

The background features a vibrant, multi-colored abstract design. On the left, there are overlapping, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Using ISE OpenAPI to automate certificate management

Steven McNutt, Cybersecurity Technical Solutions Architect, CCIE# 6495
@densem0de

DEVLIT-1220

CISCO *Live!*

#CiscoLive

Agenda

- Introduction
- ISE API Primer
- ISE System certificates
- ISE certificate management API
- 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 related tasks traditionally performed manually.
- New APIs provide an opportunity to automate these tasks
- Reduces effort and risk

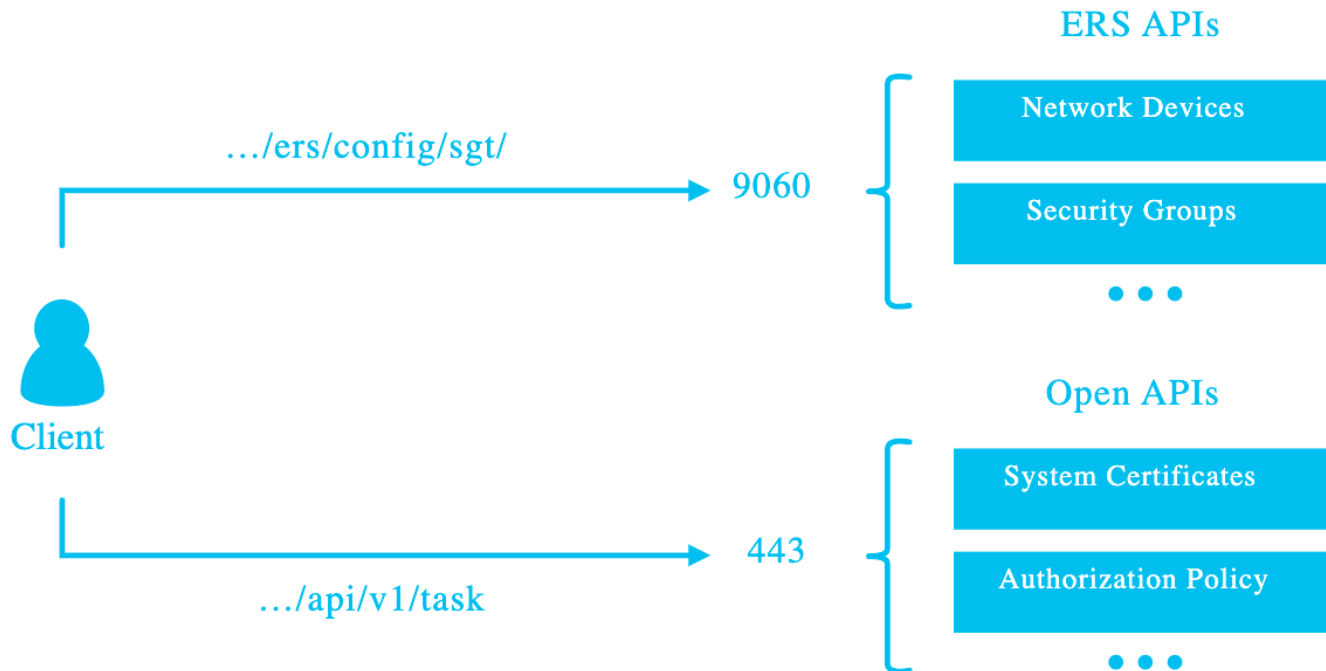
ISE API Primer

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:

