources. A callout box highlights a cell in the matrix for the "Employees" source and "Development\_Ser..." destination, which contains the text "Deny IP" with a checked checkbox icon.

Contract created on DNAC gets pushed to ISE

Source	Destination	Value
Auditors 9/0009	BYOD 15/000F	
BYOD 15/000F	Contractors 5/0005	
Contractors 5/0005	Developers 8/0008	
Developers 8/0008	Development_Ser... 12/000C	
Development_Ser... 12/000C	Employees 4/0004	Deny IP
Employees 4/0004	Guests 6/0006	Deny IP
Guests 6/0006	Network_Service... 3/0003	
Network_Service... 3/0003	PCI Servers 14/000E	
PCI Servers 14/000E	Point_of_Sale_S... 10/000A	

# Building a Fabric



# Provisioning

Devices need to be assigned to a site and provisioned before they can be in a fabric

The screenshot shows the Cisco DNA Center interface, specifically the Provisioning section. At the top, there are tabs for DESIGN, POLICY, PROVISION (which is selected), and ASSURANCE. Below that, a secondary navigation bar has 'Devices' (selected) and 'Fabric'. The main area is titled 'Device Inventory' with a 'LAN Automation' button. It displays 'Inventory (12)' and 'Unclaimed Devices (0)'. A 'Network Telemetry' button is also present. The main table lists devices with columns: Device Name, Assign Device to Site, IP Address, Site, Serial Number, Uptime, OS Version, OS Image, Sync Status, and a delete icon. The first two rows have checkboxes checked under 'Assign Device to Site'.

Device Name	Assign Device to Site	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	
FE2053.lab.cisco.com	Provision Update OS Image	Hubs 10.254.255.53	FCW2117D02T		34 days, 6:22:30.98	16.6.2	packages.conf Tag Golden	Managed	
FE2052.lab.cisco.com	Delete Device	Hubs 10.254.255.52	FCW2117C01F		32 days, 15:27:16.02	16.6.2	cat3k_caa-un... Tag Golden	Managed	
FE2051.lab.cisco.com	Switches and Hubs 10.254.255.51		FCW2117C01M		40 days, 13:23:06.15	16.6.1s	packages.conf Tag Golden	Managed	
FE2050.lab.cisco.com	Switches and Hubs 10.254.255.50		FCW2117D010		28 days, 18:41:48.83	16.6.2	packages.conf Tag Golden	Managed	
FE2037.cisco.com	Switches and Hubs 10.254.255.37		FCW2123L09B, FCW2123L0NC		31 days, 19:33:02.21	16.6.2	packages.conf Tag Golden	Managed	
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

**CISCO DNA CENTER**

# Assigning it to a Site

The screenshot shows the Cisco DNA Center interface under the 'PROVISION' tab. The 'Devices' tab is selected. A callout box in the top right corner contains the text: 'First check “apply to all” then choose the site'.

