CISCO
SECURE

Cisco Secure Access and ISE integrations

Diego Barrantes Rivera

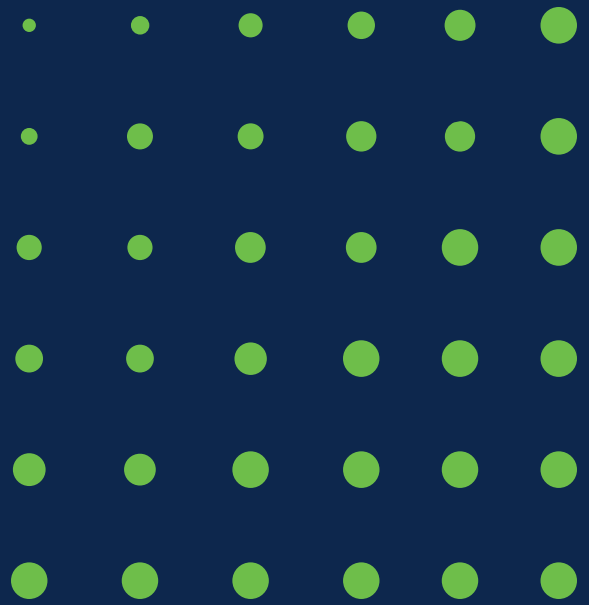
Customer Success Specialists

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 Assesment
- 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.

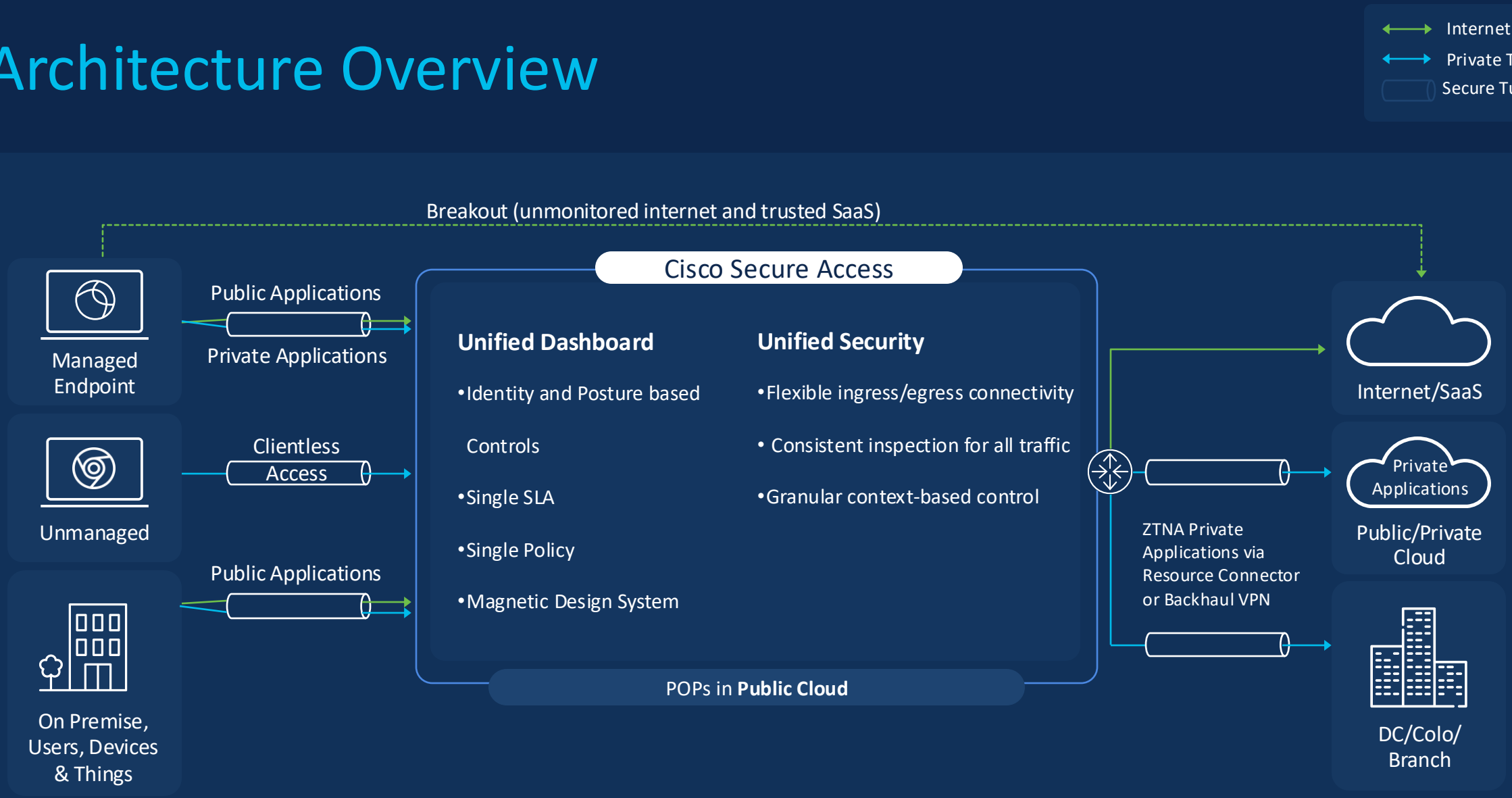
Policy Administration Node (PAN)
- Single plane of glass for ISE admin
- Replication hub for all database config changes

Monitoring and Troubleshooting Node (MnT)
- Reporting and logging node
- Syslog collector from ISE Nodes

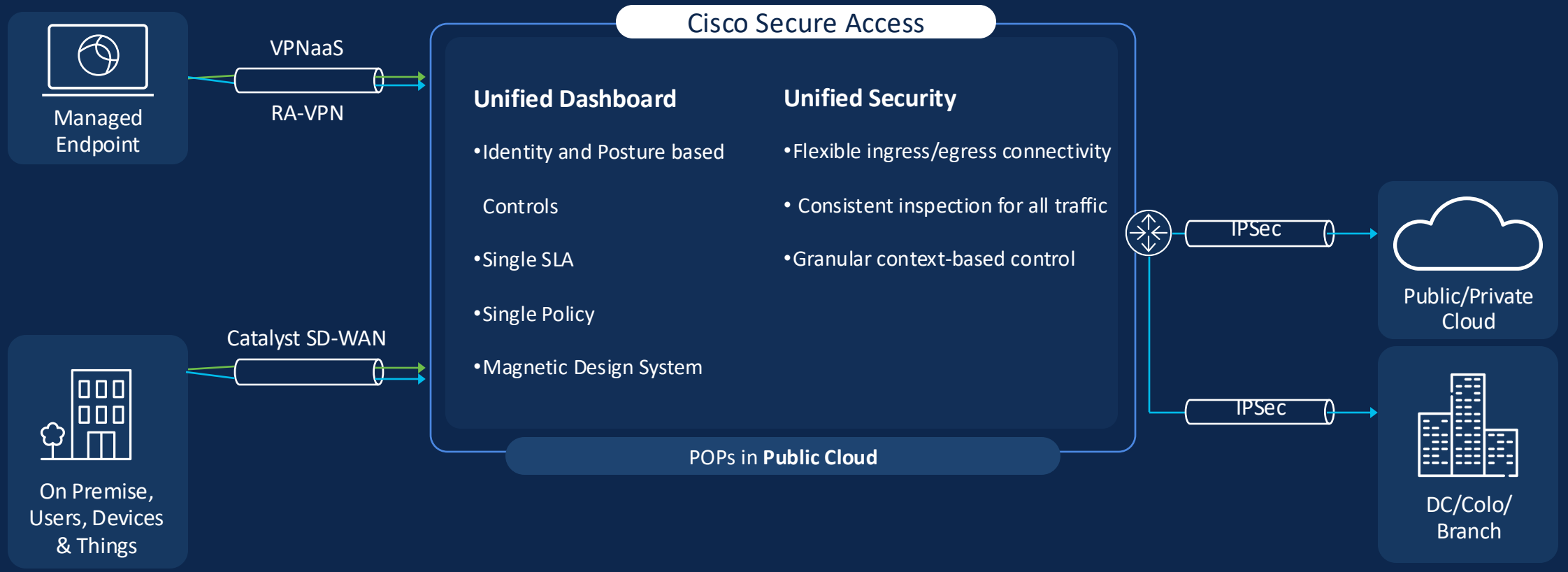
Policy Services Node (PSN)
- Makes policy decisions
- RADIUS/TACACS+ Servers

pXGrid Controller
- Facilitates sharing of context

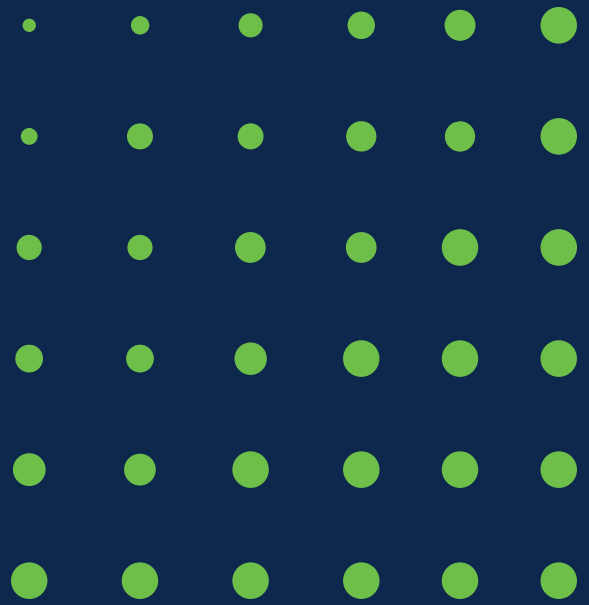
Architecture Overview



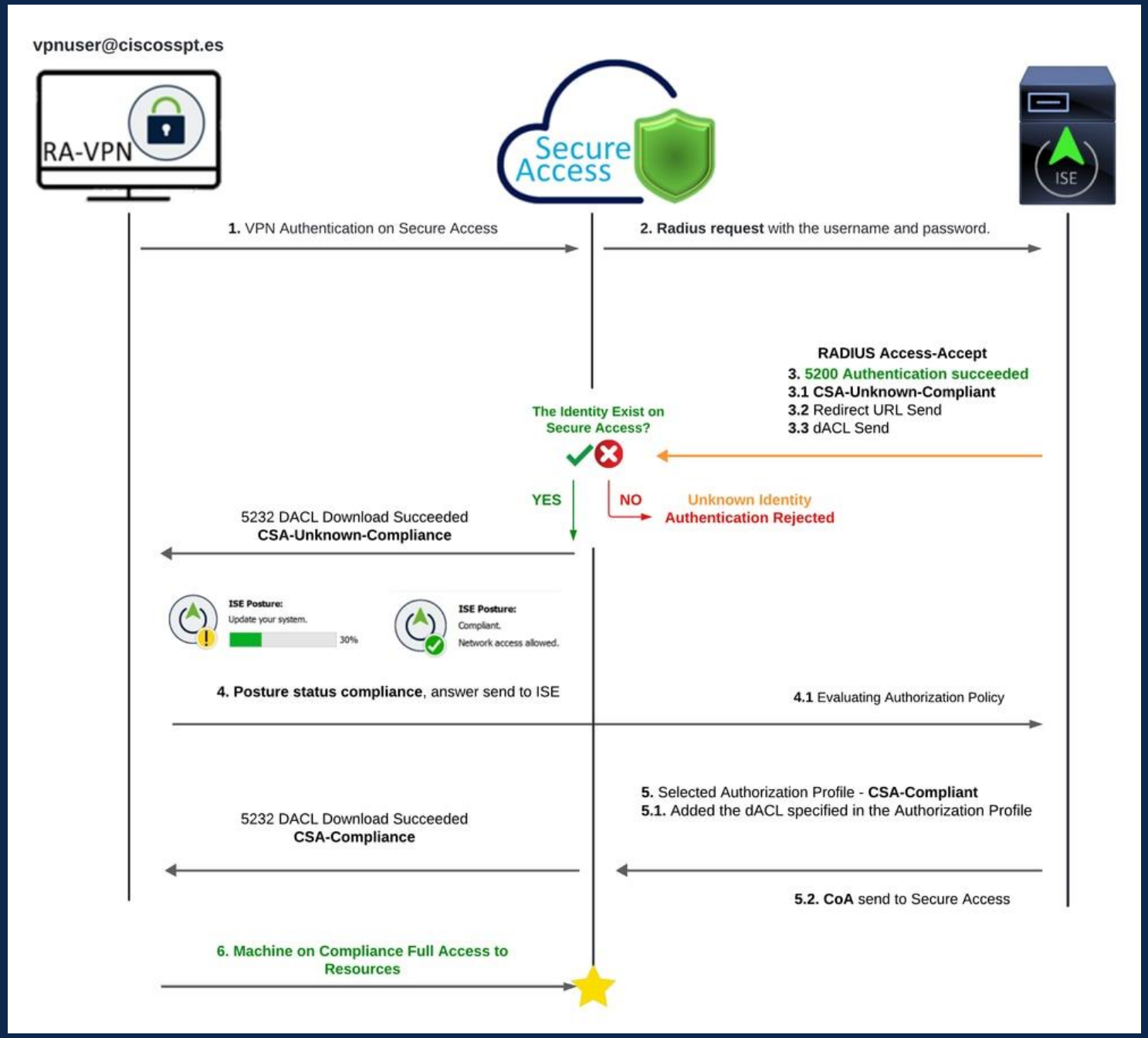
Architecture with ISE



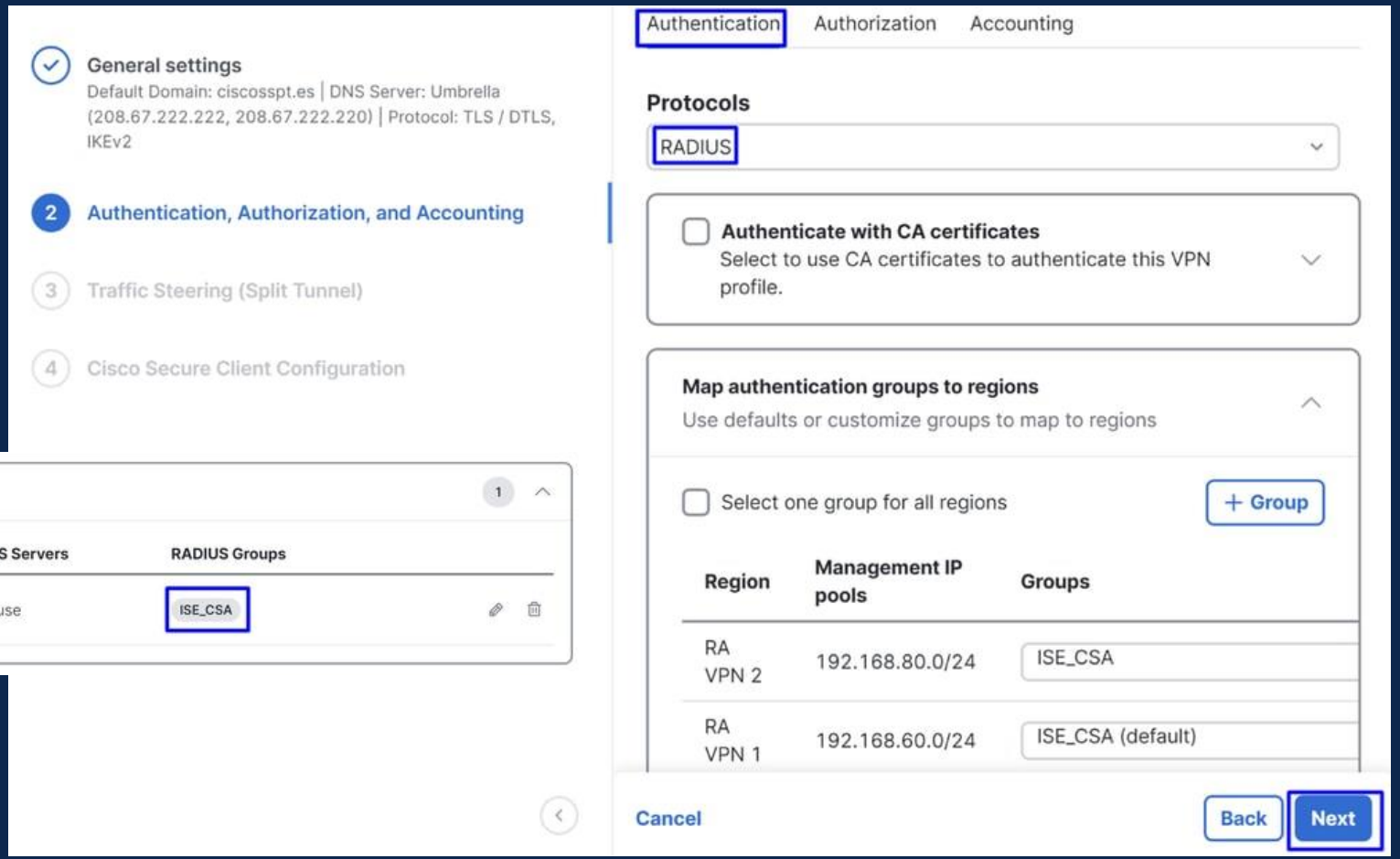
Secure Access with ISE as Radius Server and Posture



- Leverages already existing posture policies
  Cisco Identity Services Engine (ISE) or 3rd 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

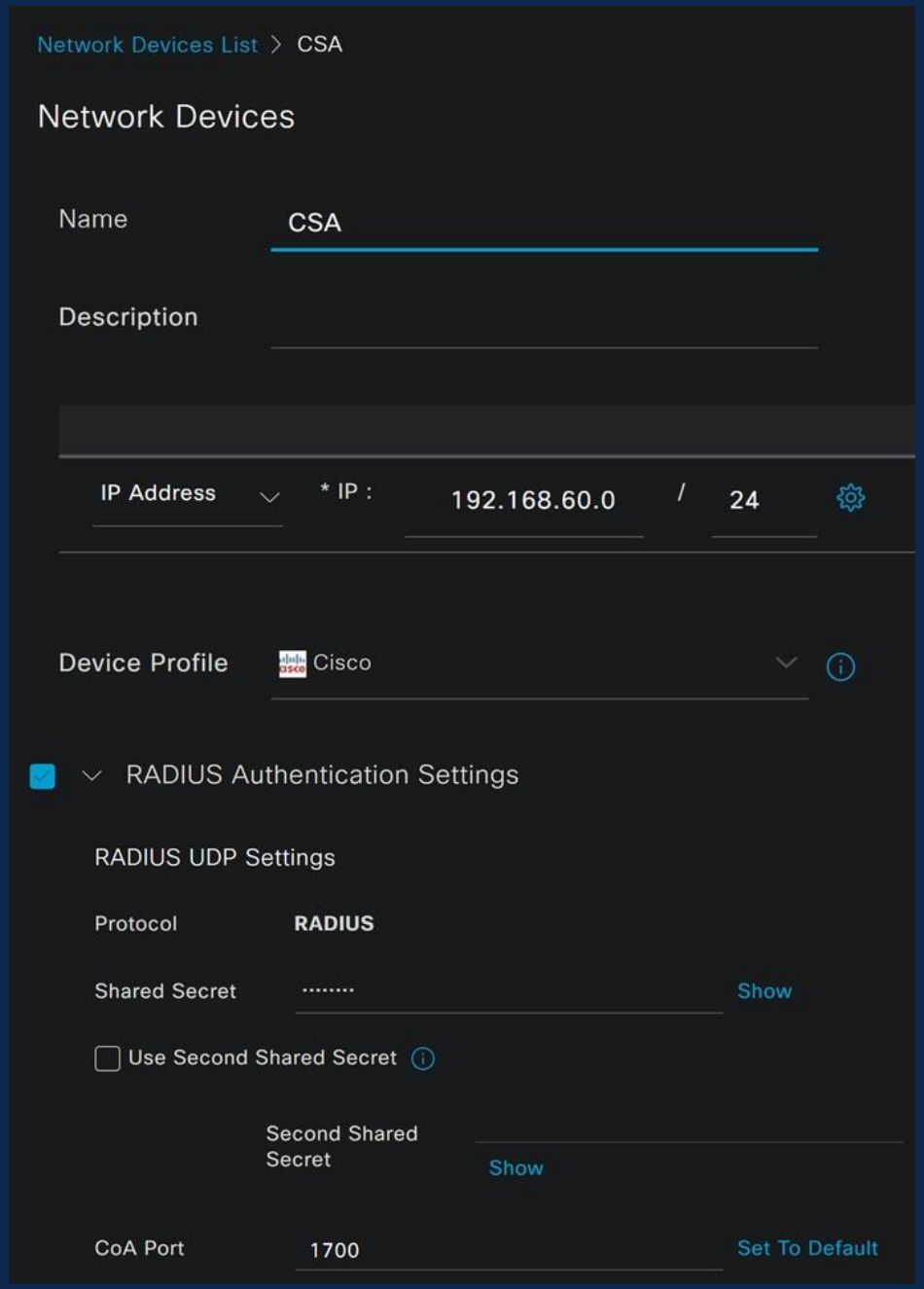


Configuration Guidelines

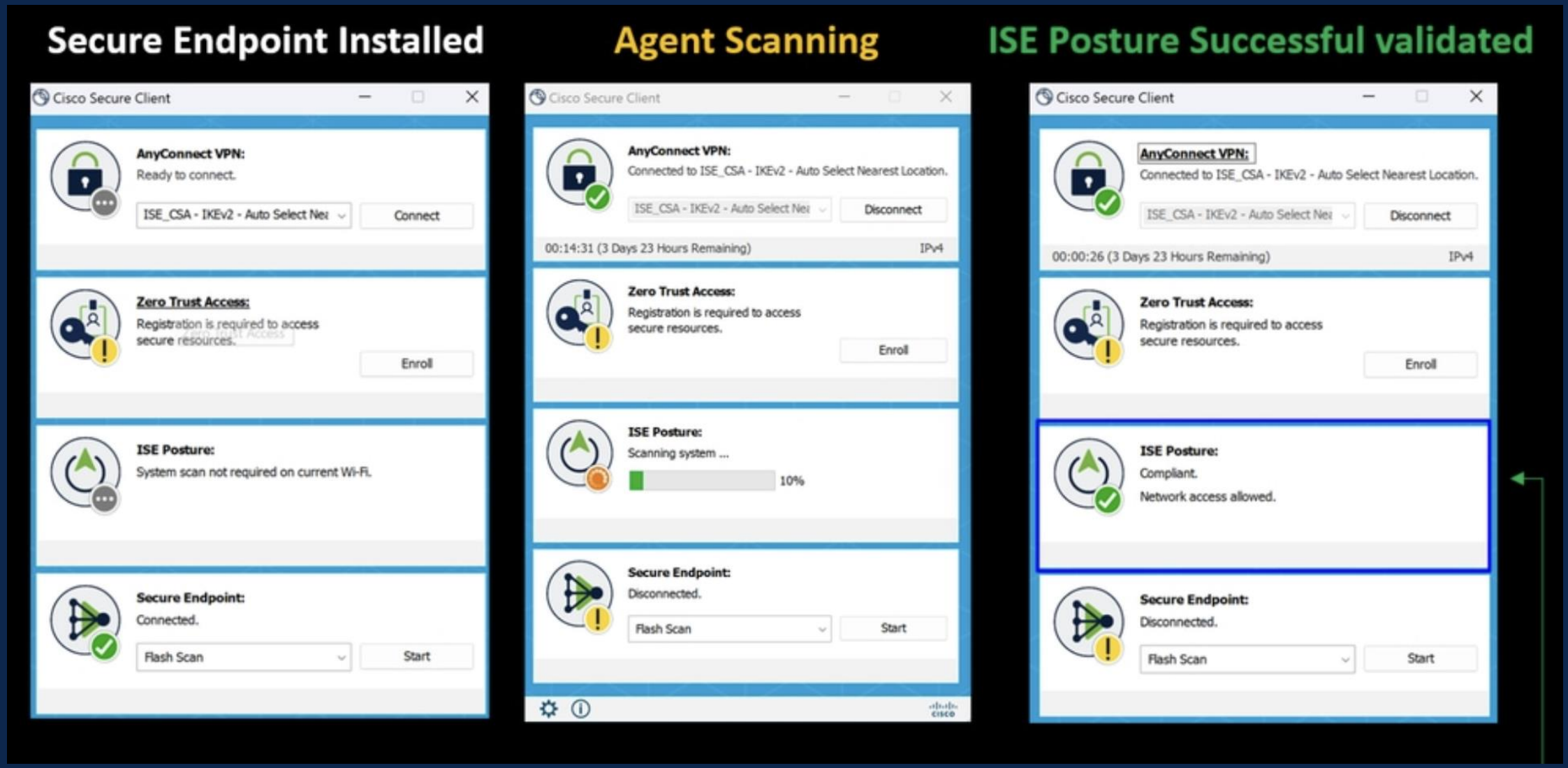


Configuration Guidelines

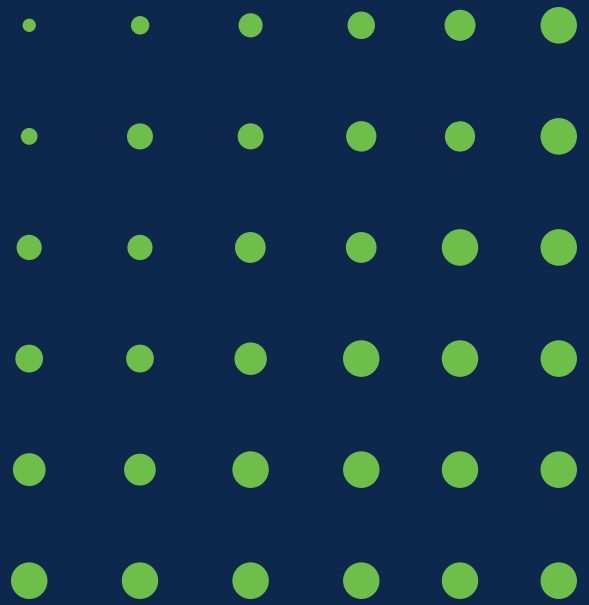
- **Name**: Use a name to Identify Secure Access
- **IP Address**: Configure the **Management Interface** of the step IP Pool configuration
- **Device Profile**: Choose Cisco
  - **Radius Authentication Settings**
    - **Shared Secret**: Configure the same shared secret set up on the Secure Access Radius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



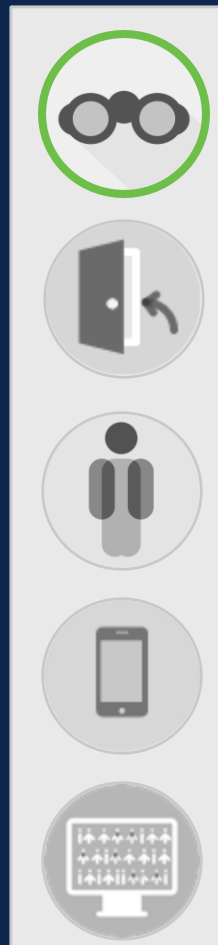
VPN-as-a-Service



Secure Access with ISE Context sharing

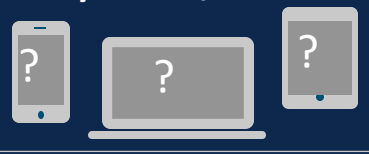


Rich Identity from Context



UNKNOWN

Without ISE

Poor context awareness		Rich context awareness
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
Access to any device/user 	RESULT	**Authorized network access** 

KNOWN

With ISE

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

- Consistent on or off-prem SGT enforcement
- SGT enforcement for internet and private access

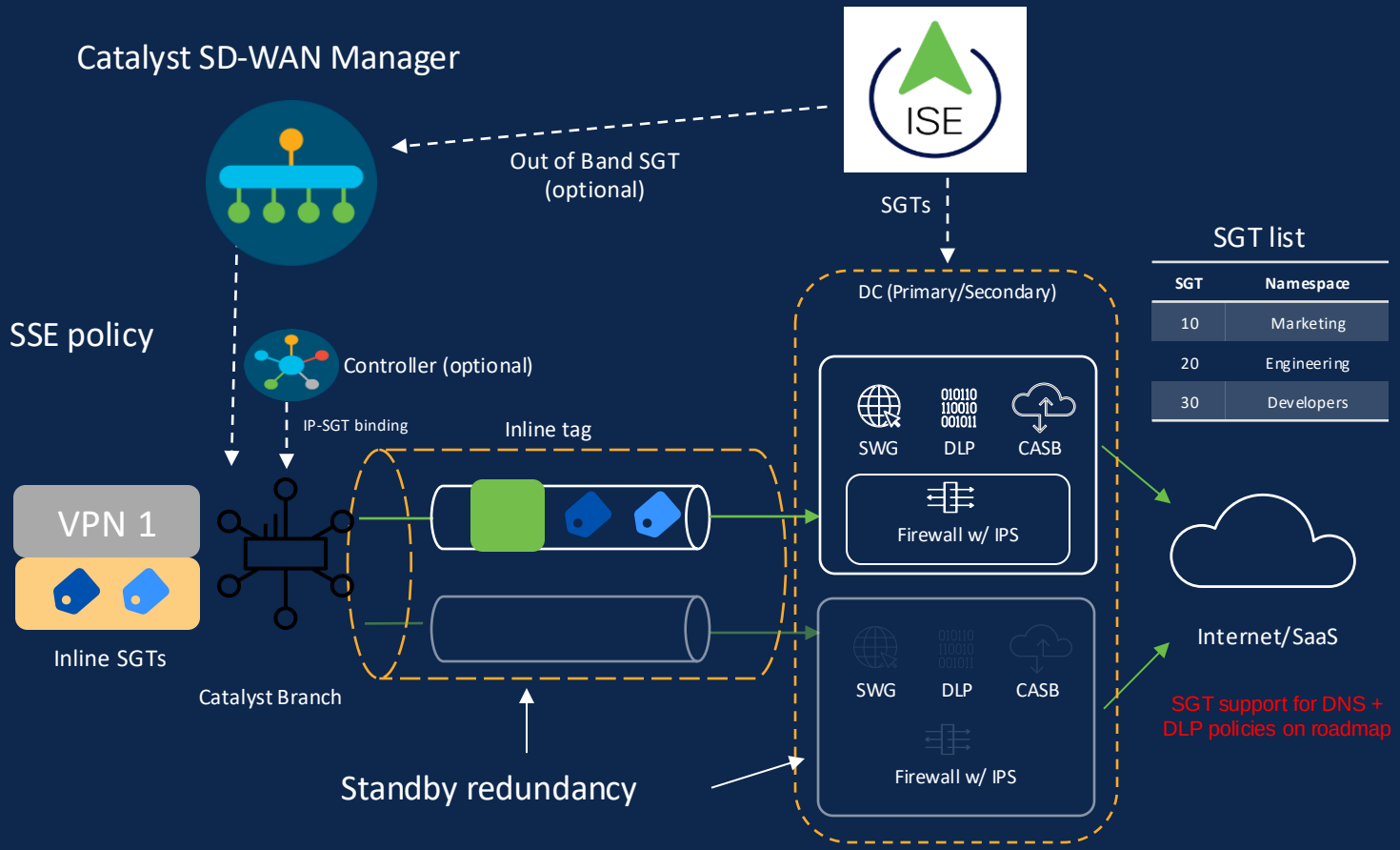
ISE supplies SGTs to Secure Access via Common Services

SGTs

SGT assignment via ISE authorization

Secure Access

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

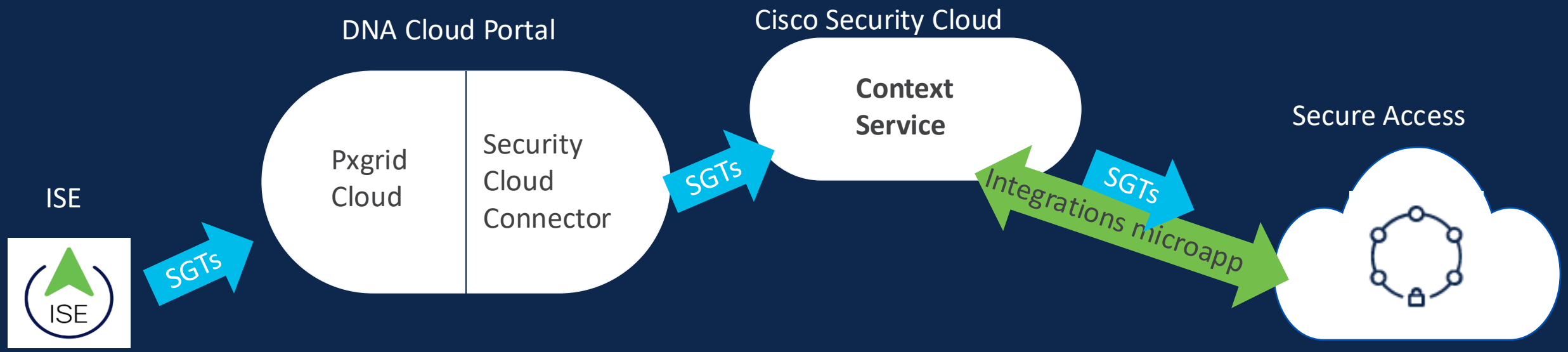


1. Cisco Secure Access establishes a secure connection with ISE context-services to consume SGTs
2. Learned SGTs can be leveraged to define access policies for branch accessing Internet/SaaS applications
3. In Catalyst Manager the Secure Service Edge policy group is configured to share SGT context in 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

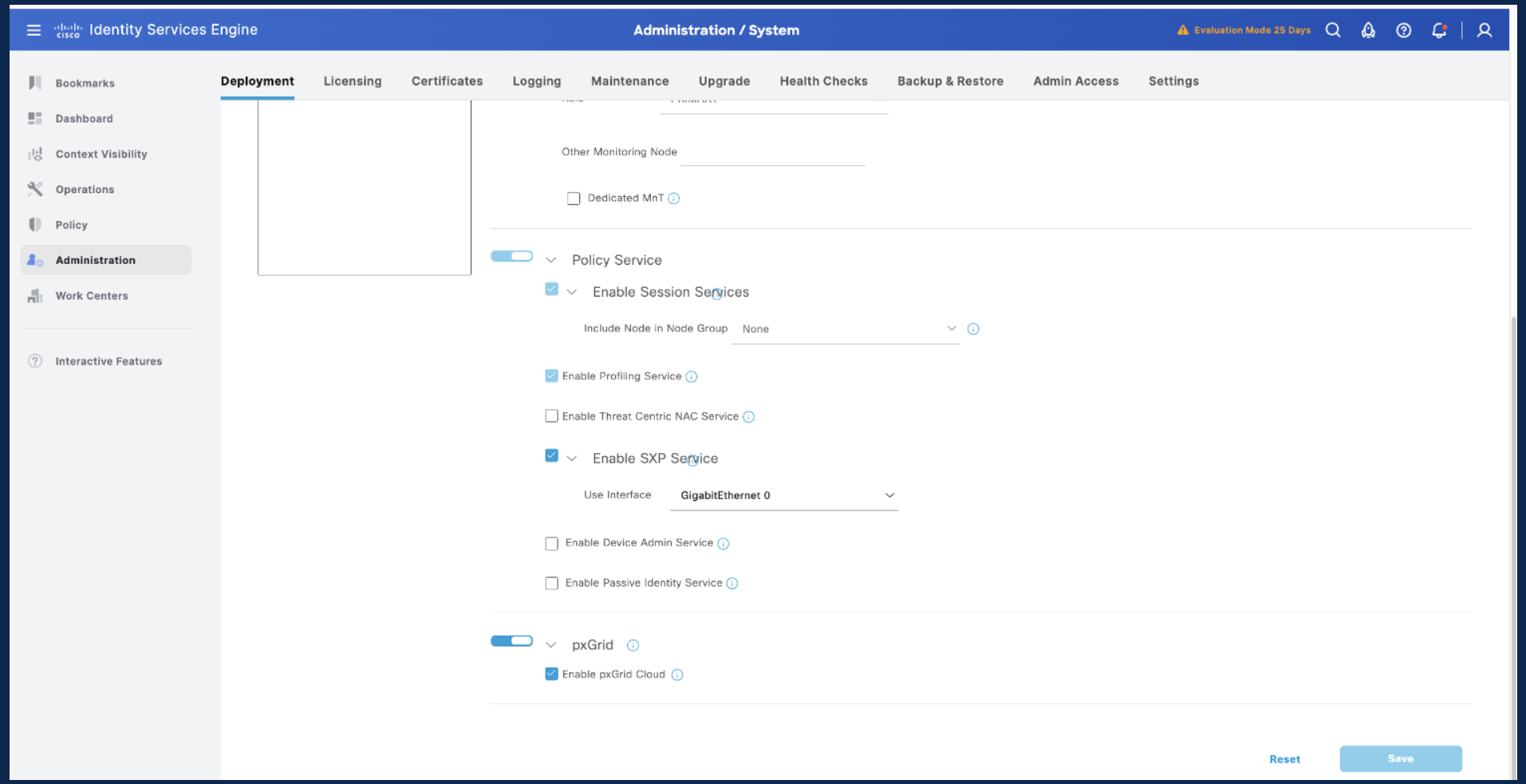
Policy: Source Object Precedence

- 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

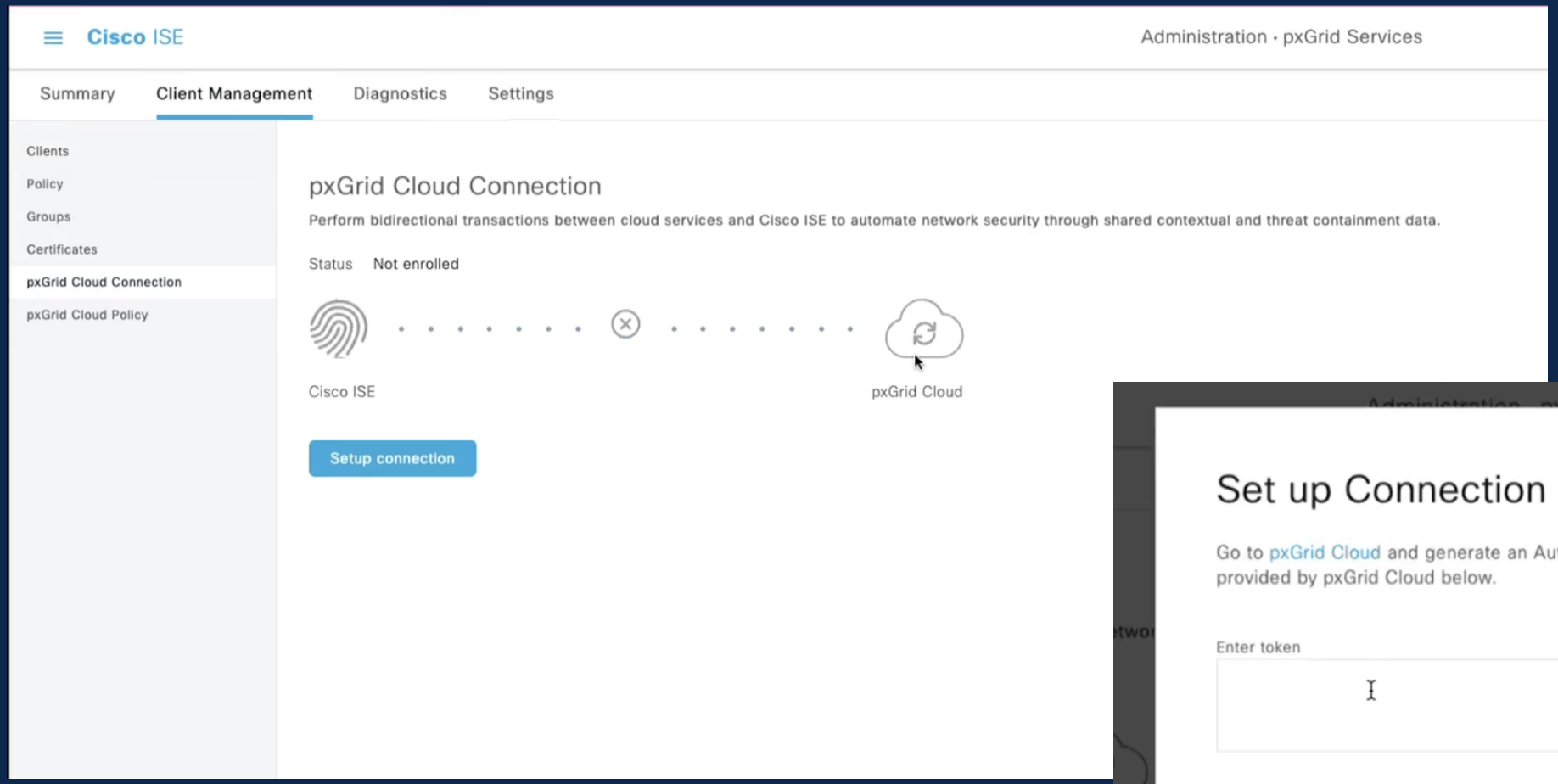
Context sharing overview

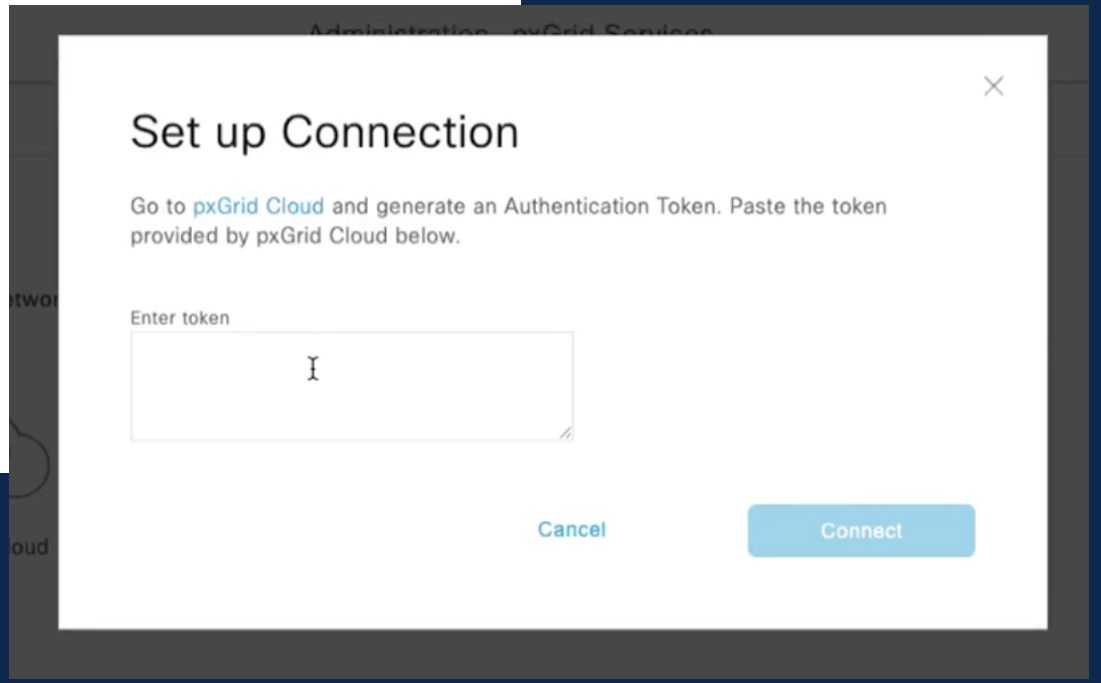


ISE – PxGrid Cloud configuration

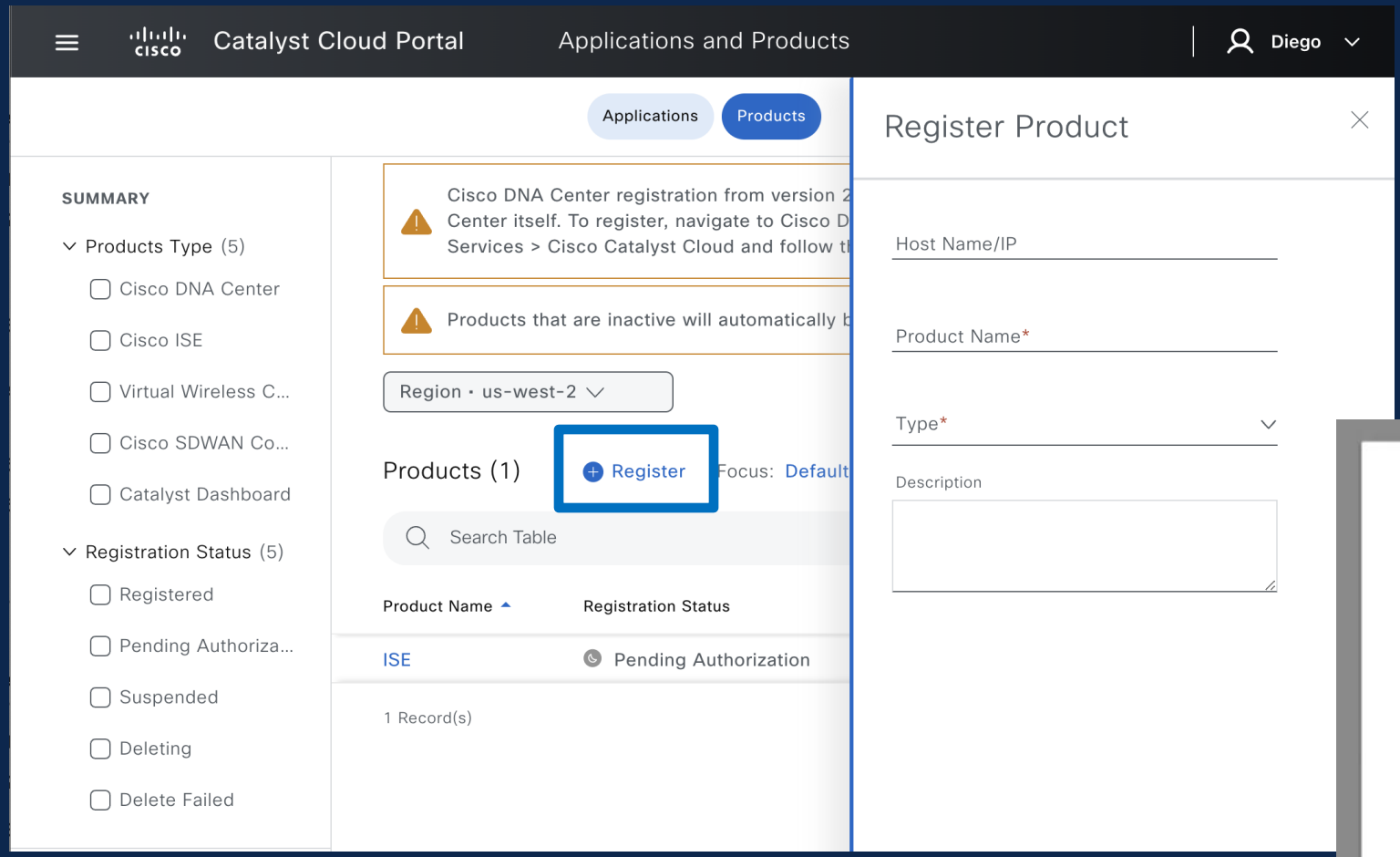


ISE – PxGrid Cloud configuration

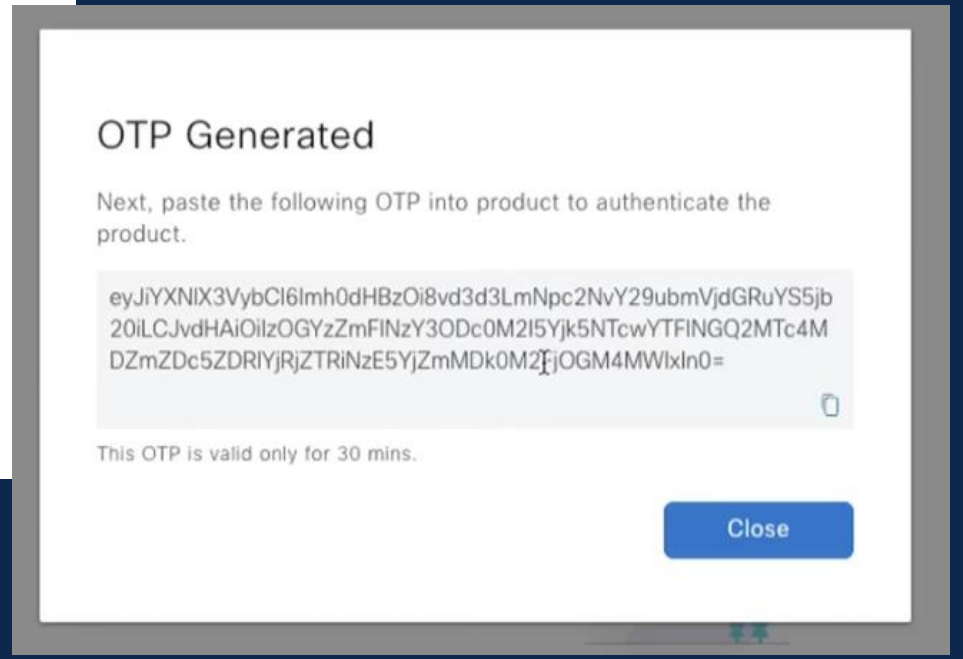




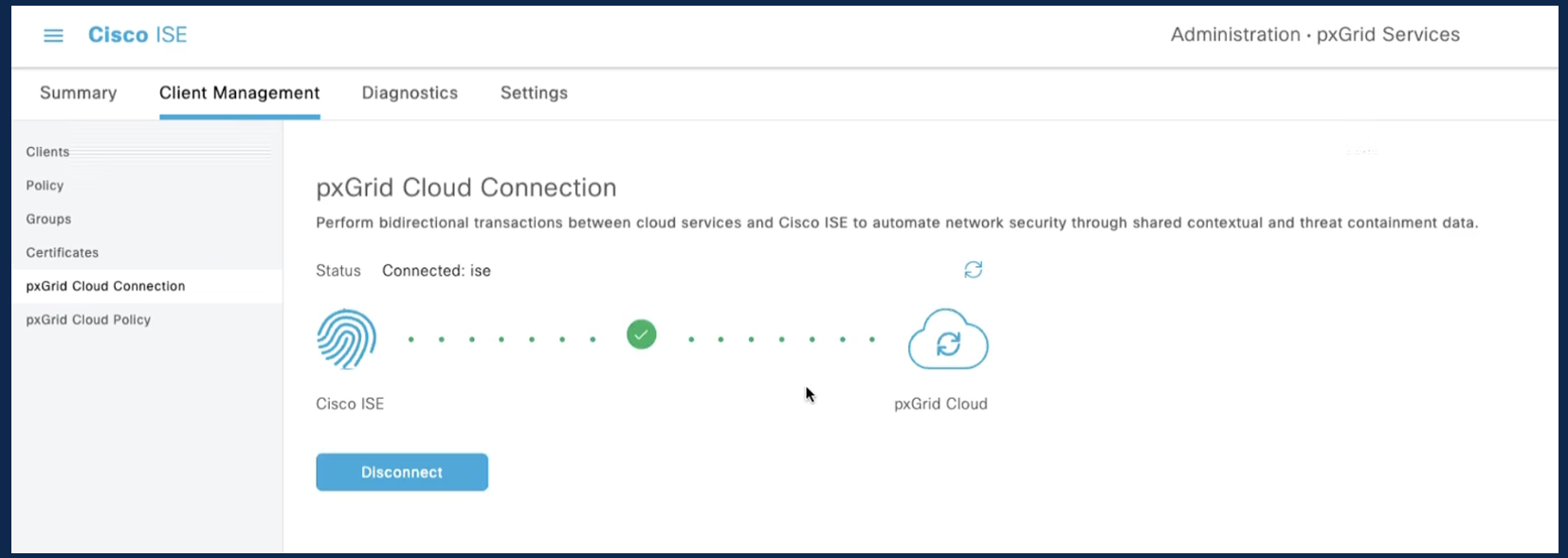
ISE – PxGrid Cloud configuration



dna.cisco.com



ISE – PxGrid Cloud configuration



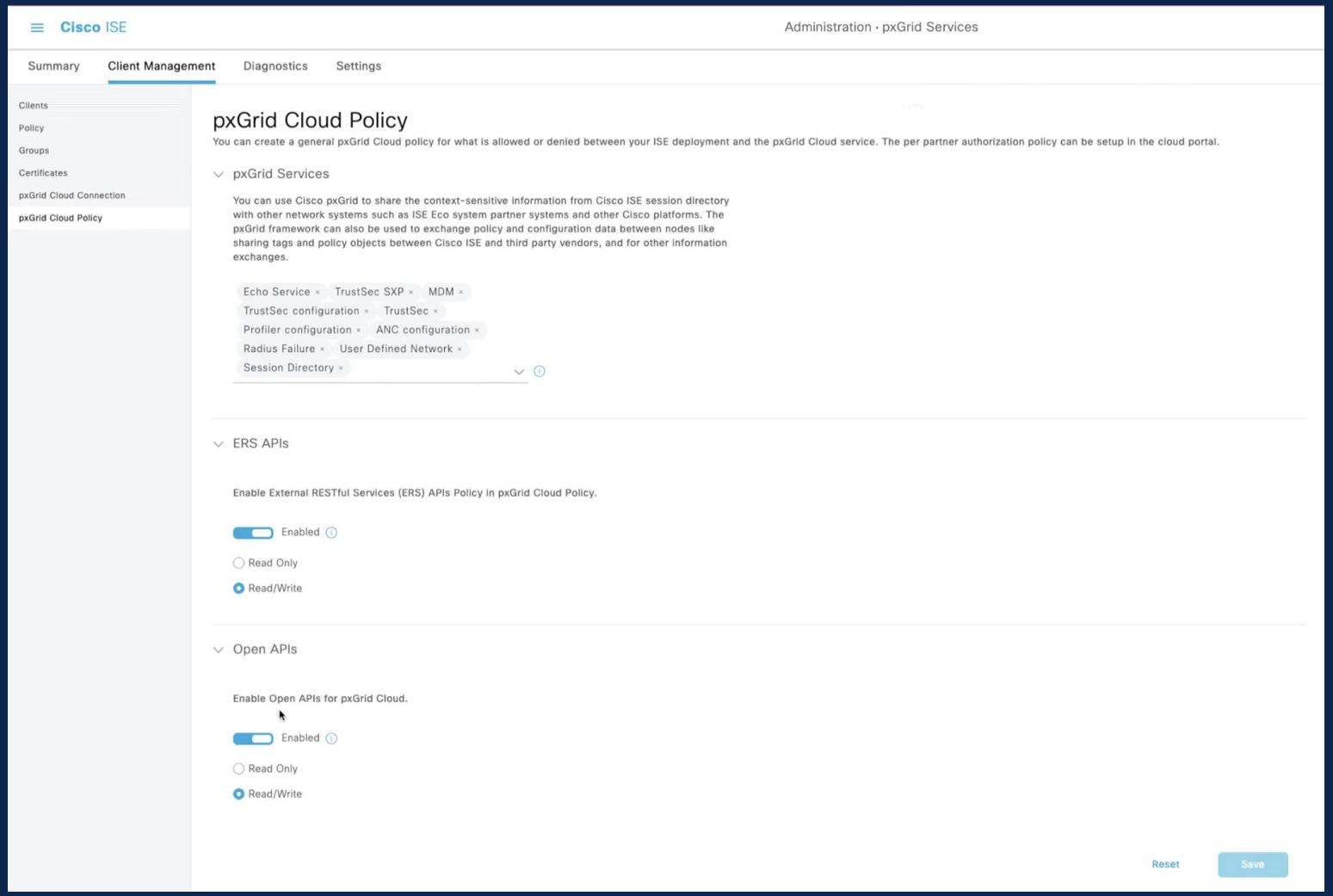
ISE – PxGrid Cloud configuration

Services consumables by Secure Access are:

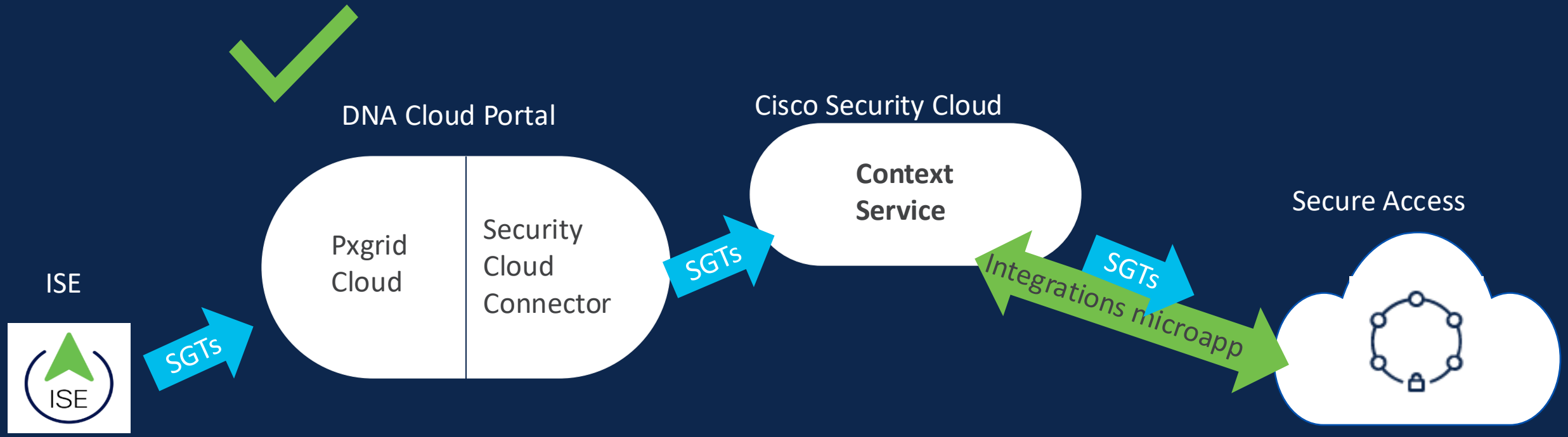
- **Trust Sec**
- **Echo Service**

ERS API: Enabled

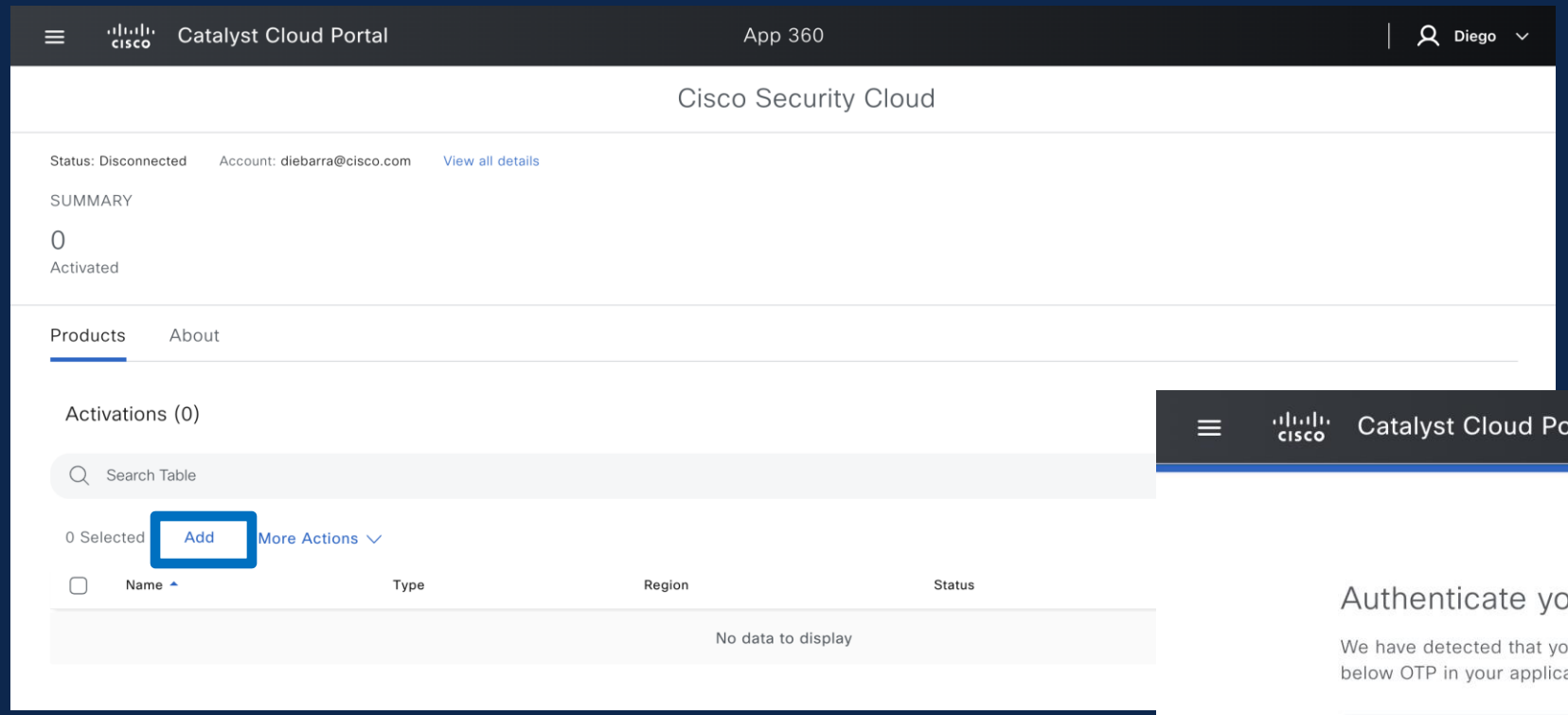
Open APIs: Enabled



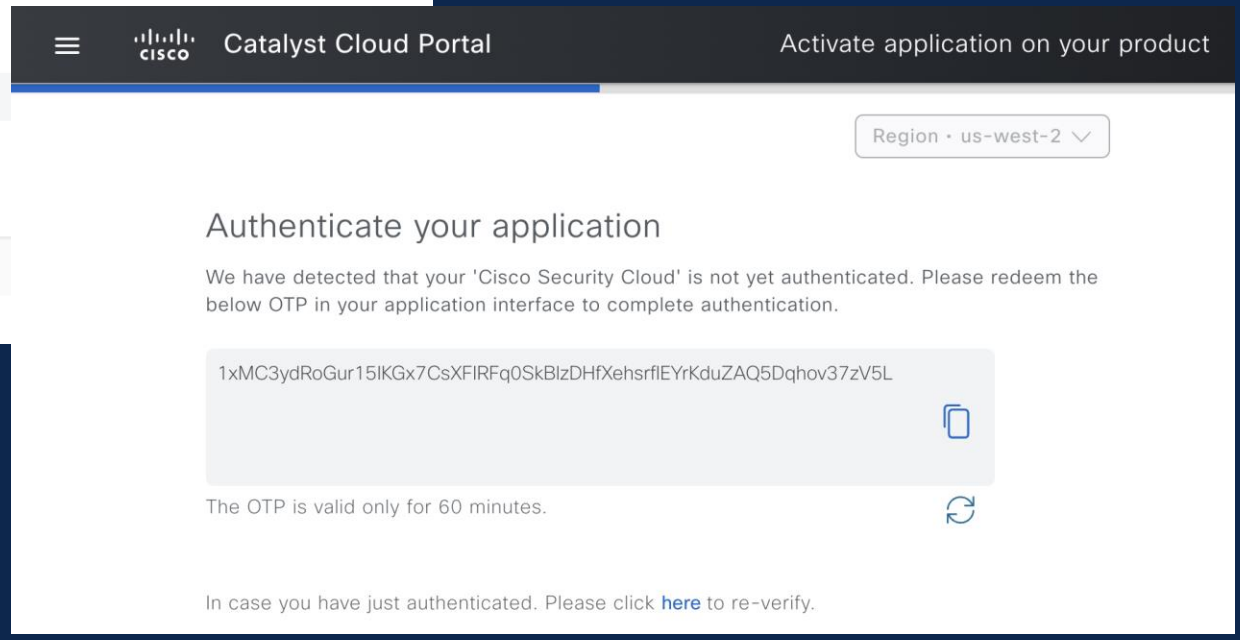
Context sharing overview



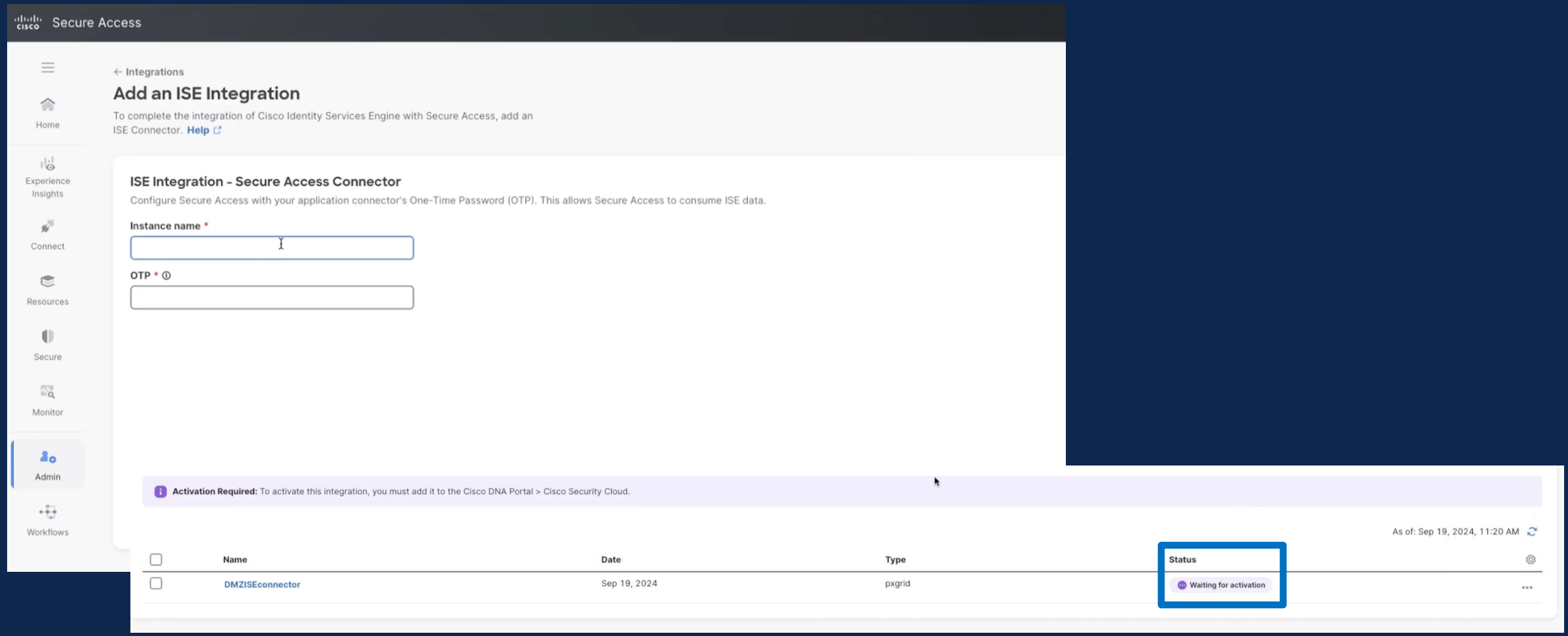
PxGrid Cloud – Secure Access configuration



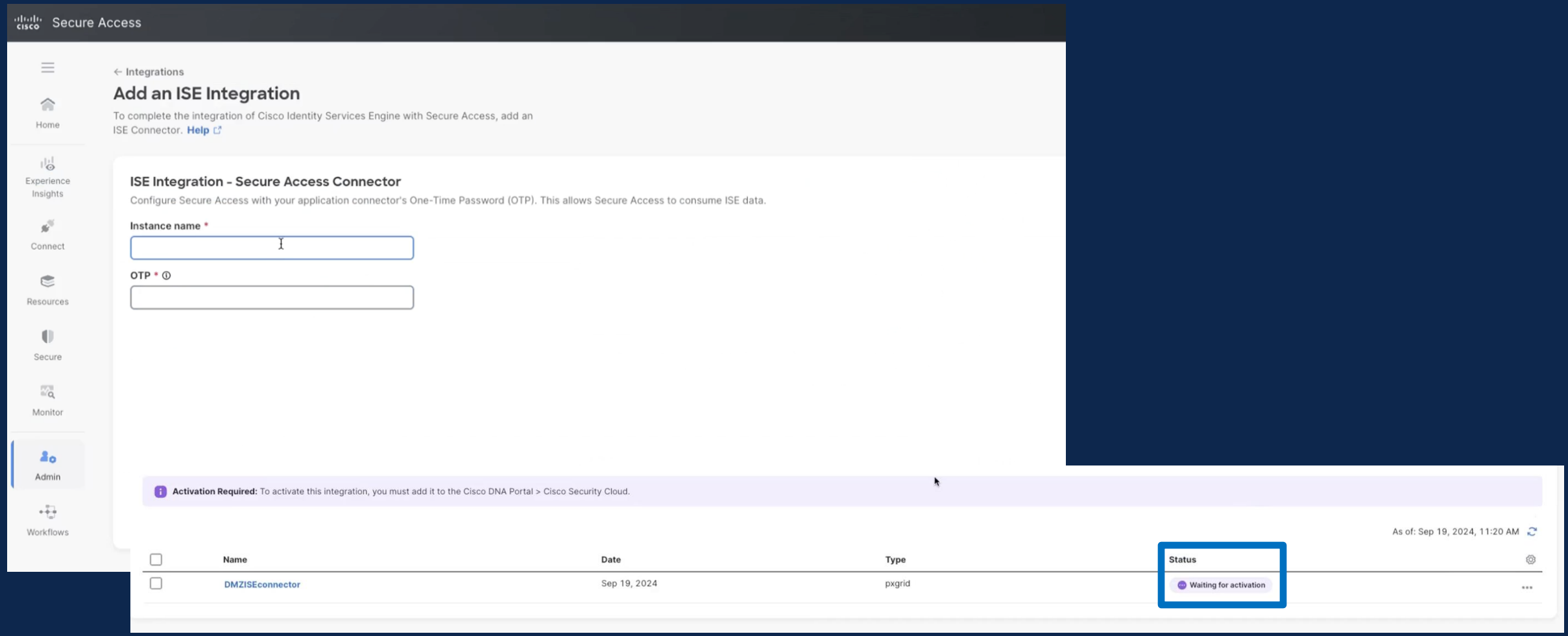
dna.cisco.com



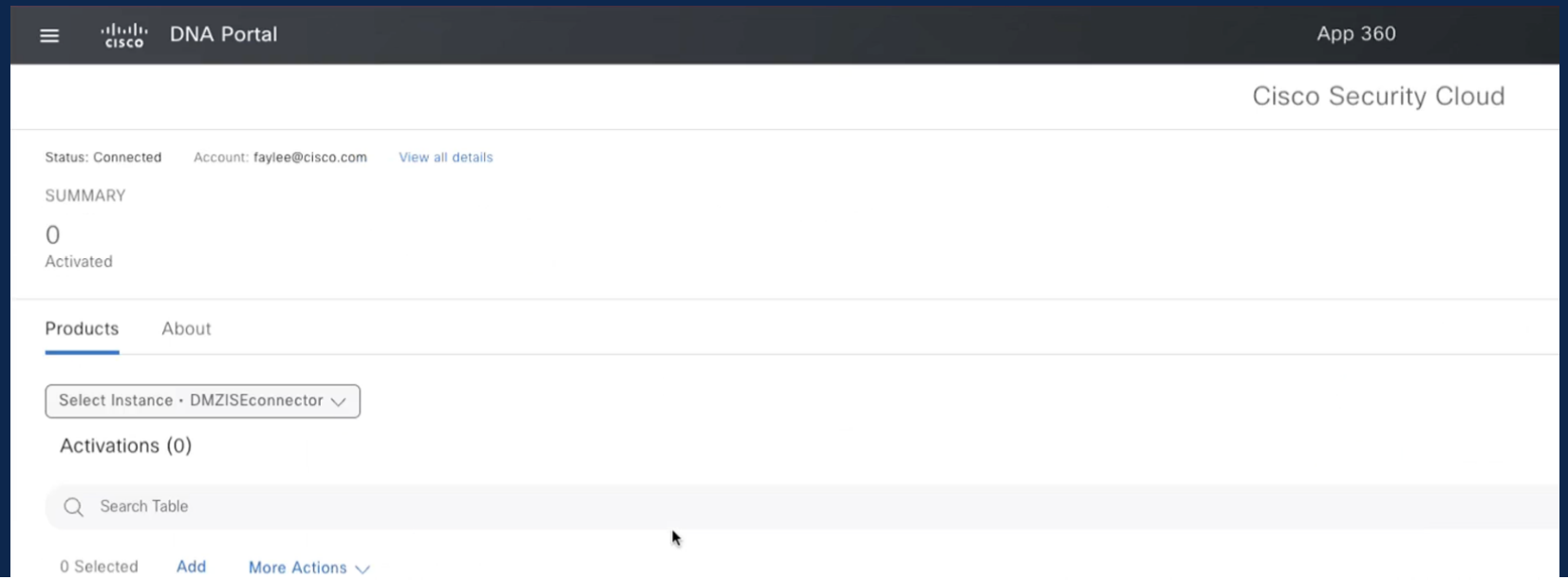
PxGrid Cloud – Secure Access configuration

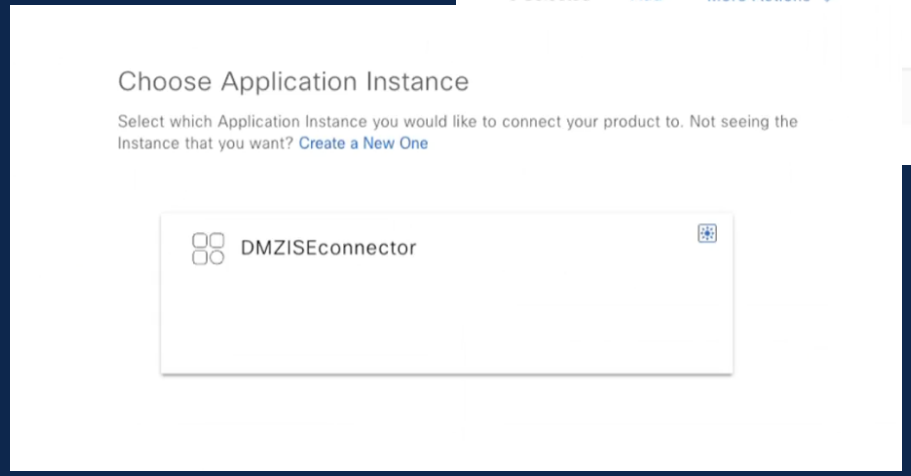


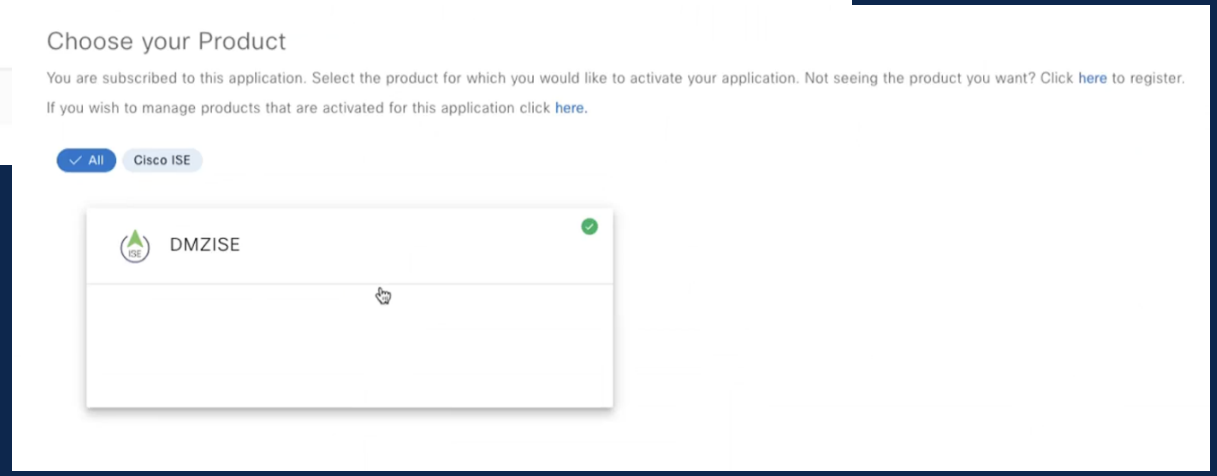
PxGrid Cloud – Secure Access configuration



PxGrid Cloud – Secure Access configuration

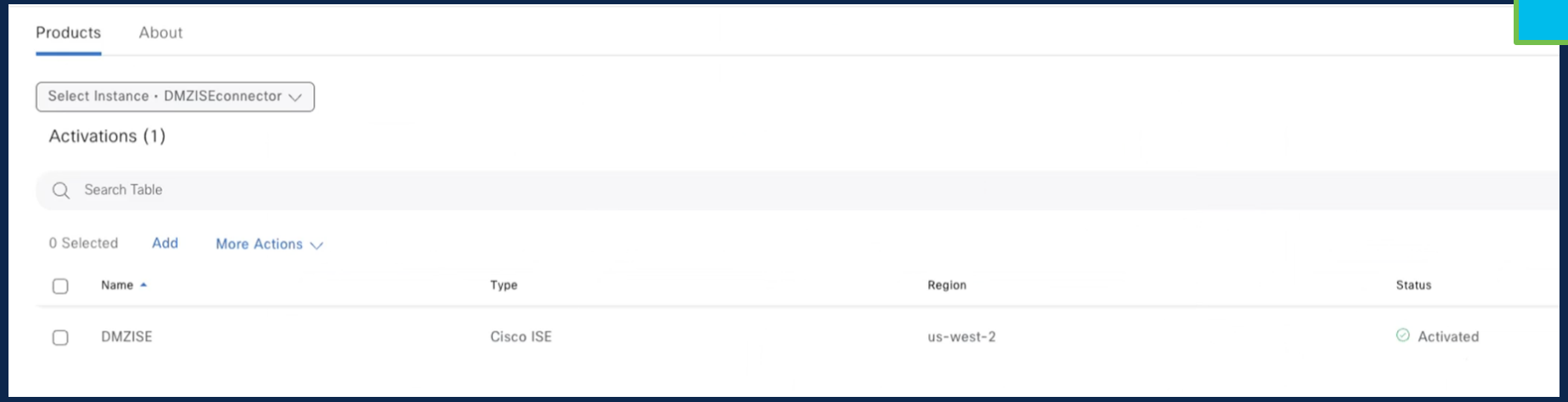






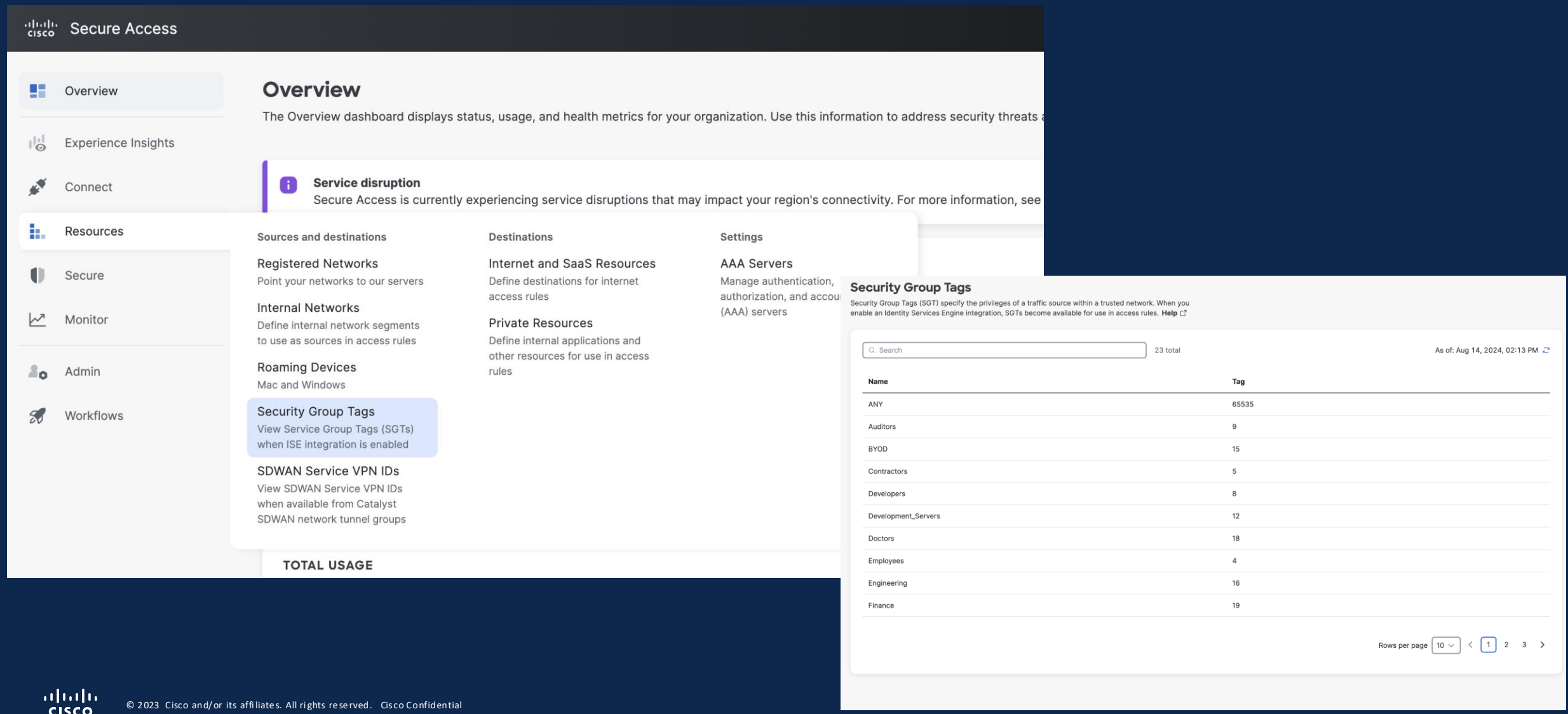
PxGrid Cloud – Secure Access configuration

dna.cisco.com

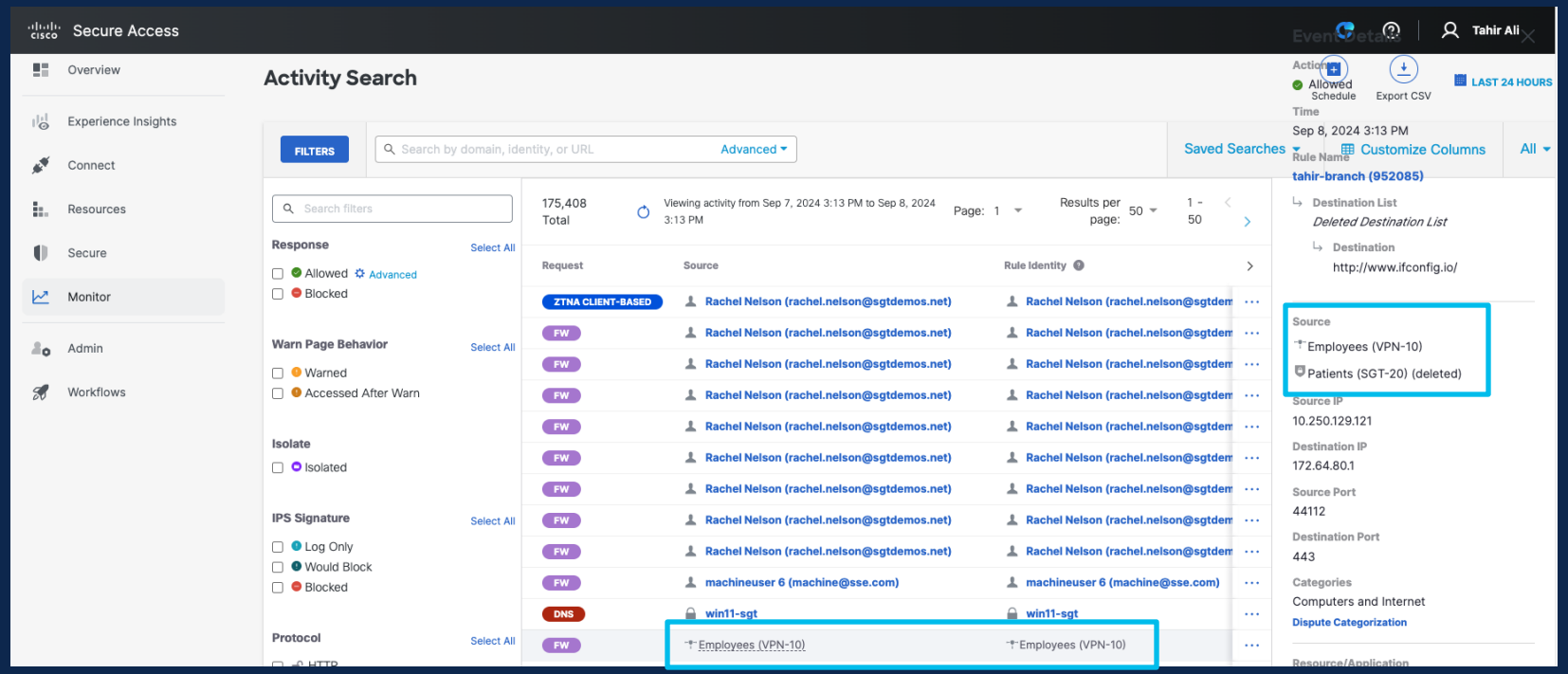


Secure Access

On Cisco Secure Access: Monitor SGT



Secure Access: Activity Search



Handy for troubleshooting context sharing enablement issues

Q&A

SECURE