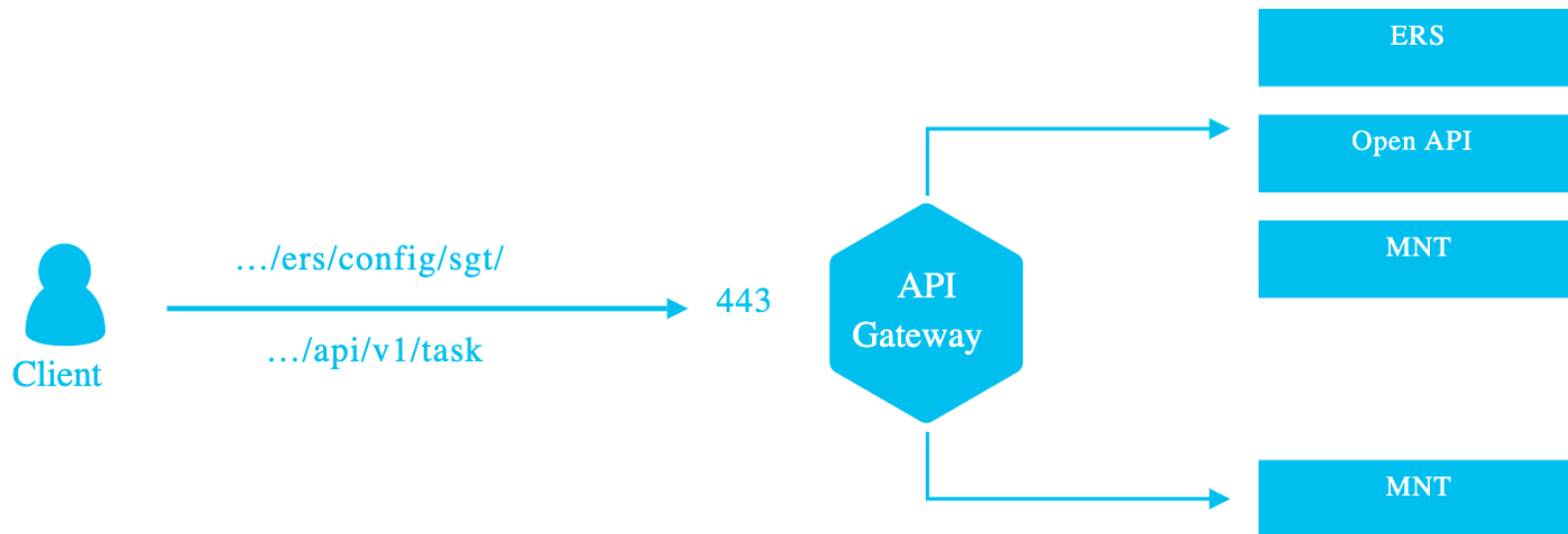


ISE API Gateway

- 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

Cisco ISE

Administration · System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access **Settings**

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings

Posture >

Profiling

Protocols >

Endpoint Scripts >

Proxy
SMTP Server
SMS Gateway
System Time

API Settings

API Settings

Overview **API Service Settings** API Gateway Settings

✓ API Service Settings for Administration Node

☒ ERS (Read/Write)

☒ Open API (Read/Write)

✓ 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:

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration · System' (1), 'Admin Access' (2), and 'Settings'. The left sidebar has 'Admin Groups' (3) selected. The main content area is titled 'Admin Groups' and features a table (4) with the following data:

<input type="checkbox"/>	Name	External Groups Mapped	Description
<input type="checkbox"/>	Customization Admin	0	Access Permission to Guest Menu and Device Portal Manage...
<input type="checkbox"/>	ERS Admin	0	Full access permission to External RESTful Services (ERS) A...
<input type="checkbox"/>	ERS Operator	0	Read-only access permission to the External RESTful Servic...

Below the table are action buttons: Edit, + Add (5), Duplicate, Delete, and Reset All Ext. groups.

Example call

```
~ curl -ku "admin: " 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

There's an extensive set of APIs

Focus on what's relevant for the task at hand

Common tasks:

- Get the System Certificate list
- Check for expiring certificates
- Export Certificates*

*easy, high-impact use case



Demo

CISCO *Live!*

Wrap up

Key Takeaways

- Understand what you're automating
 - PKI requirements depend on use case
 - Some operations can be service affecting
- Resources to develop and test your code
 - Sample code used in this talk:
 - <https://github.com/srmcnutt/devlit-1220>
 - <https://github.com/srmcnutt/ise-t>
 - DEVNET sandboxes (search for ISE in the sandbox catalog)

Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Game** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive