



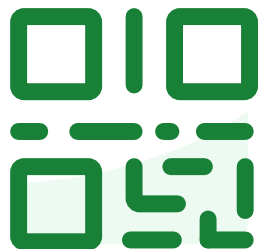
# Mastering ISE Upgrades

Best Practices, Tips and Tricks

Romain Passerel - Security Consulting Engineer  
BRKSEC-2889

slido

Please download and install the  
Slido app on all computers you  
use



Join at [slido.com](https://slido.com)  
#2889

① Start presenting to display the joining instructions on this slide.



# Agenda

- Introduction
- Pre-Upgrade Checklist
- Perform Upgrade Steps
- Common Concerns
- Conclusion & Q&A

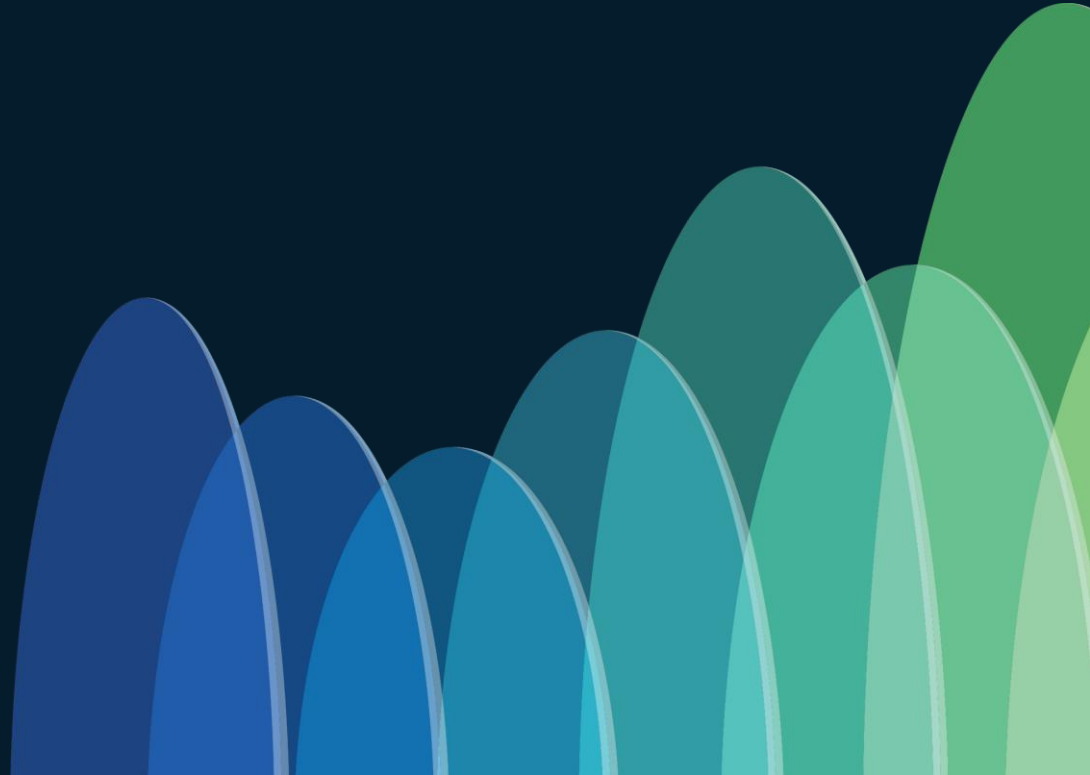
# About Romain PASSEREL

#whoami

- Security Consulting Engineer
  - Joined Cisco in September 2020
- Providing Security Professional Services (PS) for CX
  - Specialized on ISE, Secure Firewall, ASA and Secure Client
  - Experience in automation and cloud services (Umbrella, Duo, XDR,...)
- Notable achievement :
  - Designed and Supported the Olympics Project
- Fan of music and aviation!



# Introduction



# Review of ISE Personas



## Policy Administration Node – PAN



Central node for managing **configurations**

- PPAN – Primary PAN (Active)
- SPAN – Secondary PAN (Standby)

## Monitoring Node – MNT



Collects *operational data* and logs.

- PMNT – Primary MNT (Active)
- SMNT – Secondary MNT (Active)

## Policy Service Node – PSN



Executes policies and handles client authentications.

# Understanding the ISE Log File System

ISE generates various log files to help monitor and troubleshoot system performance and issues.

## 1. ADE.log (Application Deployment Engine)

- **Details:** Captures main system-level events and processes, useful for tracking upgrades, patch processes, and system errors.
- **Usage:** `show logging system ade/ADE.log`

## 2. ise-psc.log (Policy Service Component)

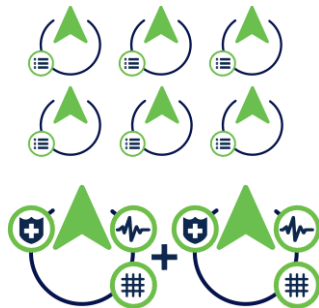
- **Details:** Focuses on internal processes and application-specific events, including errors and warnings related to policy execution and service configurations.
- **Usage:** `show logging application ise-psc.log`

# Reminders

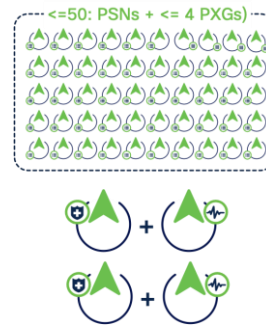
## Types of Deployments



Small Deployment  
2 x PAN + MNT + PSN  
(Optional additional PSN)



Medium Deployment  
2 x PAN + MNT  
Up to 6 PSNs



Large Deployment  
2 x PAN  
2 x MNT  
Up to 50 PSNs

 [cs.co/ise-scale](https://cs.co/ise-scale)



# Reminders

## ISE platforms



SNS 3615

SNS 3655

SNS 3695



SNS 3715

SNS 3755

SNS 3795



Traditional VM

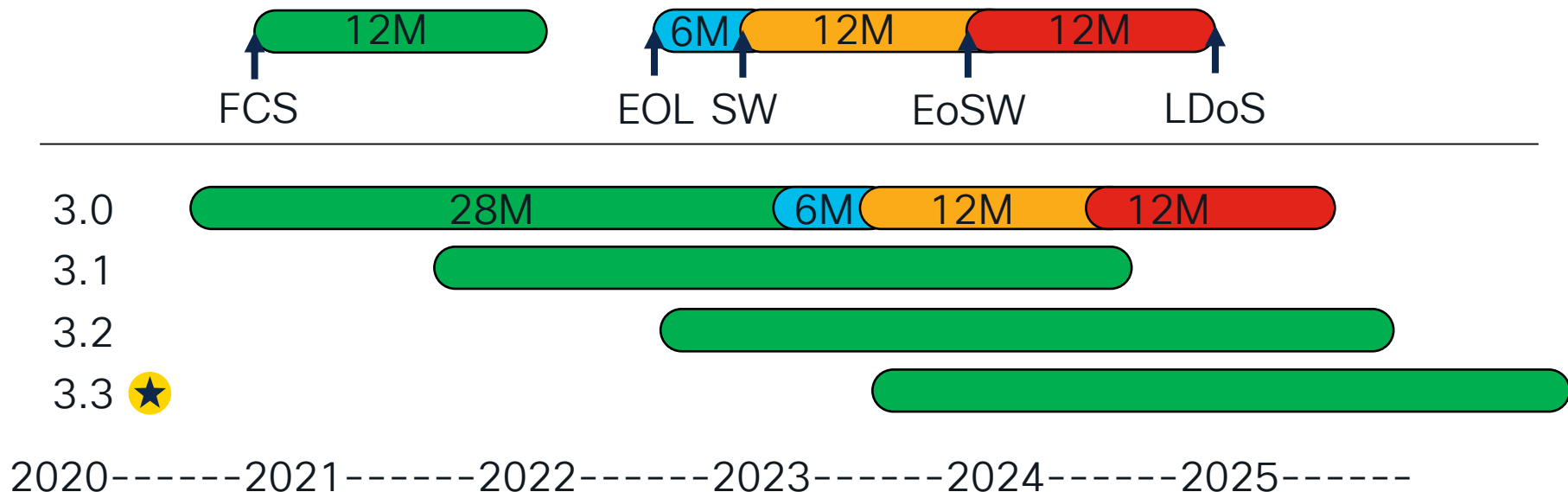
AWS

Azure & OCI



# ISE Lifecycle

- All versions are entitled to the same lifecycle
- New versions are typically released approximately every 12 months



# Reasons to Upgrade

- Enhance Product Stability
- Fix Security Vulnerabilities
- Support and Maintenance
- and...

