The bridge to possible

Using ISE OpenAPI to automate certificate management

Taking some of the friction out of managing ISE

Steven McNutt, Cybersecurity Solutions Engineer
CCIE# 6495
@densem0de

DEVNET-2140

Cisco Webex App

Questions?

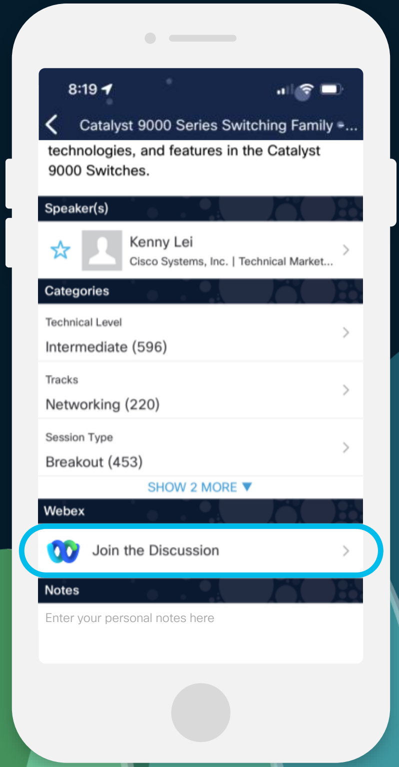
Use Cisco Webex App to chat
with the speaker after the session

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 June 7, 2024.

https://ciscolive.ciscoevents.com/
ciscolivebot/#DEVNET-2140



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Agenda

- Introduction
- ISE API Primer
- ISE System certificates
- Certificate management API
- Automation use cases
- Enrollment Protocols
- Demo
- Wrap-up

Introduction

- Certificate management is a core operational task of Identity Services Engine.
- It's also one of the biggest friction points in maintaining an ISE deployment.

- Certificate management tasks are performed manually.
- New APIs provide opportunities to automate these tasks
- Reduces effort and risk

Assumptions

- Familiar with cryptography basics
- Familiar with PKI basics
- Familiar with ISE
- Some basic python knowledge

Yes, that’s a lot of assumptions!

- Happy to answer follow up Qs in the Webex Chat

ISE API Primer

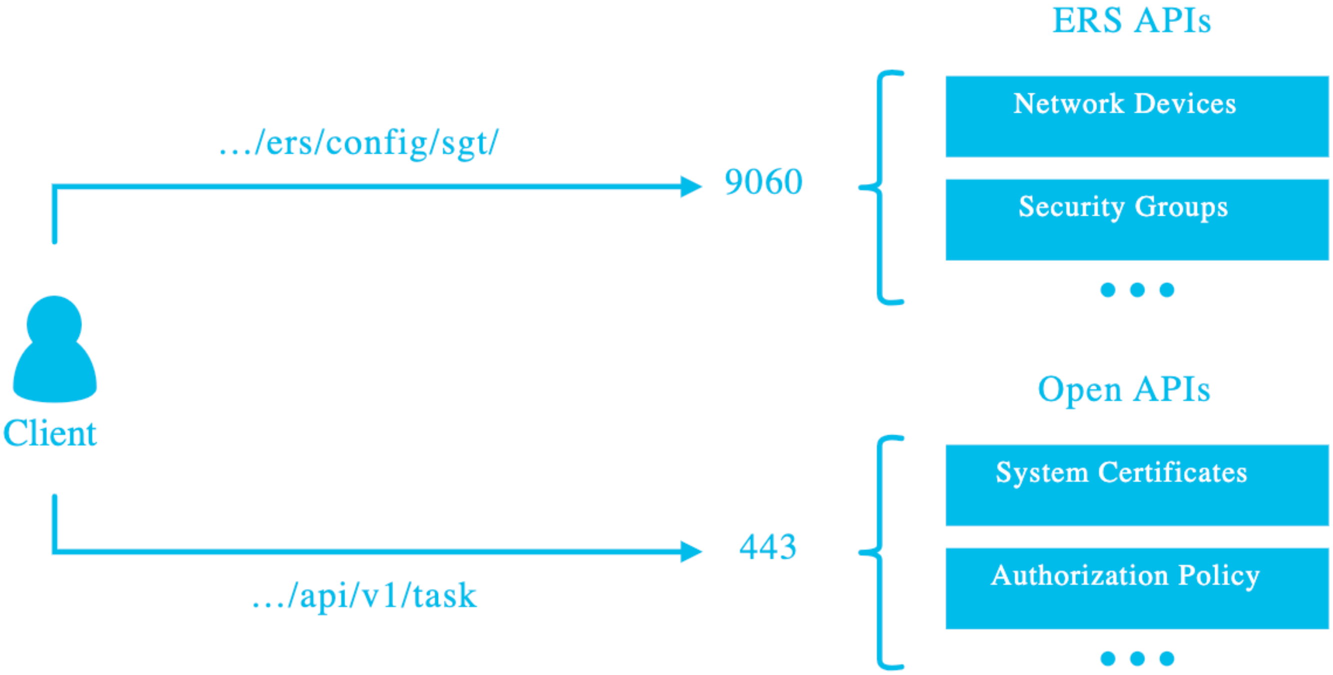
ISE API Services

- Pre-ISE 3.1:
  - MNT (Monitoring and Troubleshooting) - ISE 1.0
  - ERS (External Restful Services) - ISE 1.2

- ISE 3.1+
  - API Gateway for routing
  - OpenAPI

API Services

API Services Overview:

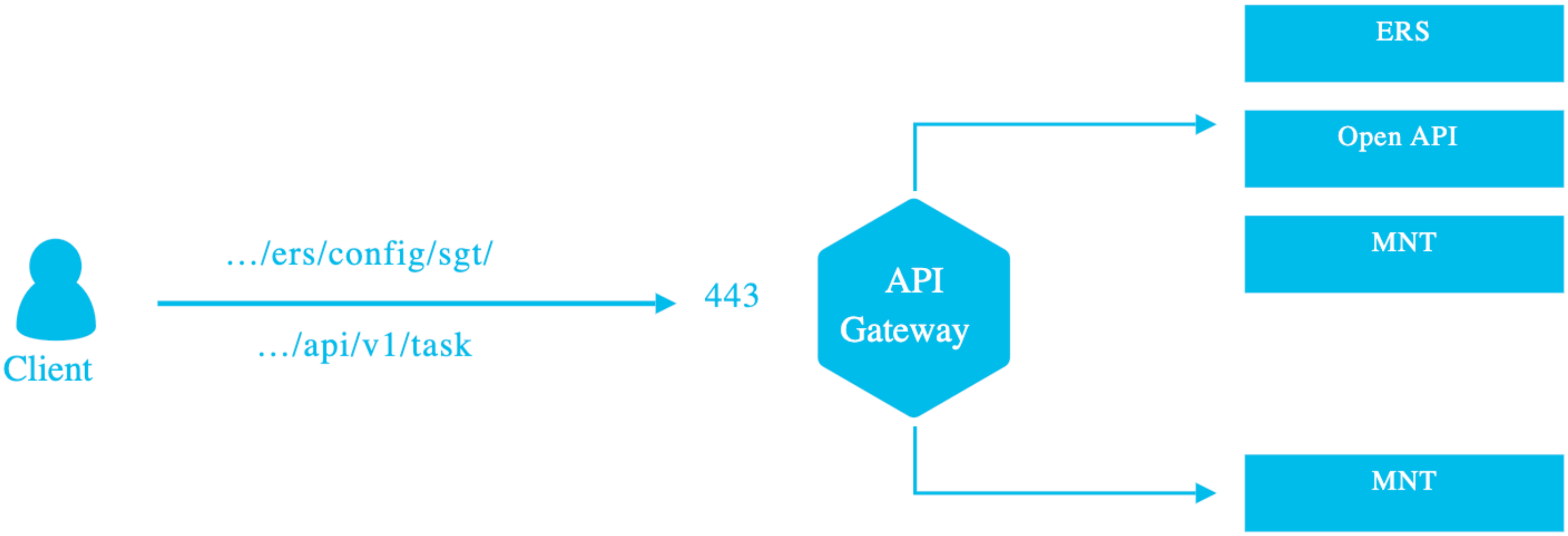


ISE API Gateway

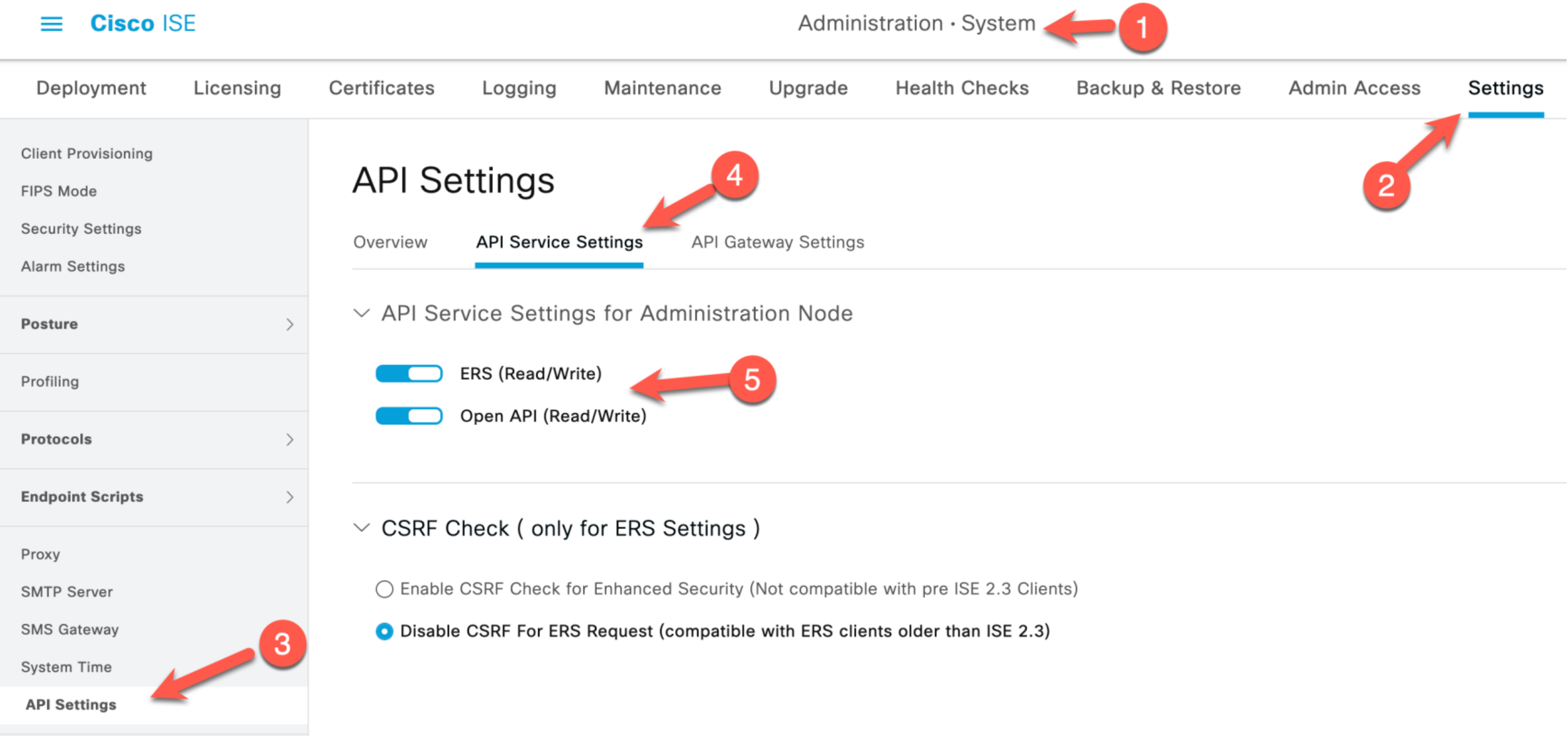
- Single access point for routing requests to different nodes
- Eliminates the need to use port 9060 to access the ERS API
- New in ISE 3.1