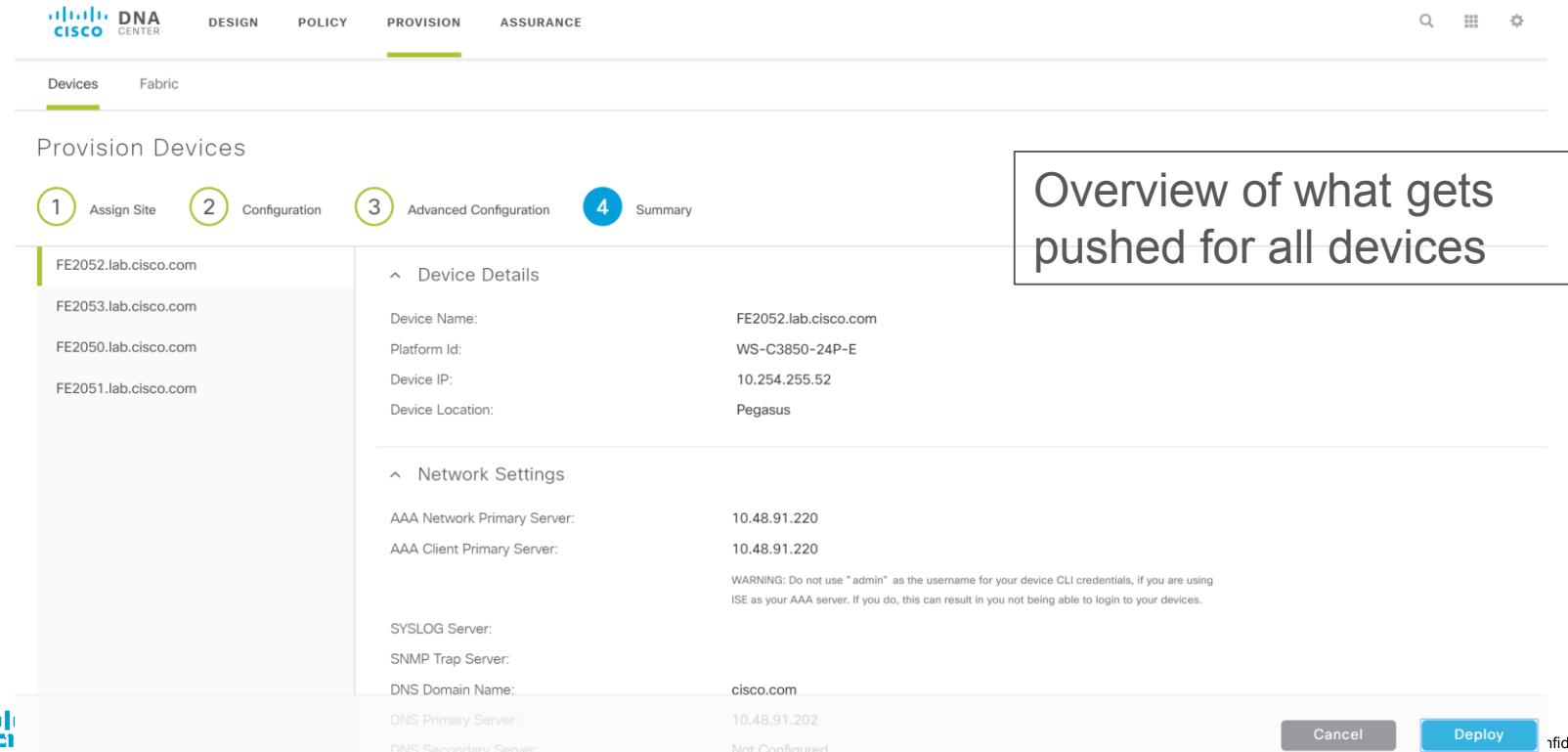
**Provision Devices**

- 1 Assign Site
- 2 Configuration
- 3 Advanced Configuration
- 4 Summary

Serial Number	Devices	Choose a site
FCW2117D02T	FE2053.lab.cisco.com	Global/Pegasus <input checked="" type="checkbox"/> Apply to All
FCW2117C01F	FE2052.lab.cisco.com	Global/Pegasus
FCW2117C01M	FE2051.lab.cisco.com	Global/Pegasus
FCW2117D010	FE2050.lab.cisco.com	Global/Pegasus



# Deploy Provisioning



The screenshot shows the Cisco DNA Center interface with the 'Provision' tab selected. The main area displays a table of devices being provisioned, with the first device's details expanded. A callout box highlights the 'Summary' step, which is part of a four-step process: Assign Site, Configuration, Advanced Configuration, and Summary.

**Provision Devices**

1 Assign Site    2 Configuration    3 Advanced Configuration    4 Summary

Device	Details
FE2052.lab.cisco.com	<p>Device Details</p> <p>Device Name: FE2052.lab.cisco.com</p> <p>Platform Id: WS-C3850-24P-E</p> <p>Device IP: 10.254.255.52</p> <p>Device Location: Pegasus</p>
FE2053.lab.cisco.com	<p>Network Settings</p> <p>AAA Network Primary Server: 10.48.91.220</p> <p>AAA Client Primary Server: 10.48.91.220</p> <p>SYSLOG Server:</p> <p>SNMP Trap Server:</p> <p>DNS Domain Name: cisco.com</p>
FE2050.lab.cisco.com	
FE2051.lab.cisco.com	

**Overview of what gets pushed for all devices**

**Cancel** **Deploy** Confidential 39

# Deployed successfully

Devices      Fabric

## Device Inventory

LAN Automation

LAN Auto Status



Inventory (12)      Unclaimed Devices (0)

Network Telemetry

Upgrade Status

Refresh

Filter

Actions

<input type="checkbox"/>	Device Name	Device Type	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status
<input type="checkbox"/>	FE2053.cisco.com	Switches and Hubs	10.254.255.53	...lobal/Pegasus	FCW2117D02T	34 days, 6:32:53.02	16.6.2	packages.conf Tag Golden	Managed	Dec 12 2017 11:54:10	Success
<input type="checkbox"/>	FE2052.lab.cisco.com	Switches and Hubs	10.254.255.52	...lobal/Pegasus	FCW2117C01F	32 days, 15:27:16.02	16.6.2	cat3k_caa-un... Tag Golden	In Progress	Dec 12 2017 11:54:14	Success
<input type="checkbox"/>	FE2051.cisco.com	Switches and Hubs	10.254.255.51	...lobal/Pegasus	FCW2117C01M	40 days, 13:42:37.12	16.6.1s	packages.conf Tag Golden	Managed	Dec 12 2017 11:54:06	Success
<input type="checkbox"/>	FE2050.cisco.com	Switches and Hubs	10.254.255.50	...lobal/Pegasus	FCW2117D010	28 days, 19:01:19.57	16.6.2	packages.conf Tag Golden	Managed	Dec 12 2017 11:54:06	Success



# Adding a new Fabric

The screenshot shows the Cisco DNA Center web interface. At the top, there's a navigation bar with tabs: DESIGN, POLICY, PROVISION (which is underlined in green), and ASSURANCE. Below the navigation bar, there are two main categories: Devices and Fabric, with Fabric being the active category. On the left, a sidebar titled "Create and Manage Fabric" lists a single item: "Default LAN Fabric" (Campus). A modal window titled "Create New Fabric" is displayed on the right. Inside the modal, there are two radio buttons: "Campus" (selected) and "WAN". Below the radio buttons is a text input field containing the value "Brussels". At the bottom right of the modal are two buttons: "Cancel" and a blue "Add" button.

# The Fabric view (pictogram)

CISCO DNA CENTER DESIGN POLICY PROVISION ASSURANCE

Devices Fabric

Brussels

Lab topology

Select Devices Host Onboarding

1 Select device to be added to the fabric  
2 Select Control Plane Node  
3 Select Border Node

Validation Cancel Save

Search Topology

Select Devices to add, remove or identify.  
Shift + Click to select multiple.

The diagram illustrates a network fabric topology. At the top, four nodes are labeled: FE2035.cisco.com, FE2051.cisco.com, FE2037.cisco.com, and Dist\_9k.cisco.com. Below them, another row of nodes includes FE2033.cisco.com, FE2053.cisco.com, FE2052.cisco.com (which has a blue selection bar), FE2050.cisco.com, Dist3k\_2.lab.cisco..., Dist3k\_1.lab.cisco..., and 3850\_XS.cisco. A large number of grey arrows indicate bidirectional connections between these nodes, forming a complex mesh. A blue rectangular box labeled "Lab topology" is positioned above the nodes. To the left, a search bar says "Search Topology" and instructions say "Select Devices to add, remove or identify. Shift + Click to select multiple.". On the right, there are icons for zooming in and out, and a blue "Save" button.

# Fabric, List view

Devices can be listed too

Devices      Fabric

Brussels

Select Devices    Host Onboarding

1                  2                  3

Select device to be added to the fabric      Select Control Plane Node      Select Border Node

Cancel      Save

Filter

Name ▾      Type      IP Address      Fabric Status      Specialty Devices      Role      Device Status

FE80::21D:45FF:FE85:BC1E      wired      FE80::21D:45FF:FE85:BC1E      N/A      HOST

FE2053.cisco.com      Cisco Catalyst38xx stack-able ethernet switch      10.254.255.53      In this FD       Control Plane       Border Node      ACCESS

FE2052.cisco.com      Cisco Catalyst38xx stack-able ethernet switch      10.254.255.52      In this FD       Control Plane       Border Node      ACCESS

FE2051.cisco.com      Cisco Catalyst38xx stack-able ethernet switch      10.254.255.51      In this FD       Control Plane       Border Node      DISTRIBUTION

FE2050.cisco.com      Cisco Catalyst38xx stack-able ethernet switch      10.254.255.50      In this FD       Control Plane       Border Node      ACCESS

Checking a device adds it to the fabric. Optionally add a speciality

Name	Type	IP Address	Fabric Status	Specialty Devices	Role	Device Status
FE80::21D:45FF:FE85:BC1E	wired	FE80::21D:45FF:FE85:BC1E	N/A		HOST	
FE2053.cisco.com	Cisco Catalyst38xx stack-able ethernet switch	10.254.255.53	In this FD	<input type="checkbox"/> Control Plane <input type="checkbox"/> Border Node	ACCESS	
FE2052.cisco.com	Cisco Catalyst38xx stack-able ethernet switch	10.254.255.52	In this FD	<input type="checkbox"/> Control Plane <input type="checkbox"/> Border Node	ACCESS	
FE2051.cisco.com	Cisco Catalyst38xx stack-able ethernet switch	10.254.255.51	In this FD	<input type="checkbox"/> Control Plane <input type="checkbox"/> Border Node	DISTRIBUTION	
FE2050.cisco.com	Cisco Catalyst38xx stack-able ethernet switch	10.254.255.50	In this FD	<input checked="" type="checkbox"/> Control Plane <input type="checkbox"/> Border Node	ACCESS	



# Linking Pool to Virtual Network

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes the Cisco DNA Center logo, DESIGN, POLICY, PROVISION (which is highlighted in green), and ASSURANCE. Below the navigation, there are tabs for Devices and Fabric, with Fabric selected. The main area is titled "Edit Virtual Network: BrusselsLab". On the left, there's a sidebar for "Brussels" with sections for "Select Devices" (Host Onboarding is selected), "Select Authentication template" (Closed Authentication is selected), and "Virtual Networks" (INFRA\_VN, BrusselsLab, and DEFAULT are listed). The main content area displays a table for IP Pool Name, Traffic Type, Address Pool, and Layer-2 Extension. The table has three entries: Data (Traffic Type: Choose Traffic, Address Pool: 192.168.1.0/24, Layer-2 Extension: Off), NetPool (Traffic Type: Choose Traffic, Address Pool: 172.16.250.0/24, Layer-2 Extension: Off), and Voice (Traffic Type: Choose Traffic, Address Pool: 192.168.100.0/24, Layer-2 Extension: Off). At the bottom, there are buttons for Cancel and Update, and a feedback link.

IP Pool Name	Traffic Type	Address Pool	Layer-2 Extension
Data	Choose Traffic	192.168.1.0/24	Off
NetPool	Choose Traffic	172.16.250.0/24	Off
Voice	Choose Traffic	192.168.100.0/24	Off

# Host Onboarding

The screenshot shows the Cisco DNA Center interface under the 'PROVISION' tab. The main table displays host information:

SSID Name	Type	Security	Traffic Type
No data to display			

Below the table, there's a 'Select Port Assignment' section with three hosts listed: FE2051.cisco.com, FE2053.cisco.com, and FE2052.cisco.com. For each host, there are two port selection panes. A blue callout box points to the second pane of the first host, which shows a dropdown menu for 'Groups' containing 'Employees', 'Developers', 'Employees', 'Production\_Users', 'Production\_Servers', and 'Employees'. The 'Employees' option is selected. The port 'GigabitEthernet1/0/21' is checked and highlighted in blue, indicating it has been assigned to the 'Employees' group.

The groups that were added to the VN show up

# Quick check Device Side setup

```
interface GigabitEthernet1/0/21
switchport access vlan 1021
switchport mode access
device-tracking attach-policy IPDT_MAX_10
load-interval 30
cts manual
policy static sgt 8
no propagate sgt
spanning-tree portfast
end
```

```
interface Vlan1021
description Configured from apic-em
mac-address 0000.0c9f.f45c
vrf forwarding BrusselsLab
ip address 192.168.1.254 255.255.255.0
ip helper-address 10.254.255.58
no ip redirects
ip local-proxy-arp
ip route-cache same-interface
no lisp mobility liveness test
lisp mobility 192_168_1_0-BrusselsLab
end
```

# AAA config pushed to device

```
FE2051#sh run | sec aaa
aaa new-model
aaa group server radius dnac-group
  server name dnac-radius_10.48.91.220
  ip radius source-interface Loopback0
aaa authentication login default group dnac-group local
aaa authentication enable default enable
aaa authentication dot1x default group dnac-group
aaa authorization exec default group dnac-group local
aaa authorization network default group dnac-group
aaa authorization network dnac-cts-list group dnac-group
aaa accounting dot1x default start-stop group dnac-group
aaa server radius dynamic-author
  client 10.48.91.220 server-key cisco123
```



# SGT policies download

```
FE2051#sh cts policy sgt 8
```

```
CTS SGT Policy
```

```
=====
```

```
RBACL Monitor All : FALSE
```

```
RBACL IP Version Supported: IPv4
```

```
SGT: 8-01:Developers
```

```
SGT Policy Flag: 0x41400001
```

```
RBACL Source List:
```

**Source SGT: 4-01:Employees-0, Destination SGT: 8-01:Developers-0**

```
rbacl_type = 80
```

```
rbacl_index = 1
```

```
name = Deny IP-00
```

RBACL showing the contract earlier defined



# And ofcourse the LISP configuration

```
FE2051#sh running-config | sec router lisp
router lisp
locator-table default
locator-set rloc_775fbc22-8abb-4313-8fe8-0b2d78e179c8
IPv4-interface Loopback0 priority 10 weight 10
exit-locator-set
!
locator default-set rloc_775fbc22-8abb-4313-8fe8-0b2d78e179c8
service ipv4
encapsulation vxlan
map-cache-limit 25000
database-mapping limit dynamic 5000
itr map-resolver 10.254.255.50
etr map-server 10.254.255.50 key uci
etr map-server 10.254.255.50 proxy-reply
etr
sgt
proxy itr 10.254.255.51
exit-service-ipv4
.....
```

Only partially showing