# New Features !



## • ISE 3.2 new features :

- Data Connect
- Better automation
- Cloud support
- pxGrid Direct
- Dark mode

## • ISE 3.3 new features :

- Certificate based API calls
- AI powered profiling
- Native IPsec
- New split-upgrade workflow

## • ISE 3.4 new features :

- Configure VTI with Native IPsec
- TLS 1.3
- PAC-less RADIUS for Trustsec
- Many improvements



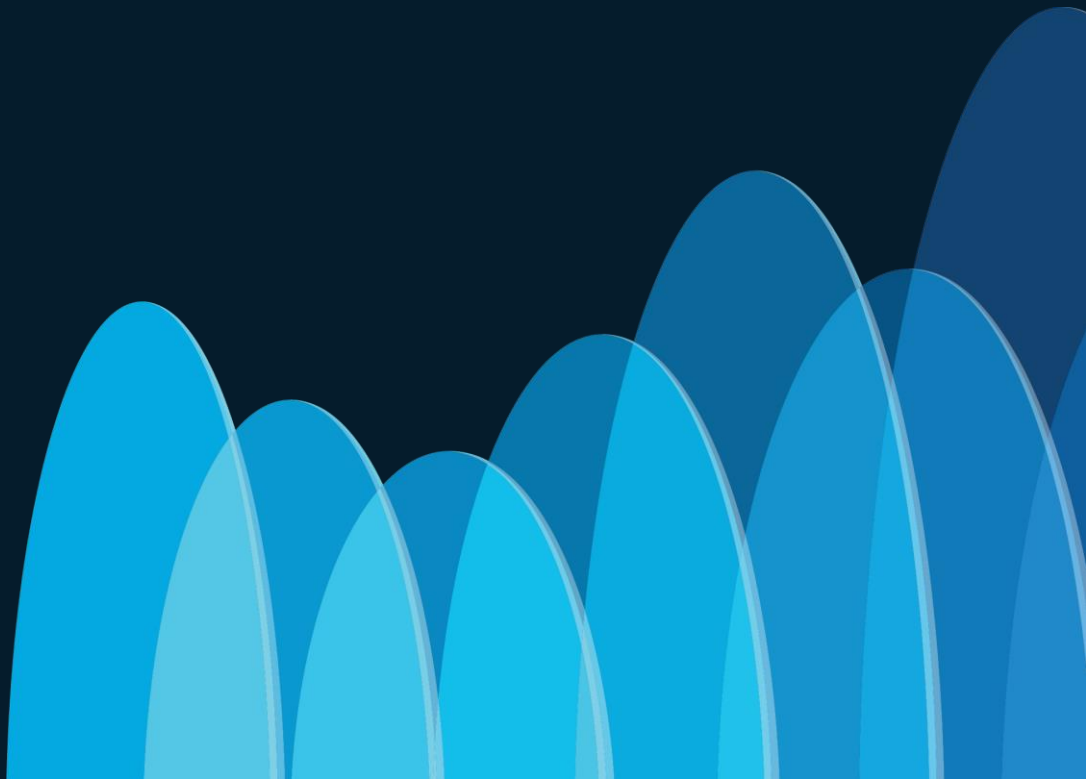
# What is your one-word opinion on ISE upgrades?

① Start presenting to display the poll results on this slide.

Upgrading ISE is not  
easy, unless you are  
well prepared!



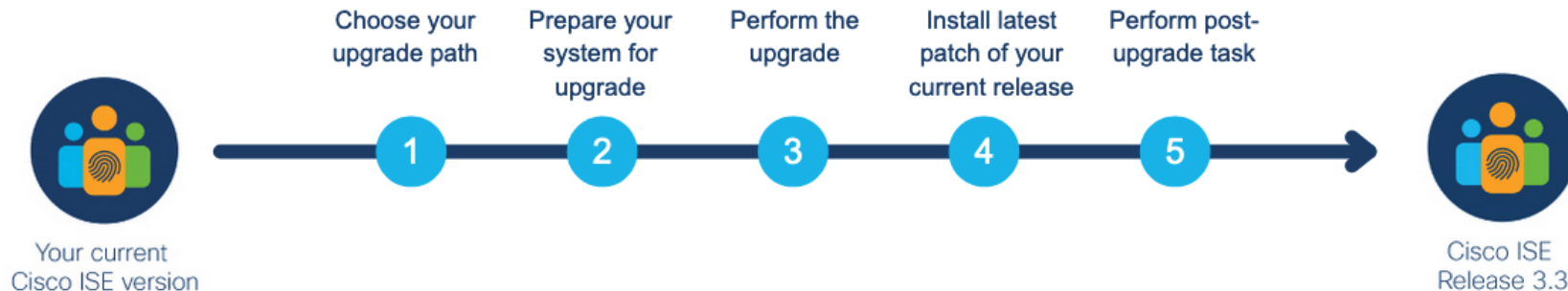
# Pre-Upgrade Checklist



# Cisco Official Documentation

## Your Cisco ISE Upgrade Journey

*Click on each step to follow the upgrade process*




[Cisco Identity Services Engine Upgrade Journey, Release 3.3 - Cisco](#)



# Prepare The Upgrade – Checklist

## Important tasks :

- Choose the target version : ...
- Check the suggested release 
- Review compatibility (Hardware, Integrations)
- Validate Licensing  
[Cisco ISE Licensing Guide – Cisco](#)
- Review Open Bugs :
  - [Bug Search Tool](#)
- More detailed recommendation:
  - Engage Cisco CX Services

# Prepare The Upgrade – Checklist

## Important tasks :

- Choose the target version : ...
  - Validate Upgrade Path : Direct / Two-Step



Two-step upgrade : Perform the biggest jump first

# Prepare The Upgrade – Checklist

## Important tasks :

- Choose the target version : ...
  - Validate Upgrade Path : Direct / Two-Step
- Install latest patch (**before** and after)

### Patch from GUI :

- First node be patched is PPAN
- Following nodes are patched in **alphabetical** order one after the other.

### Patch from CLI:

- You can test the patch on any node before deploying to the rest of the deployment.
- You can patch nodes simultaneously !

# Tips : Waiting for ISE Application Server to run

- After patching, upgrading, or installing, ensure the ISE Application Server is running. Use the command : *show application status ise* or check the **ise-psc.log** file to verify the server status.

```
#screen-length 0 !// replacing 'terminal length 0' since ISE 3.2
#show logging application ise-psc.log tail | include "Application Server"
```

```
2024-11-22 13:50:18,483 INFO [Infra-UpdateNICVersion-Thread][[]]
cisco.cpm.infrastructure.systemconfig.UpdateNICPatchVersion -:::- stdout :
Application Server initializing
```




```
2024-11-22 13:50:29,028 INFO [Infra-UpdateNICVersion-Thread][[]]
cisco.cpm.infrastructure.systemconfig.UpdateNICPatchVersion -:::- stdout :
Application Server running 22816
```

# Prepare The Upgrade – Checklist

## Important tasks :

- Choose the target version : ...
  - Validate Upgrade Path : Direct / Two-Step
- Install latest patch (**before** and after)
- Choose your upgrade method : .....

# Choose your Upgrade Method

Backup & Restore 		GUI 		CLI 
Recommended Method	Split Upgrade	Full Upgrade	TAC preferred	
Reinstall all nodes to the new version using installation ISO.	Step-by-step guide	Added 2.6P10, 2.7P4, 3.0P3	Advanced knowledge of ISE upgrade needed	
Configuration backup is restored on SPAN. Data is replicated between nodes.	Starting 3.2P3 and 3.3 allowing to upgrade more nodes simultaneously in iterations: <b>New Split Upgrade.</b>	Two steps upgrade: 1. PPAN 2. All other nodes	Better visibility and control over the upgrade.	
Only option available for Cloud Instances.	Include pre-checks	No persona change !	Usually used if failed GUI upgrade	
Best for large deployments to optimize upgrade duration (Fastest method)	Great for small and medium deployment	Faster approach but <b>downtime required</b>	Best for distributed deployment across multiple regions	

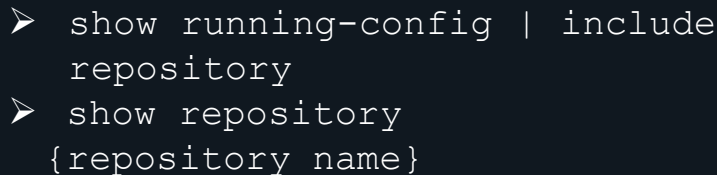
# Prepare The Upgrade – Checklist

## Important tasks :

- Choose the target version : ...
  - Validate Upgrade Path : Direct / Two-Step
- Install latest patch (**before** and after)
- Choose your upgrade method : .....
- Set up and validate repository

Make sure they are accessible and **as close as possible** from the ISE nodes.

Validating repositories through CLI on all nodes :



```
➤ show running-config | include repository
➤ show repository {repository_name}
```

# Tips: Using the local disk as repository

You can use the Local Disk (disk) to store URT, Upgrade bundle or ISO Installation file.

- Configure the repository from GUI :
- Use the `copy` command on CLI to copy files to the local disk or use GUI !
- Use the `dir` command to list the files on the local disk or check the free space.

[Repository List](#) > Add Repository

## Repository Configuration

\* Repository Name

\* Protocol

Location

\* Path

Submit



Since ISE 3.1, manage local disk files from the GUI !  
(Admin-System-Maintenance)

Navigation: Cisco ISE Administration · System

Menu: Deployment Licensing Certificates Logging **Maintenance** Upgrade

Sub-menu: Patch Management Repository Operational Data Purging **Localdisk Management**

### Files

Files from the table below will be used for Localdisk Management. The files must be downloaded or deleted one at a time. Folder can

Buttons: Refresh Upload Download Delete



# Prepare The Upgrade – Checklist

## Important tasks :

- Choose the target version : ...
  - Validate Upgrade Path : Direct / Two-Step
- Install latest patch (**before** and after)
- Choose your upgrade method : .....
- Set up and validate repository
- Run the URT
  - optional for New Split Upgrade and Full Upgrade

## Upgrade Readiness Tool

- Runs on SPAN (*application install {URT} {repository}*)
- Verifies that **configuration** DB is compatible with new version.
- Provide an estimate for upgrade duration per node (Does not apply to B&R)

# How to estimate your upgrade duration ?



\*Disclaimer: Estimated timings subject to environment specifics

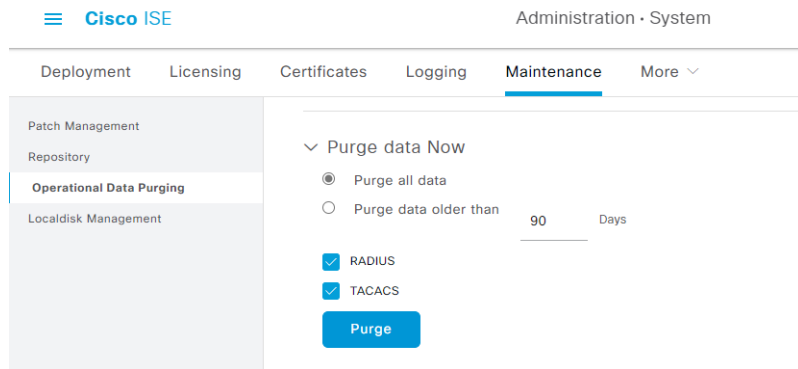


Improving the upgrade duration can be achieved by cleaning endpoints, users, and logs.

Operation	Estimated duration
Reimaging ISE	60-70 minutes
Restoring a configuration backup (PPAN)	40-60 minutes*
Register node into cluster	20-30 minutes*
Upgrading a node	70-120 minutes*
Upgrading operational data (MNT)	<u>5 mins / GB of operational data</u>
Patching	20-30 minutes
Persona change	15 minutes

# How to reduce upgrade duration (except B&R)

- You can purge MNT node operational data using the 'Purge data Now' option in the ISE GUI.
- Operational data logs are not synchronized between the MNTs in case of a persona change !



Use the following CLI command to purge logs on the node :

```
# application configure ise
[... ] [3]Purge M&T Operational Data [... ]
# 3
[... ] Enter days to be retained: 1
```

# Prepare The Upgrade – Checklist



## Important tasks :

- Choose the target version : ...
  - Validate Upgrade Path : Direct / Two-Step
- Install latest patch (**before** and after)
- Choose your upgrade method : .....
- Set up and validate repository
- Run the URT
  - optional for New Split Upgrade and Full Upgrade
- Backup Configuration !
  - Optional Operational data backup.
    - If not required export and purge.
- Backup
  - Network devices, endpoints (.csv)
  - Export certificates and private keys
  - Export internal CA certificates from CLI
- Take notes
  - AD Credentials, MDM credentials, and other similar credentials
  - Profiler configuration for each PSN
- Clean
  - Delete expired certificates
  - Purge operational data, inactive endpoints and guest accounts
- Do not forget
  - **Perform Health Checks** (since 2.6P8+)
  - Disable PAN Failover & Scheduled Backup



Which upgrade method preserves the existing persona configuration throughout the process?

① Start presenting to display the poll results on this slide.

Upgrading ISE is not  
easy, unless you are  
well prepared!



Cruising altitude  
checklist | Jeffery Wong

# Perform Upgrade Steps



# Before That : understanding the upgrade

- Old deployment



PPAN - SMNT  
PSN



SPAN - PMNT  
PSN



- New deployment



# Before That : understanding the upgrade

- Old deployment



PPAN – SMNT  
PSN

- New deployment



SPAN – PMNT  
PSN

# Before That : understanding the upgrade

- Old deployment



PPAN – SMNT  
PSN



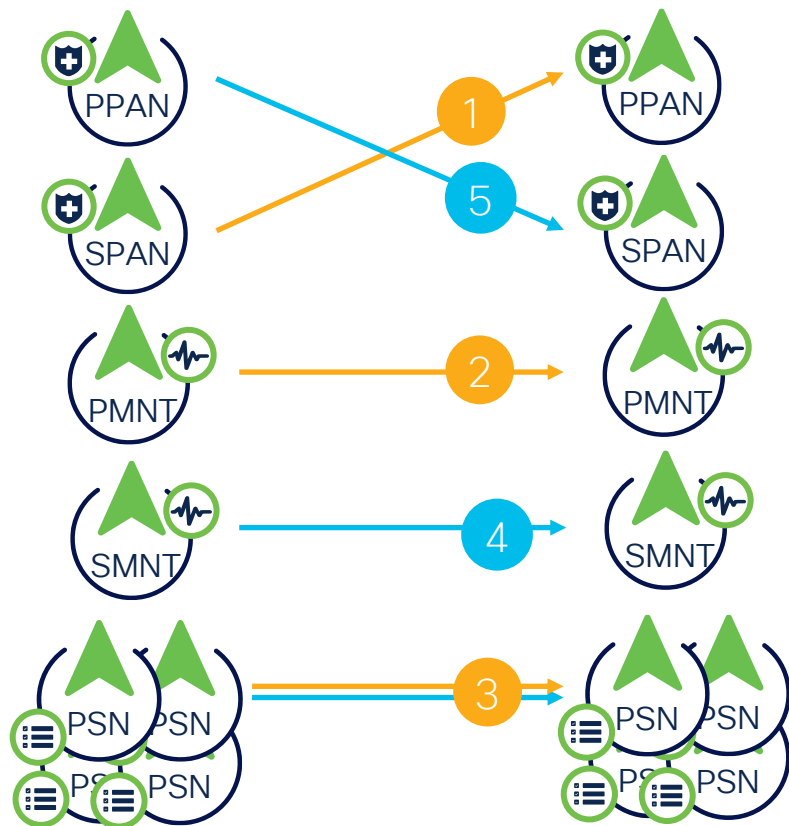
- New deployment



PPAN – PMNT  
PSN

Upgrading an ISE cluster consists of creating a new cluster in the targeted version.