API Gateway

API Gateway Overview:



Enabling API Services



API Service Settings for Administration Node

- ERS (Read/Write) — enabled
- Open API (Read/Write) — enabled

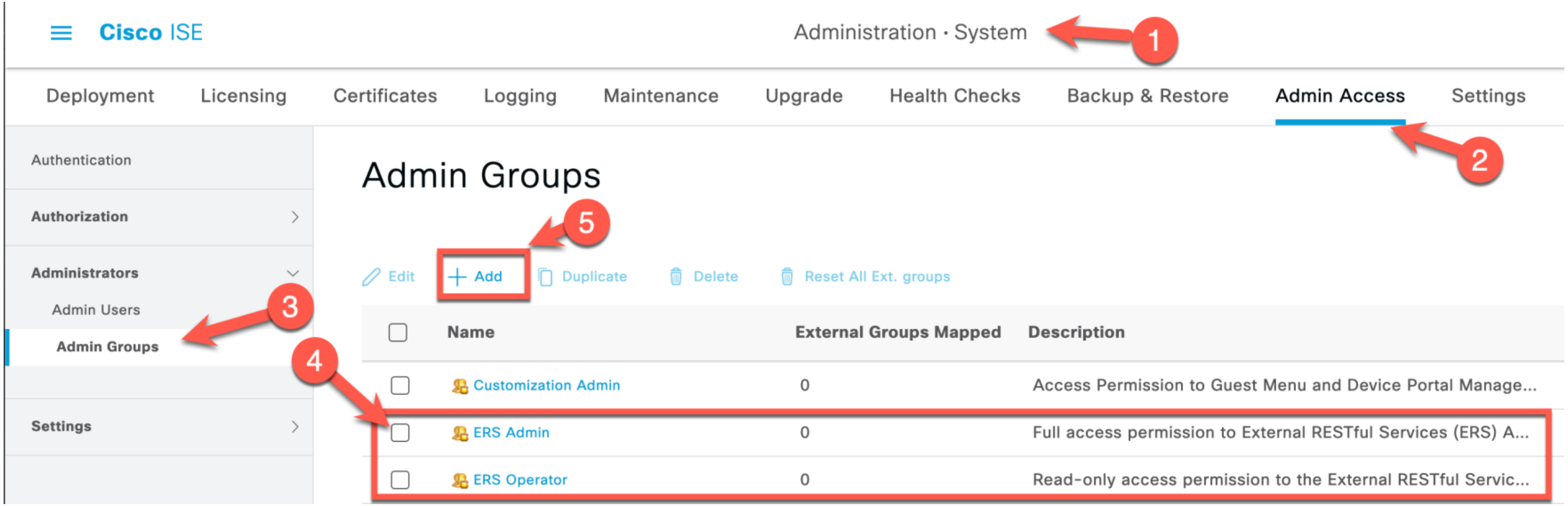
CSRF Check (only for ERS Settings)

○ Enable 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)

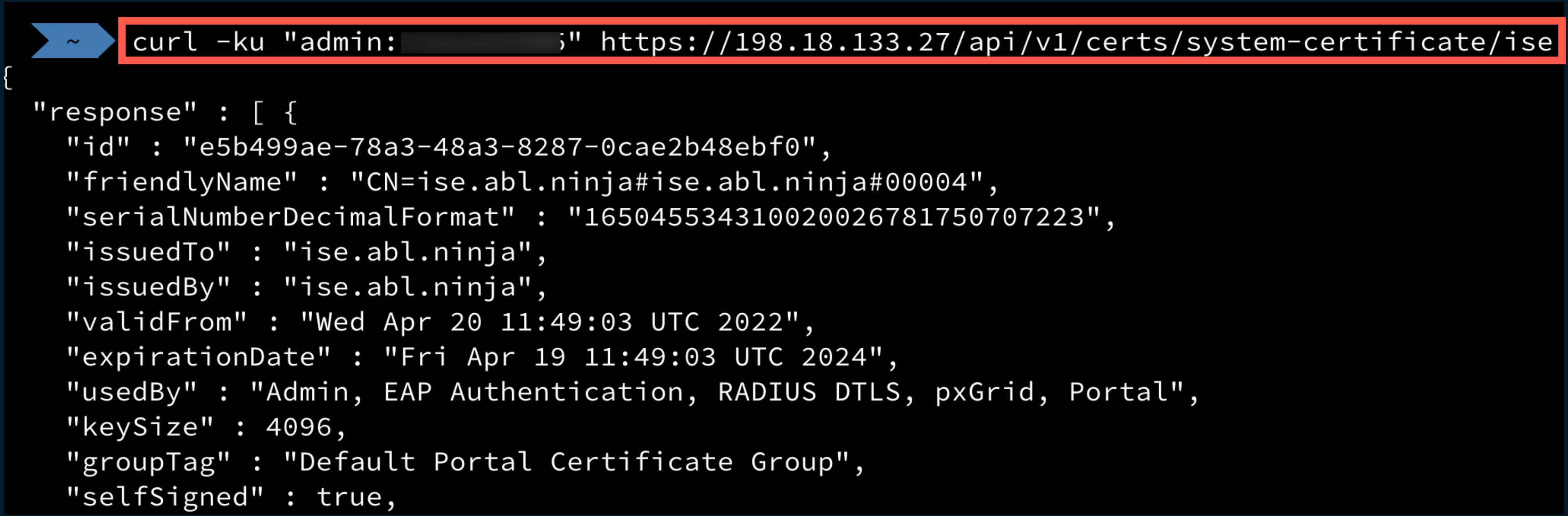
Authorizing Admin Users

Add an admin user to one of these ERS groups:



□	Name	External Groups Mapped	Description
□	Customization Admin	0	Access Permission to Guest Menu and Device Portal Manage...
□	ERS Admin	0	Full access permission to External RESTful Services (ERS) A...
□	ERS Operator	0	Read-only access permission to the External RESTful Servic...

Example call



```
~  curl -ku "admin:[redacted]" https://198.18.133.27/api/v1/certs/system-certificate/ise
{
  "response" : [ {
    "id" : "e5b499ae-78a3-48a3-8287-0cae2b48ebf0",
    "friendlyName" : "CN=ise.abl.ninja#ise.abl.ninja#00004",
    "serialNumberDecimalFormat" : "165045534310020026781750707223",
    "issuedTo" : "ise.abl.ninja",
    "issuedBy" : "ise.abl.ninja",
    "validFrom" : "Wed Apr 20 11:49:03 UTC 2022",
    "expirationDate" : "Fri Apr 19 11:49:03 UTC 2024",
    "usedBy" : "Admin, EAP Authentication, RADIUS DTLS, pxGrid, Portal",
    "keySize" : 4096,
    "groupTag" : "Default Portal Certificate Group",
    "selfSigned" : true,
```

System Certificates

System Certificate considerations

- Public PKI
  - Best used for non-corporate devices
  - Short lifetime
  - CA validation means SAN entries often get stripped from CSRs
  - Portal certificates good fit
- Internal PKI (ex: Active Directory Certificate Services)
  - Best used for corporate-managed devices
  - Longer lifetime
  - Unlimited flexibility with certificate design
- Self-signed (no PKI)
  - Limited usefulness, only type that supports renewal

System Certificates (partial list)

- Admin
  - Internal PKI
  - Good idea to include SAN entries for IP addresses, short names, etc
- Portal
  - Public PKI (short lifetime, SAN entries problematic)
- EAP (used for 802.1x)
  - Internal PKI (longer lifetime, trusted by enrolled devices)
- SAML
  - Use public PKI, must be dedicated certificate
- PxGrid
  - Internal PKI – easier to integrate other services (i.e. firepower)

