



# Cisco Secure Access and ISE integrations

Diego Barrantes Rivera

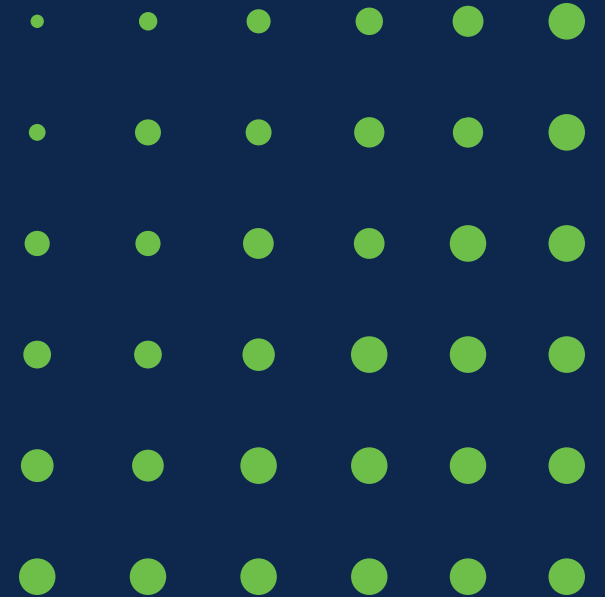
Customer Success Specialists

April 2025

# Agenda

- Secure Access and ISE use cases
- Secure Access with ISE as Radius and Posture
- Secure Access with ISE Context sharing
- Q&A

# Use Cases



# Who should use this integration?

You have a mature ISE deployment on your network

- Posture Assessment
- SGT Microsegmentation
- Radius Authentication for VPN

Easy conversion from on-prem VPN to VPNaaS

Interim step from legacy solutions to ZTNA per app microsegmentation

# Architecture Overview – Identity Service Engine

- Network Access Control (NAC) solution
- AAA for wired, wireless and VPN networks
- Available in appliances (SNS), virtualized and Cloud marketplaces
- **Trust Sec** allows for segmentation of the network using Security Group Tags (SGT) instead of VLAN/ACL segmentation.



## Policy Administration Node (PAN)

- Single plane of glass for ISE admin
- Replication hub for all database config changes



## Monitoring and Troubleshooting Node (MnT)

- Reporting and logging node
- Syslog collector from ISE Nodes



## Policy Services Node (PSN)

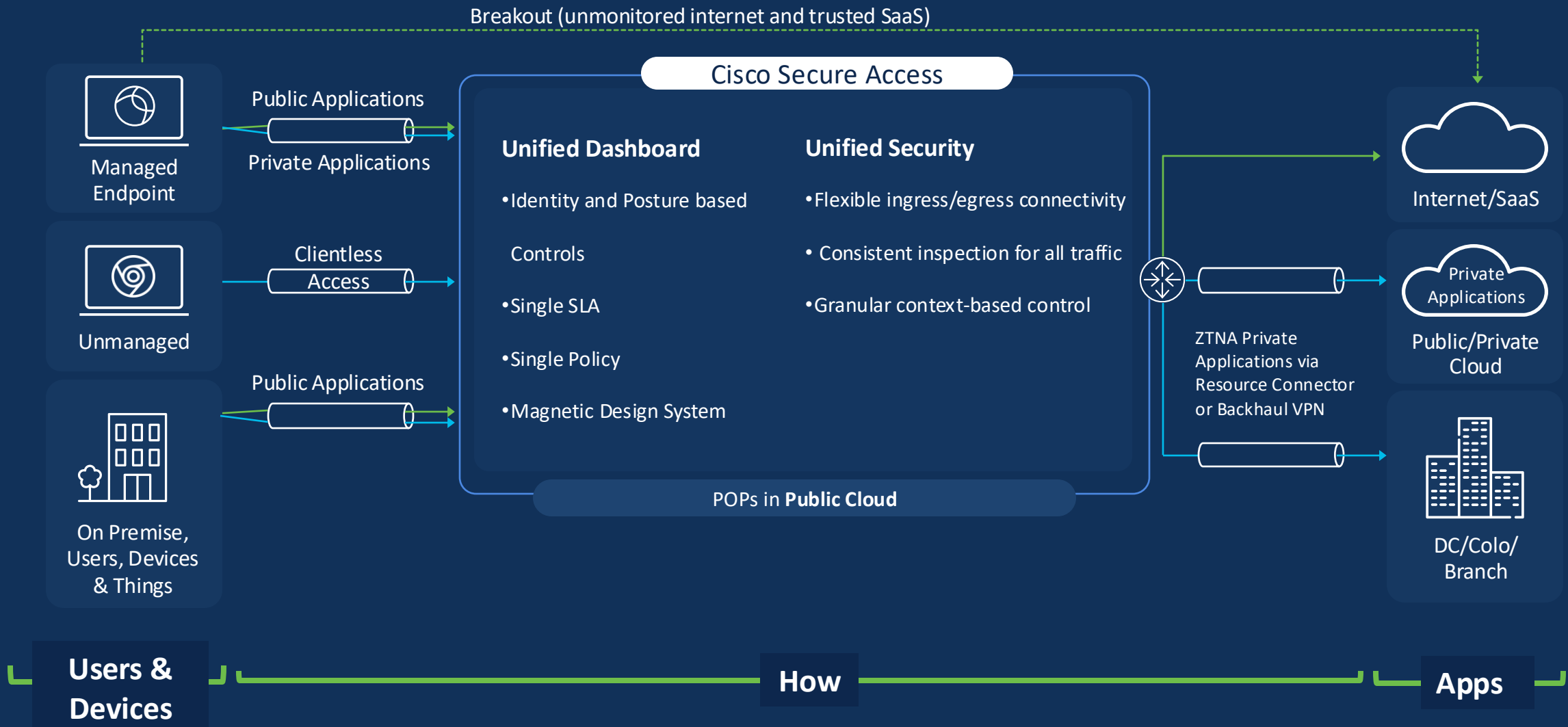
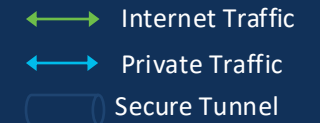
- Makes policy decisions
- RADIUS/TACACS+ Servers



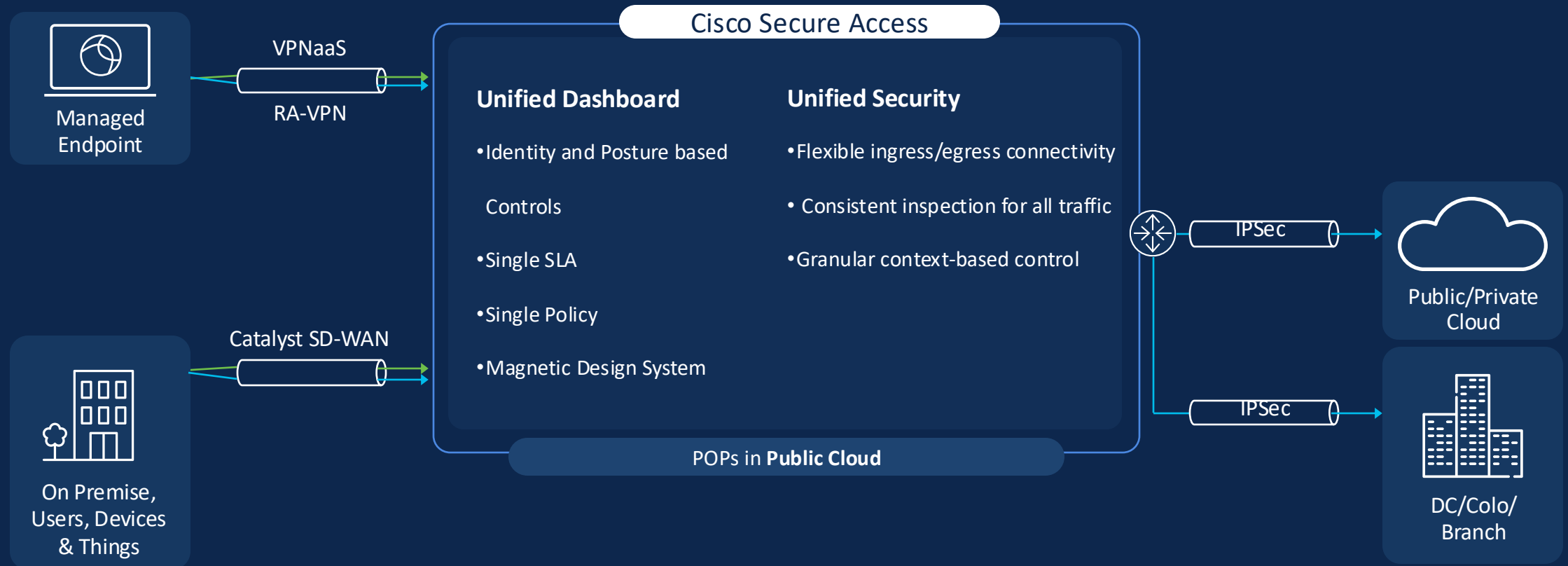
## pXGrid Controller

- Facilitates sharing of context

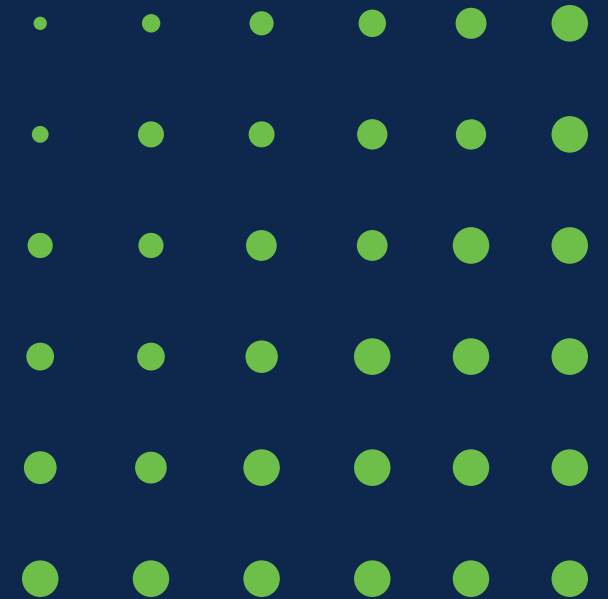
# Architecture Overview



# Architecture with ISE

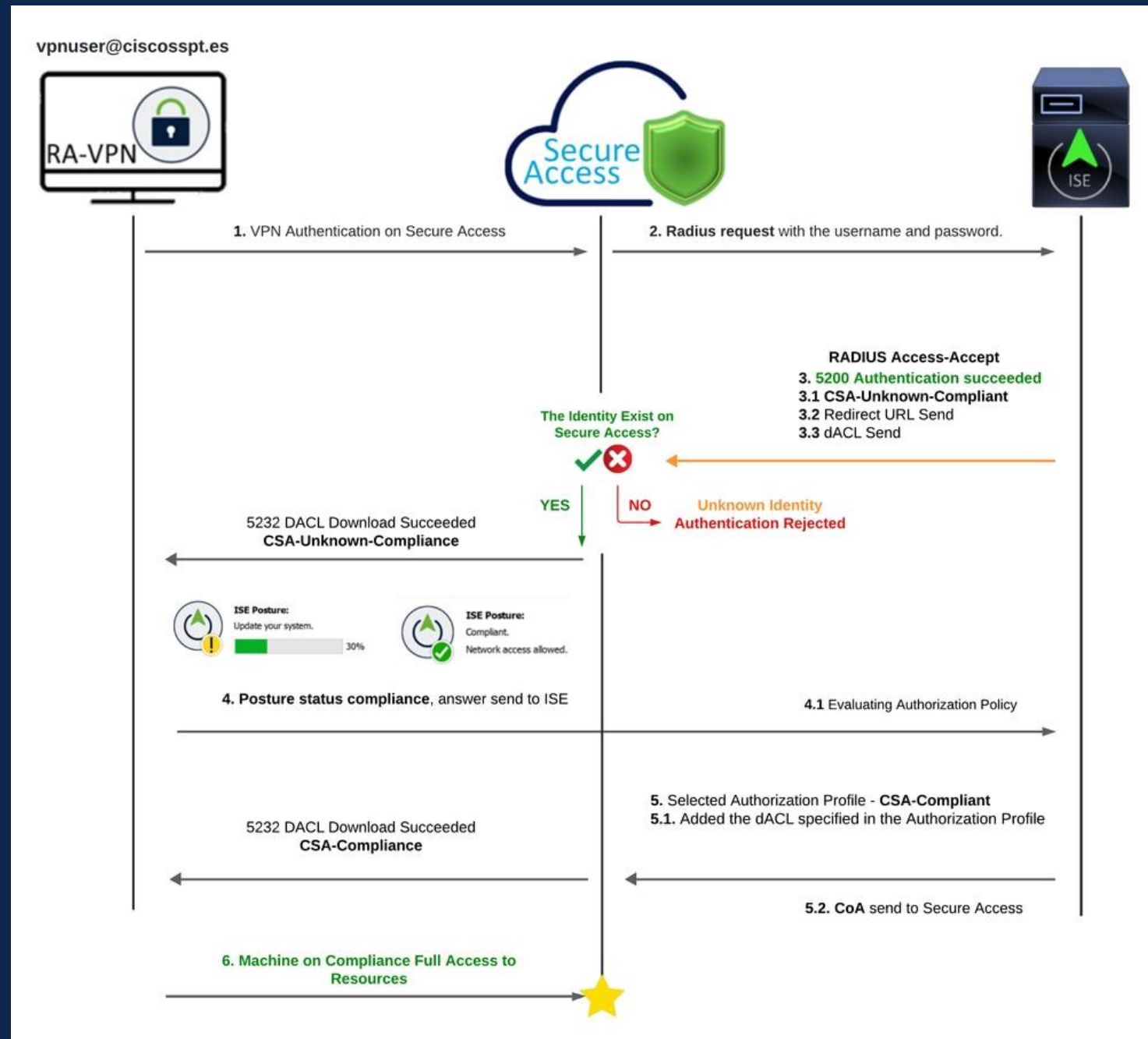


# Secure Access with ISE as Radius Server and Posture





- Leverages already existing posture policies  
Cisco Identity Services Engine (ISE) or 3<sup>rd</sup> Party RADIUS supported
- AAA or authorize only
- Up to 8 servers within a single server group
- Dynamic ACLs supported
- CoA support with Cisco ISE
- ISE posture supported



# Configuration Guidelines

Authentication Authorization Accounting

**General settings**  
Default Domain: ciscospt.es | DNS Server: Umbrella (208.67.222.222, 208.67.222.220) | Protocol: TLS / DTLS, IKEv2

**2 Authentication, Authorization, and Accounting**

3 Traffic Steering (Split Tunnel)

4 Cisco Secure Client Configuration

**Protocols**  
RADIUS

**Authenticate with CA certificates**  
Select to use CA certificates to authenticate this VPN profile.

**Map authentication groups to regions**  
Use defaults or customize groups to map to regions

Select one group for all regions + Group

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)

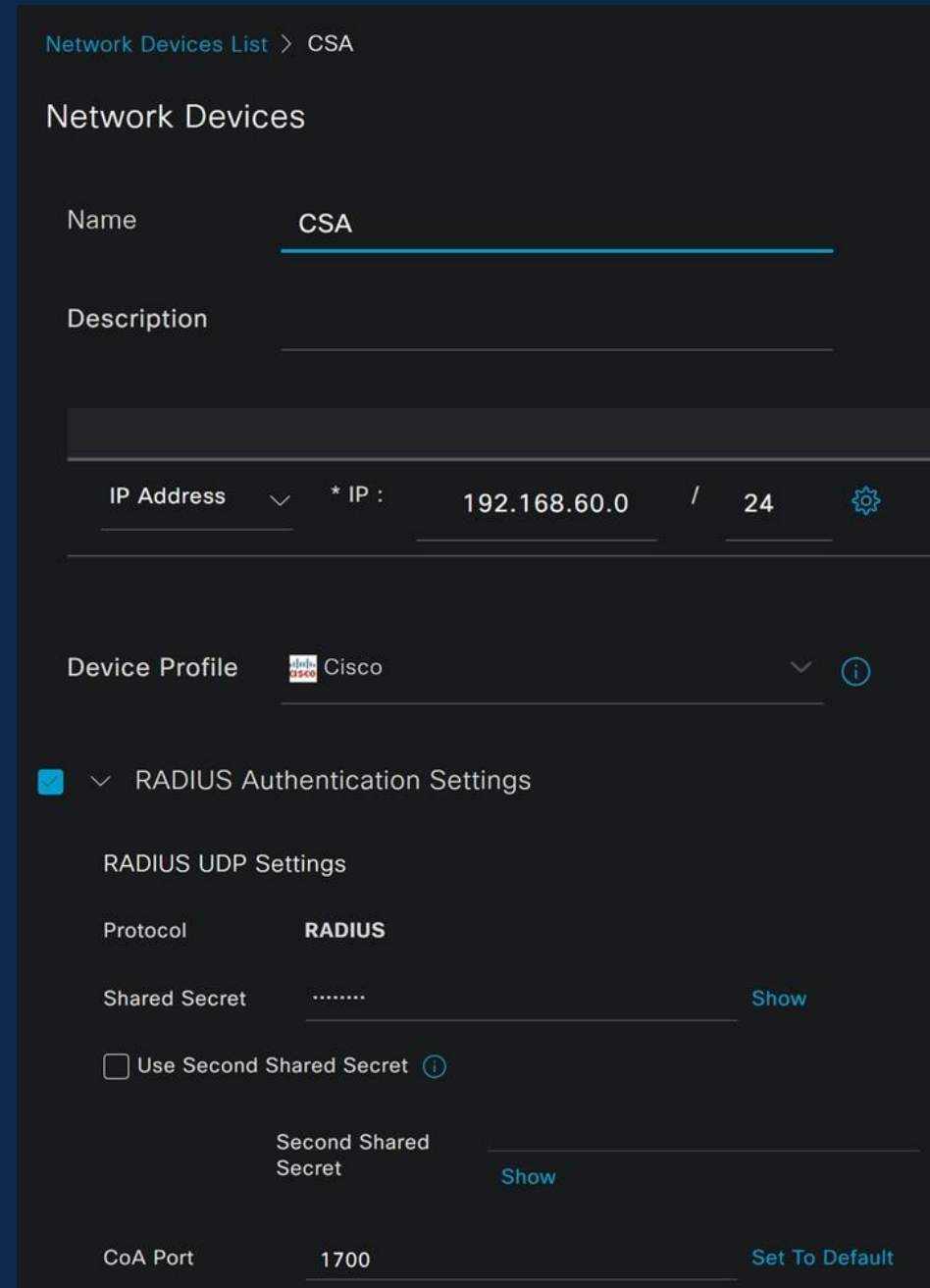
Cancel Back Next

EUROPE 1 ^

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	ISE_CSA

# Configuration Guidelines

- **Name:** Use a name to Identify Secure Access
- **IP Address:** Configure the **Management Interface** of the step IP Pool configuration
- **Device Profile:** Choose Cisco
  - **Radius Authentication Settings**
    - **Shared Secret:** Configure the same shared secret set up on the Secure Access Radius Group
    - **CoA Port:** Let it as default; 1700 is also used in Secure Access



## Secure Endpoint Installed

Cisco Secure Client

**AnyConnect VPN:**  
Ready to connect.  
ISE\_CSA - IKEv2 - Auto Select Nearest Location [v]

**Zero Trust Access:**  
Registration is required to access secure resources.

**ISE Posture:**  
System scan not required on current Wi-Fi.

**Secure Endpoint:**  
Connected.  
Flash Scan [v]

## Agent Scanning

Cisco Secure Client

**AnyConnect VPN:**  
Connected to ISE\_CSA - IKEv2 - Auto Select Nearest Location.  
ISE\_CSA - IKEv2 - Auto Select Nearest Location [v]

00:14:31 (3 Days 23 Hours Remaining) IPv4

**Zero Trust Access:**  
Registration is required to access secure resources.

**ISE Posture:**  
Scanning system ...  
10%

**Secure Endpoint:**  
Disconnected.  
Flash Scan [v]

## ISE Posture Successful validated

Cisco Secure Client

**AnyConnect VPN:**  
Connected to ISE\_CSA - IKEv2 - Auto Select Nearest Location.  
ISE\_CSA - IKEv2 - Auto Select Nearest Location [v]

00:00:26 (3 Days 23 Hours Remaining) IPv4

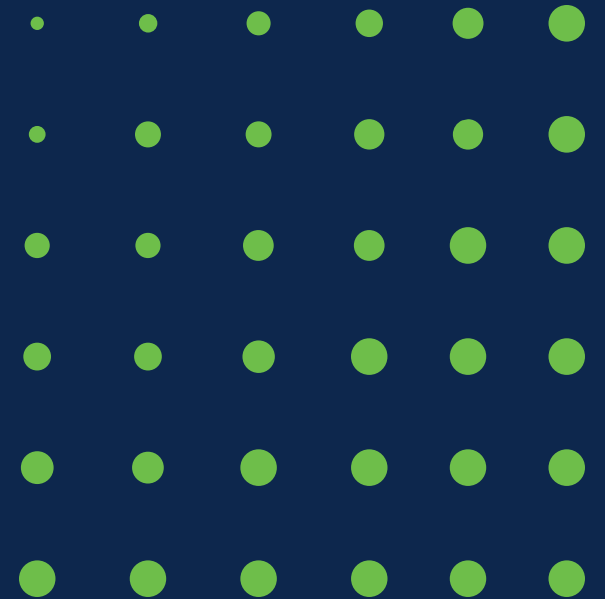
**Zero Trust Access:**  
Registration is required to access secure resources.

**ISE Posture:**  
Compliant.  
Network access allowed.

**Secure Endpoint:**  
Disconnected.  
Flash Scan [v]

# Secure Access with ISE

## Context sharing



# Rich Identity from Context

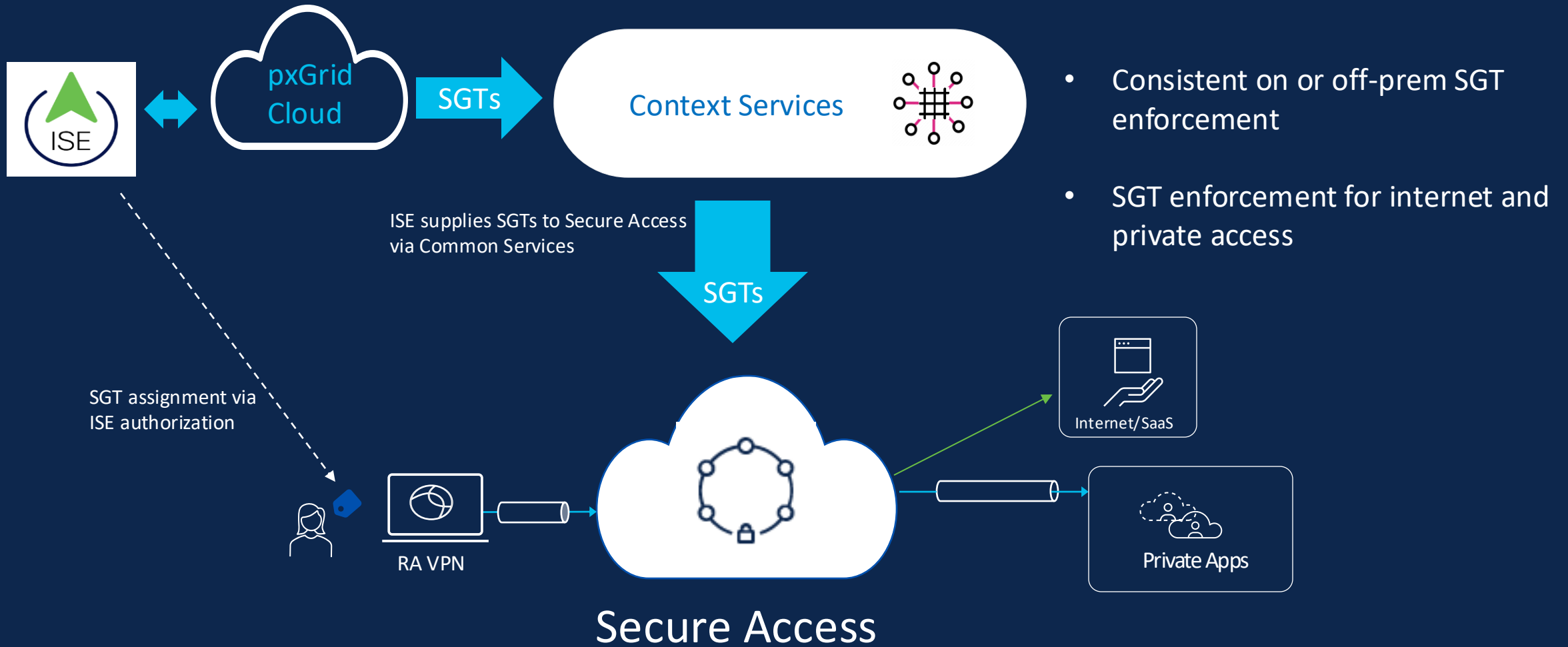




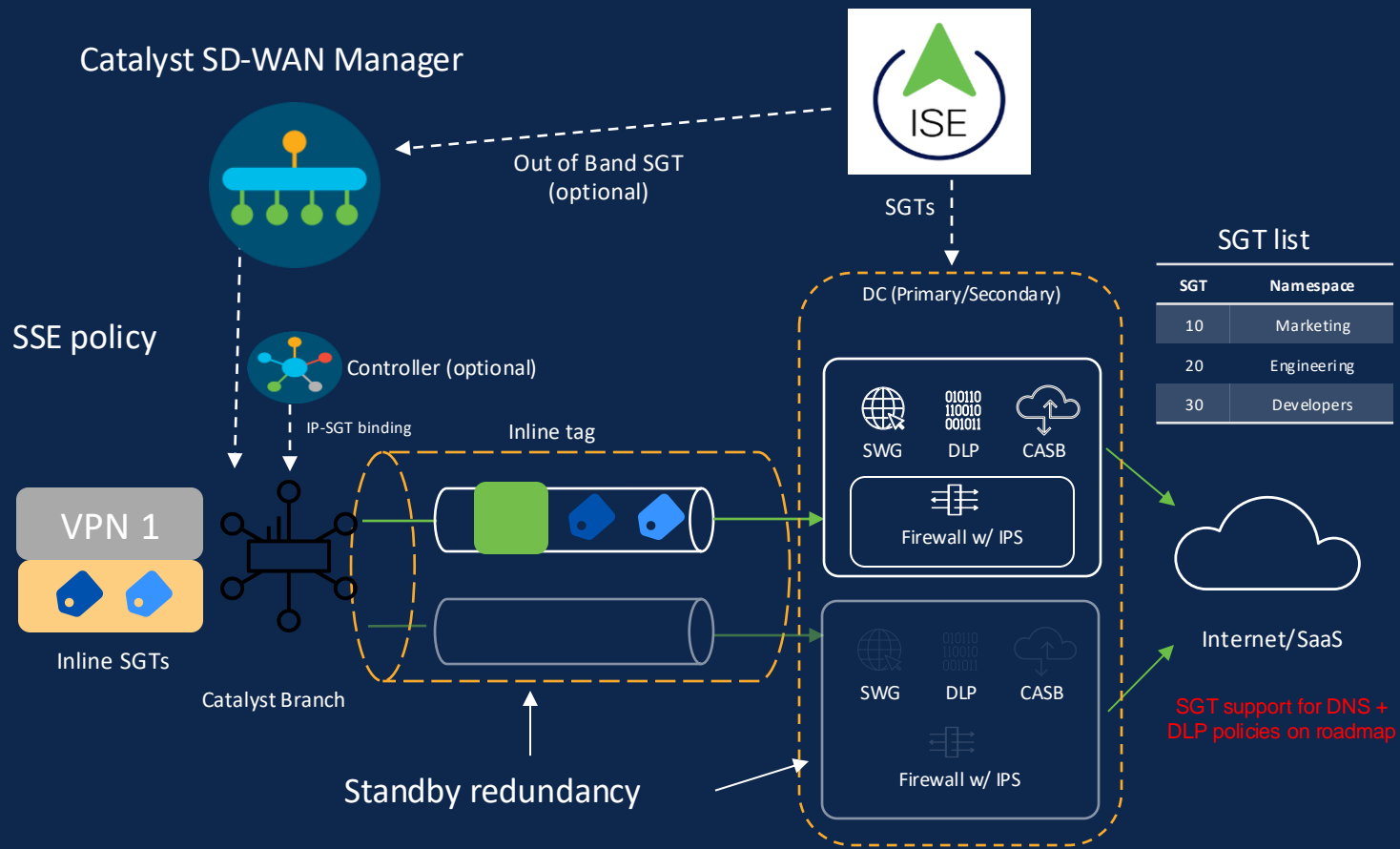


 <b>UNKNOWN</b>	<b>Poor context awareness</b>		<b>Rich context awareness</b>
	IP ADDRESS: 192.168.2.101	WHO	Bob (Employee)
	Unknown	WHAT	Apple iPad/iOS/11.0.1
	Unknown	WHEN	10:30 AM PST
	Unknown	WHERE	Floor-1, San Jose, Building 19
	Unknown	HOW	Wireless
	Unknown	APPS	Firefox, MS Word, AnyConnect
	Unknown	SPEC	Serial number, CPU, memory
<b>Without ISE</b>	<b>Access to any device/user</b> 	<b>RESULT</b>	<b>Authorized network access</b> 
			<b>KNOWN</b>
			<b>With ISE</b>

# Context Sharing: Extending Micro-segmentation (SGT) from VPNaaS



# Context Sharing: Extending Micro-segmentation (SGT) from branch



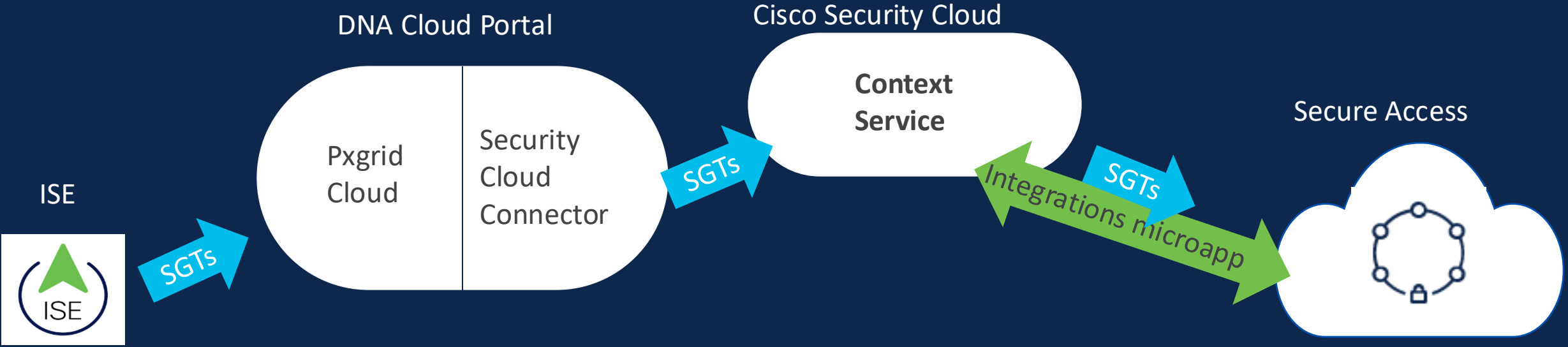
1. Cisco Secure Access establishes a secure connection with ISE context-services to consume SGTs
2. Learned SGTs can be leveraged to define access policies for branch accessing Internet/SaaS applications
3. In Catalyst Manager the Secure Service Edge policy group is configured to share SGT context in tunnels
4. Once tunnels are up, SGT identities, learned from enterprise are shared inline in the IPsec meta data header towards Cisco Secure Access.
5. Packets with SGT ID context are then subject to SSE policy match as source objects
6. SGT to IP Mapping can be learn both using inline or using OOB catalyst SD-WAN Manager ISE integration. Inline tag preferred over OOB.
7. SGT context sharing is optional
8. Both VPN and SGT can be shared together



# Policy: Source Object Precedence

- Highest to least precedence  
**User or group identity -> VPN id/SGT -> Network Tunnel Group**
- Logical **OR** for rules with multiple sources.
- If both VRF and SGT sent and rule has VRF and SGT as sources, rule matches on VRF as tie breaker
- Rule match is top-down like ACL

# Context sharing overview



# ISE – PxGrid Cloud configuration

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System configuration page. The interface includes a top navigation bar with the Cisco logo, 'Identity Services Engine', and 'Administration / System'. A right-hand notification bar shows 'Evaluation Mode 25 Days' and various utility icons. A secondary navigation bar contains tabs for Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The left sidebar lists navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Features. The main content area is titled 'Deployment' and features a 'Policy Service' section with a toggle switch turned on. Under 'Policy Service', several services are listed with checkboxes: 'Enable Session Services' (checked), 'Include Node in Node Group' (set to 'None'), 'Enable Profiling Service' (checked), 'Enable Threat Centric NAC Service' (unchecked), 'Enable SXP Service' (checked), 'Use Interface' (set to 'GigabitEthernet 0'), 'Enable Device Admin Service' (unchecked), and 'Enable Passive Identity Service' (unchecked). Below this, the 'pxGrid' section has a toggle switch turned on, with 'Enable pxGrid Cloud' checked. At the bottom right, there are 'Reset' and 'Save' buttons.

# ISE – PxGrid Cloud configuration

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes the Cisco ISE logo and the path "Administration > pxGrid Services". Below this, there are tabs for "Summary", "Client Management" (which is active), "Diagnostics", and "Settings". A left-hand sidebar contains a menu with items: "Clients", "Policy", "Groups", "Certificates", "pxGrid Cloud Connection" (highlighted), and "pxGrid Cloud Policy". The main content area is titled "pxGrid Cloud Connection" and contains the following text: "Perform bidirectional transactions between cloud services and Cisco ISE to automate network security through shared contextual and threat containment data." Below this, the status is shown as "Status Not enrolled". A diagram illustrates the connection between "Cisco ISE" (represented by a fingerprint icon) and "pxGrid Cloud" (represented by a cloud icon with a refresh symbol). A dotted line with a circled 'X' in the middle indicates a broken or unestablished connection. A blue "Setup connection" button is located at the bottom left of the main content area.

The screenshot shows a modal dialog box titled "Set up Connection" with a close button (X) in the top right corner. The dialog contains the following text: "Go to [pxGrid Cloud](#) and generate an Authentication Token. Paste the token provided by pxGrid Cloud below." Below this text is a text input field with the placeholder text "Enter token". At the bottom of the dialog, there are two buttons: "Cancel" and "Connect".

# ISE – PxGrid Cloud configuration

Catalyst Cloud Portal Applications and Products | Diego

Applications Products

**SUMMARY**

- Products Type (5)
  - Cisco DNA Center
  - Cisco ISE
  - Virtual Wireless C...
  - Cisco SDWAN Co...
  - Catalyst Dashboard
- Registration Status (5)
  - Registered
  - Pending Authoriza...
  - Suspended
  - Deleting
  - Delete Failed

Region: us-west-2

Products (1) **+ Register** Focus: Default

Search Table

Product Name	Registration Status
ISE	Pending Authorization

1 Record(s)

### Register Product

Host Name/IP

Product Name\*

Type\*

Description

dna.cisco.com

### OTP Generated

Next, paste the following OTP into product to authenticate the product.

```
eyJiYXNIX3VybCl6Imh0dHBzOi8vd3d3LmNpc2NvY29ubmVjdGRuYS5jb20iLCJvdHAI0ilzOGYzZmFINzY3ODc0M2I5Yjk5NTcwYTFINGQ2MTc4MDZmZDc5ZDRlYjRjZTRlNzE5YjZmMDk0M2IjOGM4MmWlxln0=
```

This OTP is valid only for 30 mins.

Close

# ISE – PxGrid Cloud configuration

The screenshot displays the Cisco ISE Administration console for 'pxGrid Services'. The navigation menu on the left includes 'Clients', 'Policy', 'Groups', 'Certificates', 'pxGrid Cloud Connection', and 'pxGrid Cloud Policy'. The main content area is titled 'pxGrid Cloud Connection' and contains the following elements:

- Status:** Connected: ise
- Diagram:** A visual representation of the connection between 'Cisco ISE' (represented by a fingerprint icon) and 'pxGrid Cloud' (represented by a cloud icon with a refresh symbol). A green checkmark in a circle is positioned in the center of a dotted line connecting the two entities, indicating a successful connection.
- Action:** A blue 'Disconnect' button is located below the diagram.

# ISE – PxGrid Cloud configuration

## Services consumables by Secure Access are:

- Trust Sec
- Echo Service

ERS API: Enabled

Open APIs: Enabled

Cisco ISE Administration - pxGrid Services

Summary Client Management Diagnostics Settings

Clients  
Policy  
Groups  
Certificates  
pxGrid Cloud Connection  
pxGrid Cloud Policy

### pxGrid Cloud Policy

You can create a general pxGrid Cloud policy for what is allowed or denied between your ISE deployment and the pxGrid Cloud service. The per partner authorization policy can be setup in the cloud portal.

pxGrid Services

You can use Cisco pxGrid to share the context-sensitive information from Cisco ISE session directory with other network systems such as ISE Eco system partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes like sharing tags and policy objects between Cisco ISE and third party vendors, and for other information exchanges.

Echo Service × TrustSec SXP × MDM ×  
TrustSec configuration × TrustSec ×  
Profiler configuration × ANC configuration ×  
Radius Failure × User Defined Network ×  
Session Directory ×

ERS APIs

Enable External RESTful Services (ERS) APIs Policy in pxGrid Cloud Policy.

Enabled ⓘ  
 Read Only  
 Read/Write

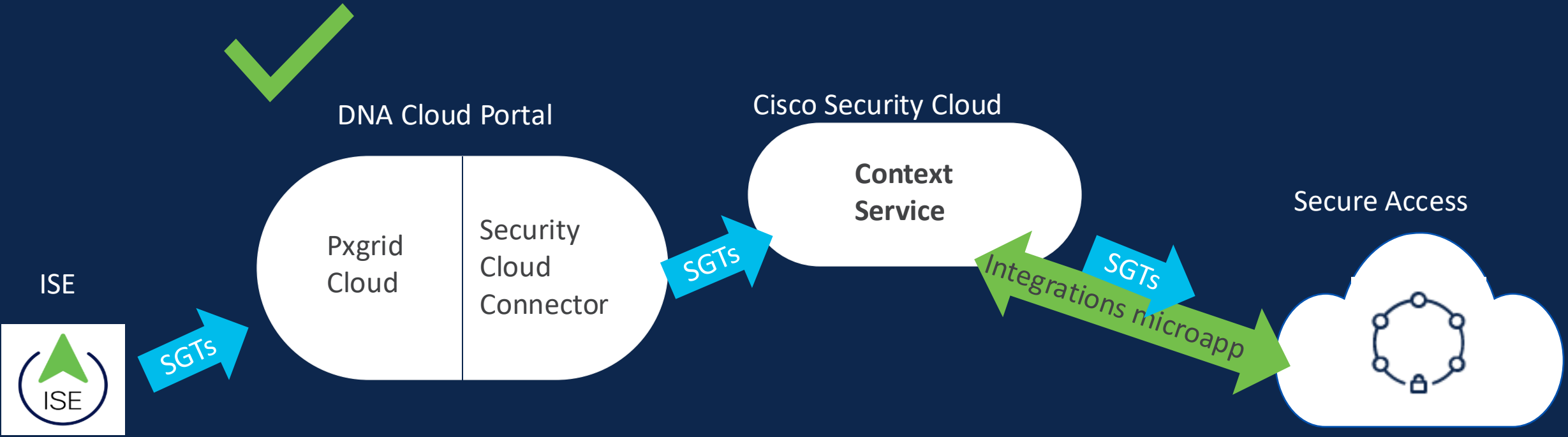
Open APIs

Enable Open APIs for pxGrid Cloud.

Enabled ⓘ  
 Read Only  
 Read/Write

Reset Save

# Context sharing overview





# PxGrid Cloud – Secure Access configuration

Catalyst Cloud Portal App 360 Diego

## Cisco Security Cloud

Status: Disconnected Account: diebarra@cisco.com [View all details](#)

SUMMARY

0 Activated

Products About

Activations (0)

Search Table

0 Selected **Add** More Actions

Name	Type	Region	Status
No data to display			

dna.cisco.com

Catalyst Cloud Portal Activate application on your product

Region us-west-2

## Authenticate your application

We have detected that your 'Cisco Security Cloud' is not yet authenticated. Please redeem the below OTP in your application interface to complete authentication.

1xMC3ydRoGur15IKGx7CsXFIRFq0SkBlzDHfXehsrflEYrKduZQA5Dqhov37zV5L

The OTP is valid only for 60 minutes.

In case you have just authenticated. Please click [here](#) to re-verify.

# PxGrid Cloud – Secure Access configuration

**Secure Access**

← Integrations

## Add an ISE Integration

To complete the integration of Cisco Identity Services Engine with Secure Access, add an ISE Connector. [Help](#)

### ISE Integration - Secure Access Connector

Configure Secure Access with your application connector's One-Time Password (OTP). This allows Secure Access to consume ISE data.

**Instance name \***

**OTP \* ⓘ**

**Activation Required:** To activate this integration, you must add it to the Cisco DNA Portal > Cisco Security Cloud.

<input type="checkbox"/>	Name	Date	Type	Status	
<input type="checkbox"/>	DMZISEconnector	Sep 19, 2024	pxgrid	Waiting for activation	...

As of: Sep 19, 2024, 11:20 AM

# PxGrid Cloud – Secure Access configuration

**Secure Access**

← Integrations

## Add an ISE Integration

To complete the integration of Cisco Identity Services Engine with Secure Access, add an ISE Connector. [Help](#)

### ISE Integration - Secure Access Connector

Configure Secure Access with your application connector's One-Time Password (OTP). This allows Secure Access to consume ISE data.

**Instance name \***

**OTP \* ⓘ**

**Activation Required:** To activate this integration, you must add it to the Cisco DNA Portal > Cisco Security Cloud.

<input type="checkbox"/>	Name	Date	Type	Status	
<input type="checkbox"/>	DMZISEconnector	Sep 19, 2024	pxgrid	Waiting for activation	...

As of: Sep 19, 2024, 11:20 AM

# PxGrid Cloud – Secure Access configuration

The screenshot shows the Cisco DNA Portal interface for Cisco Security Cloud. At the top, it displays 'DNA Portal' and 'App 360'. The main header is 'Cisco Security Cloud'. Below this, the status is 'Connected' with the account 'faylee@cisco.com' and a 'View all details' link. A 'SUMMARY' section shows '0 Activated' products. There are tabs for 'Products' and 'About'. A dropdown menu is set to 'Select Instance · DMZISEconnector'. Below that, it says 'Activations (0)'. A search bar is labeled 'Search Table'. At the bottom of this section, it shows '0 Selected', an 'Add' button, and a 'More Actions' dropdown.

## Choose Application Instance

Select which Application Instance you would like to connect your product to. Not seeing the Instance that you want? [Create a New One](#)

A card for the 'DMZISEconnector' application instance. It features a grid icon on the left and a small settings icon on the right.

## Type

## Choose your Product

You are subscribed to this application. Select the product for which you would like to activate your application. Not seeing the product you want? Click [here](#) to register. If you wish to manage products that are activated for this application click [here](#).

✓ All Cisco ISE

A card for the 'DMZISE' product. It features a green checkmark icon on the left and a green checkmark icon on the right. A mouse cursor is hovering over the card.

# PxGrid Cloud – Secure Access configuration

dna.cisco.com

Products About

Select Instance · DMZISEconnector ▾

### Activations (1)

Search Table

0 Selected [Add](#) [More Actions](#) ▾

<input type="checkbox"/>	Name ▲	Type	Region	Status
<input type="checkbox"/>	DMZISE	Cisco ISE	us-west-2	🟢 Activated

Secure Access

## Integrations

Secure Access supports the integration of various Cisco solutions, which allow you to enhance Secure Access network management and security. [Help](#) 📄

### Cisco Identity Services Engine – Security Group Tag (SGT) Integration

The integration of Secure Access with Identity Services Engine (ISE) streamlines the deployment of Security Group Tags (SGTs). This enables dynamic network segmentation and allows for more granulate access controls. [Help](#) 📄

<input type="checkbox"/>	Name	Date	Type	Status
<input type="checkbox"/>	<a href="#">DMZISEconnector</a>	Sep 19, 2024	pxgrid	🟢 Active

# On Cisco Secure Access: Monitor SGT

**Secure Access**

- Overview
- Experience Insights
- Connect
- Resources
  - Secure
  - Monitor
  - Admin
  - Workflows

## Overview

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and...

**Service disruption**  
Secure Access is currently experiencing service disruptions that may impact your region's connectivity. For more information, see...

### Sources and destinations

- Registered Networks**  
Point your networks to our servers
- Internal Networks**  
Define internal network segments to use as sources in access rules
- Roaming Devices**  
Mac and Windows
- Security Group Tags**  
View Service Group Tags (SGTs) when ISE integration is enabled
- SDWAN Service VPN IDs**  
View SDWAN Service VPN IDs when available from Catalyst SDWAN network tunnel groups

### Destinations

- Internet and SaaS Resources**  
Define destinations for internet access rules
- Private Resources**  
Define internal applications and other resources for use in access rules

### Settings

- AAA Servers**  
Manage authentication, authorization, and accounting (AAA) servers

### Security Group Tags

Security Group Tags (SGT) specify the privileges of a traffic source within a trusted network. When you enable an Identity Services Engine integration, SGTs become available for use in access rules. [Help](#)

Q Search 23 total As of: Aug 14, 2024, 02:13 PM

Name	Tag
ANY	65535
Auditors	9
BYOD	15
Contractors	5
Developers	8
Development_Servers	12
Doctors	18
Employees	4
Engineering	16
Finance	19

Rows per page: 10 < 1 2 3 >

# Secure Access: Activity Search

The screenshot displays the Cisco Secure Access Activity Search interface. The main content area shows a table of search results with columns for Request, Source, and Rule Identity. A search filter is applied for "Employees (VPN-10)". The table lists multiple entries for Rachel Nelson (rachel.nelson@sgtdemos.net) and machineuser 6 (machine@sse.com). A right-hand pane shows details for the selected rule, including a Destination List with "Deleted Destination List" and "http://www.ifconfig.io/". A red box highlights the "Source" field in the details pane, which contains "Employees (VPN-10)" and "Patients (SGT-20) (deleted)". Another red box highlights the "win11-sgt" rule identity in the table.

Handy for troubleshooting context sharing enablement issues



# Q&A





SECURE