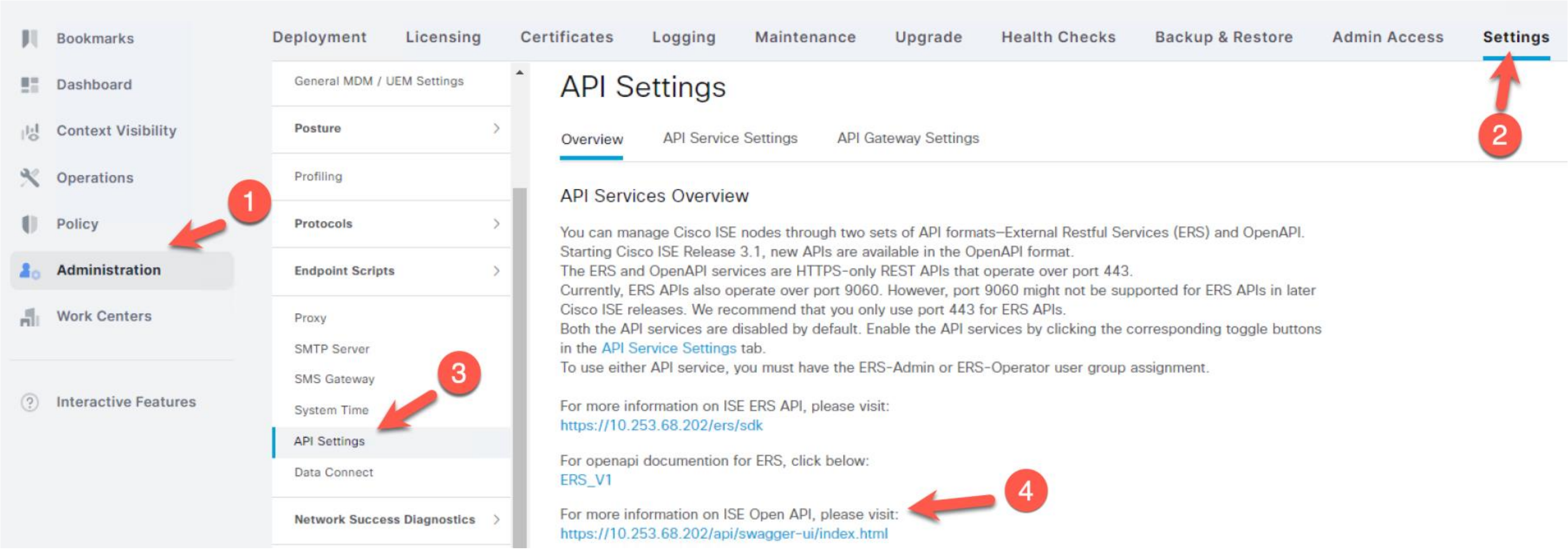
Certificate APIs

Certificate API Taxonomy

- Base path: /api/v1/certs
- Roughly 22 endpoints
- Six Categories of operations

- Signing requests
- System certificate ops
- Trusted certificate ops
- Regenerate Root CA
- Bind certificate
- Renew OSCP certificate

Accessing the swagger docs



API Settings

API Services Overview

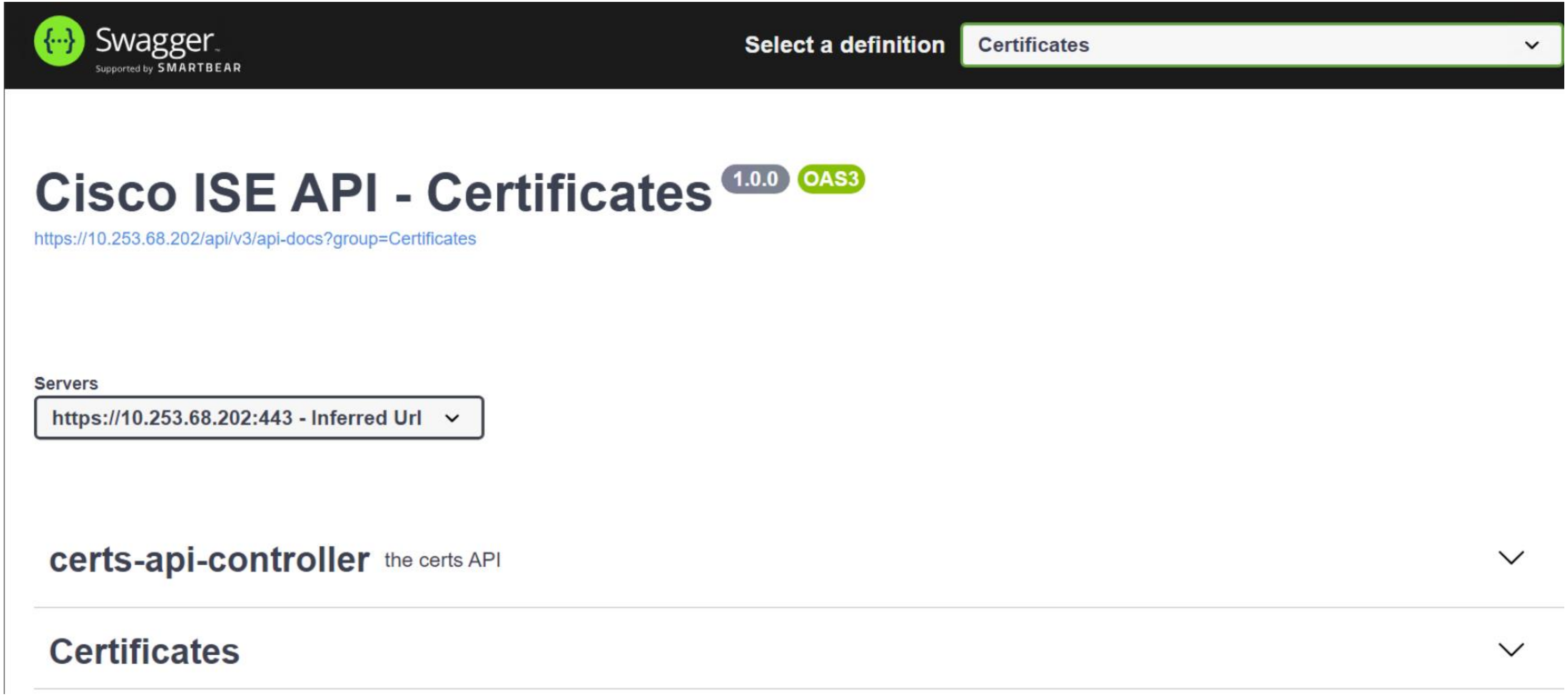
You can manage Cisco ISE nodes through two sets of API formats–External Restful Services (ERS) and OpenAPI.
Starting Cisco ISE Release 3.1, new APIs are available in the OpenAPI format.
The ERS and OpenAPI services are HTTPS-only REST APIs that operate over port 443.
Currently, ERS APIs also operate over port 9060. However, port 9060 might not be supported for ERS APIs in later Cisco ISE releases. We recommend that you only use port 443 for ERS APIs.
Both the API services are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API Service Settings tab.
To use either API service, you must have the ERS-Admin or ERS-Operator user group assignment.

For more information on ISE ERS API, please visit:
https://10.253.68.202/ers/sdk

For openapi documention for ERS, click below:
ERS_V1

For more information on ISE Open API, please visit:
https://10.253.68.202/api/swagger-ui/index.html

Selecting the Certificate API in Swagger



Select a definition: Certificates

Cisco ISE API - Certificates

1.0.0 OAS3

https://10.253.68.202/api/v3/api-docs?group=Certificates

Servers: https://10.253.68.202:443 - Inferred Url

certs-api-controller the certs API

Certificates

Use Cases

Reducing clickOps for fun and profit

- Get the system certificate lists for all nodes
- Check for expiring certificates
- Generate certificate signing requests
- Replace expiring certificates
- Combine multiple operations into a workflow
- Export certificates*

- *easy, high-impact use case

The big one…

- What if we could autoenroll with a CA?
- It would help solve some high impact problems
- But it’s not trivial to implement…

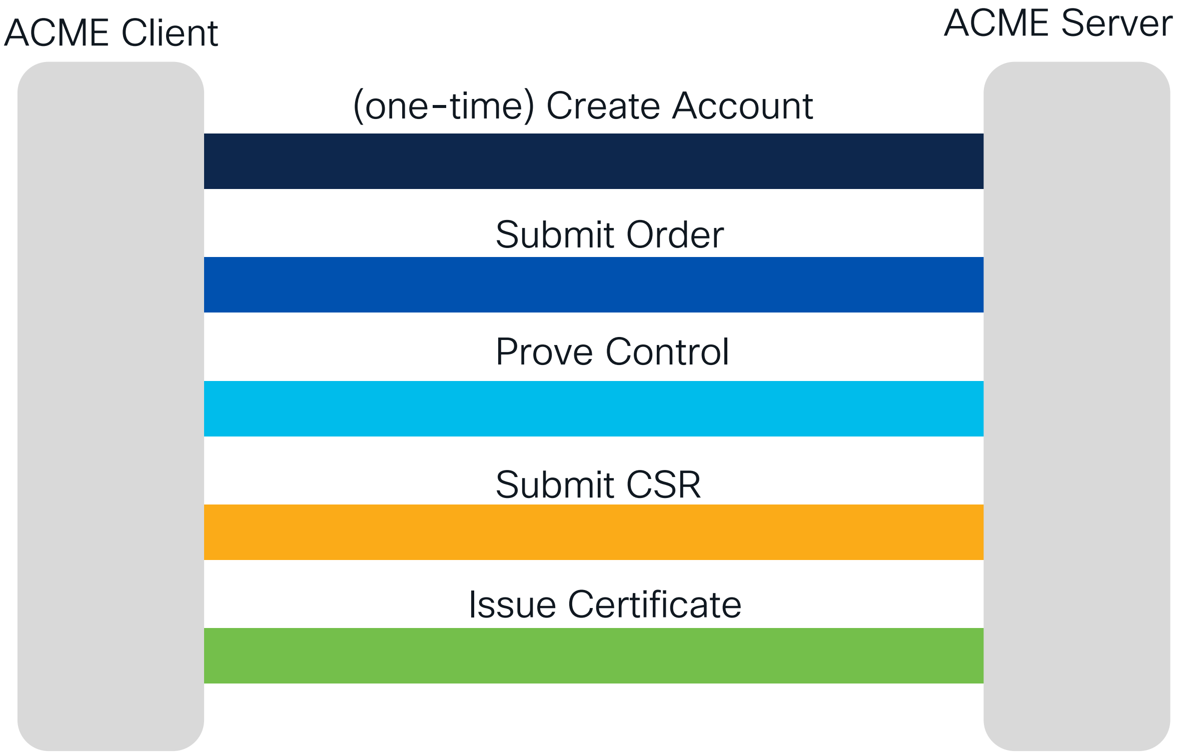
Enrollment Protocols

Automatic Certificate Management Environment

Also known as ACME

- Originally developed for Let’s Encrypt
- Gaining traction as an open standard
- Automates processing of Domain Validation certificates
- RFC 8555
- Uses challenge-based authentication
  - “prove to me you control this domain”
- Challenge portion is extensible
  - Currently only DNS-01 and HTTP-01 are widely supported

ACME



ACME Client

ACME Server

(one-time) Create Account

Submit Order

Prove Control

Submit CSR

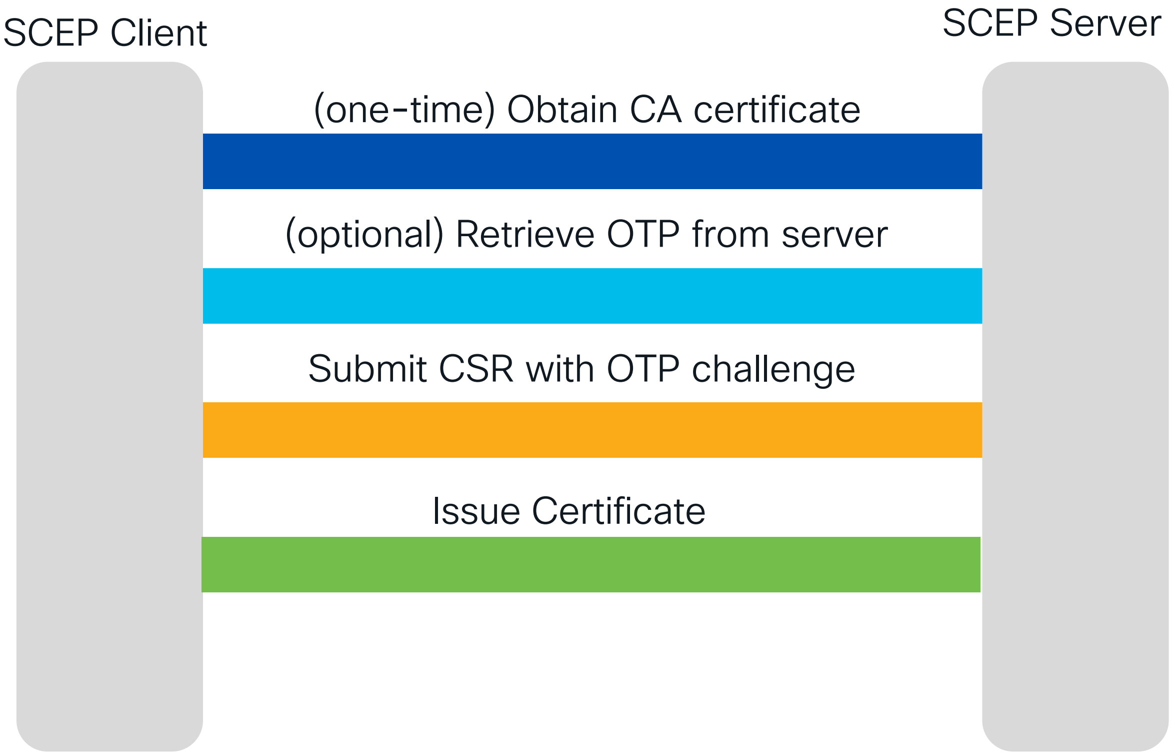
Issue Certificate

Simple Certificate Enrollment Protocol

Also known as SCEP

- Developed by Cisco!
- De facto standard for device certificate enrollment
- Uses commands sent as operation= URL parameter
- RFC 8894
- Popularized by the Microsoft NDES service shipping since 2008
- Used by Intune for onboarding Windows devices
- Authentication combination of OTP and PKCS #7 envelope

SCEP



SCEP Client
SCEP Server
(one-time) Obtain CA certificate
(optional) Retrieve OTP from server
Submit CSR with OTP challenge
Issue Certificate

SCEP vs ACME

Which one do I use?

- ACME is more modern
  - Uses JSON for messaging
  - Private key used to sign CSR is not required to submit request
- Active Directory Certificate Services doesn't support ACME directly
  - But there are proxies available (prepare to get your hands dirty though)
- SCEP is directly supported by ADCS
  - Limitation of one template per NDES server
- SCEP can't use ISE-generated CSRs
  - Do everything outside of ISE and import the cert + private key

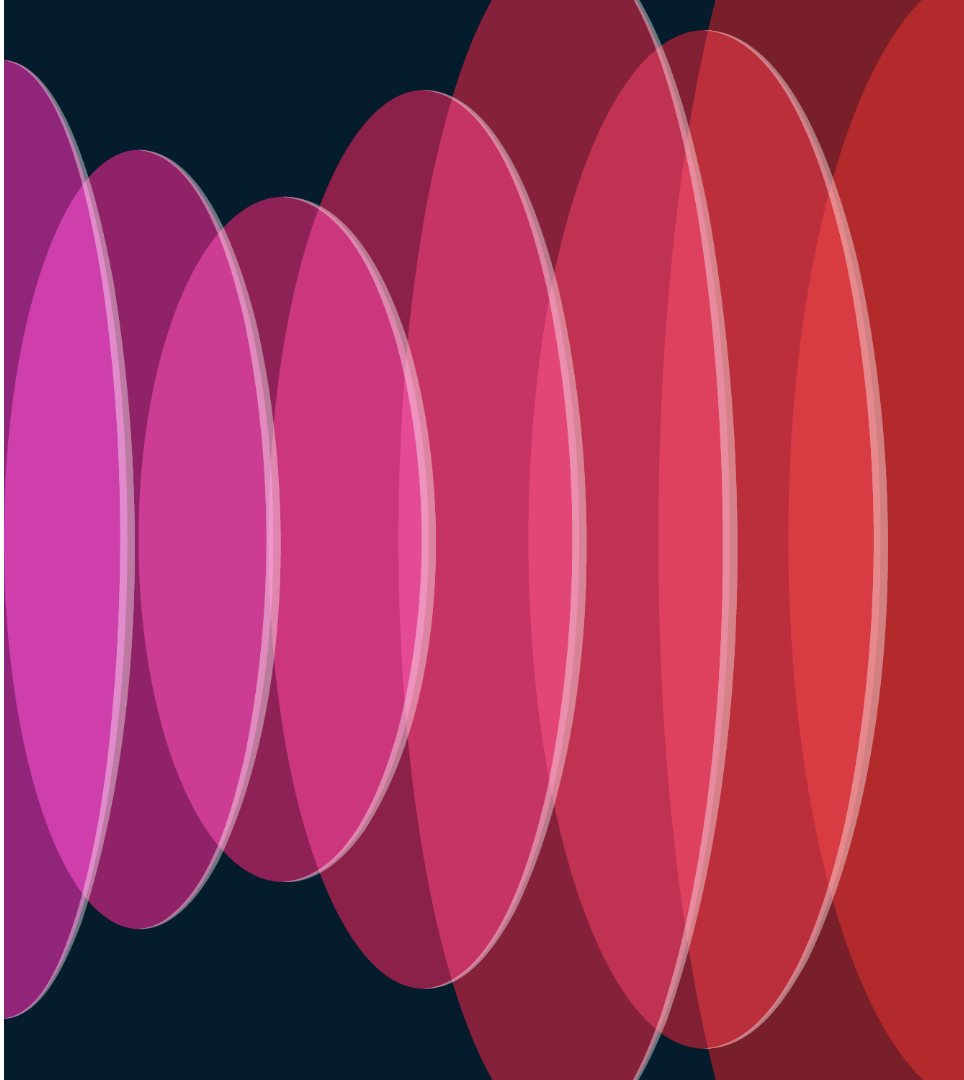
Wait – why use ADCS? Letsencrypt is free!!

- All publicly issued certificates are logged
- Certificate transparency project (for detecting compromised CAs)
- RFC 9162
- Bad idea to use it for internal certificates
  - Allows attackers to enumerate your internal infrastructure
- Have some fun with this: https://crt.sh/

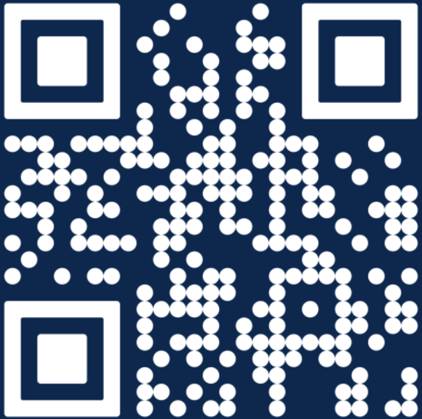
Bottom Line:

- Autoenrollment is not easy
- But it can be done!

Demo



Link to the demo source code



SCAN ME

Wrap up

Key Takeaways

- Understand what you're automating
  - PKI requirements depend on use case
  - Some operations can be service affecting
- Automating enrollment – ACME vs SCEP
  - Each has its tradeoffs
  - Protect the private key
- Resources to develop and test your code
  - Sample code used in this talk:
    - https://github.com/srmcnutt/devnet-2140
  - DEVNET sandboxes (search for ISE in the sandbox catalog)

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: www.linkedin.com/in/smcnutt

cisco Live!
DevNet

Continue your learning journey after the event with Cisco DevNet!

- Personalized learning modules
- Live interactive tooling
- Other resources

Scan to get started

The bridge to possible

Thank you

#CiscoLive