# Recommended Upgrade Sequence – 5 steps



1. SPAN → PPAN
2. PMNT → PMNT  
(no persona change)
3. PSNs → PSNs  
(Take as many steps as needed to avoid impacting services.)
4. SMNT → SMNT
5. PPAN → SPAN



MNTs and PSNs can be upgraded at the same time !

# Tips : Reimaging ISE nodes

- For faster parallel ISE reinstallation on multiple VMs, use the ISO image instead of the OVA.
- Ensure the ISO is located close to the server to minimize installation delays, particularly when using a mounted ISO over CIMC KVM.



Localized ISE Installation (3.1P9, 3.2P5, 3.3P3, 3.4)

- Copy ISO to local disk
- application configure ise
- [36]Localised ISE Install

→ Faster reimage timings for VMs and Appliances !

# Performing the upgrade - Checklist



- Plan maintenance windows and inform about possible downtime
- Open a TAC proactive case
- Follow a documented procedure (CX Professional services assistance available)

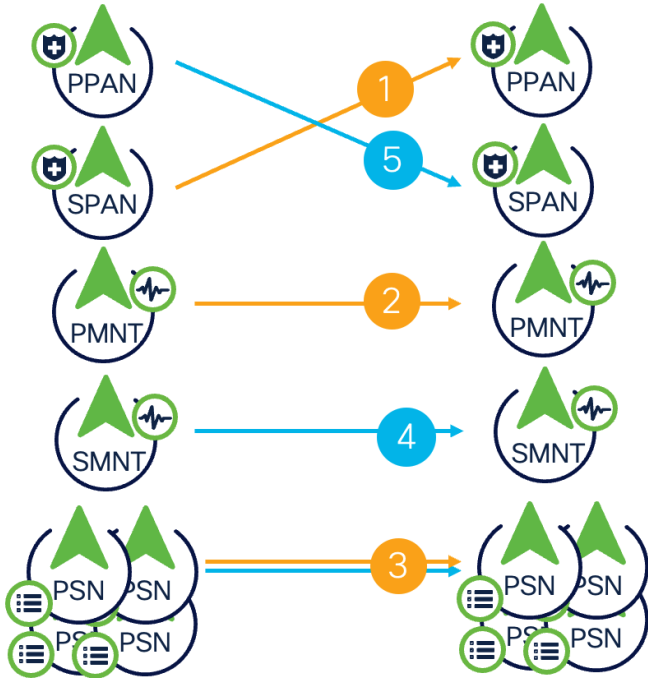
Backup & Restore	GUI	CLI
Follow the upgrade sequence: 1. Deregister the node 2. Reimage the node 3. <b>(optional) Patch</b> 4. Restore on 1st node / Join 5. Test / Verify 6. Repeat	Follow the steps from the guide : 1. Select the nodes 2. Upgrade Nodes 3. Test / Verify 4. Repeat	Follow the upgrade sequence: 1. Upgrade the node ( <i><b>using Console terminal</b></i> ) 2. Test / Verify 3. Repeat <b>Do not patch until all the nodes are upgraded !</b>



Warning for Large Deployments on Persona changes (see next slide)

# Persona Changes on Large deployments

- Each Deployment needs to contain a least one MNT.



- After step 1, MNT persona will automatically be enabled on new PPAN

→ Before step 4, disable MNT persona on new PPAN.

- Old PPAN cannot be alone in old deployment with no MNT.

→ Before step 4, MNT persona needs to be enabled on old PPAN

- Steps automatically included using GUI upgrades.

# How to monitor the upgrade process ?

- All operations linked to the upgrade process will be detailed in the ADE log file. After STEP 10, the node will reboot.

```
> show logging system ade/ADE.log tail | include STEP
```

```
info:[application:install:upgrade:preinstall.sh] STEP 0: Running pre-checks
info:[application:operation:preinstall.sh] STEP 1: Stopping ISE application...
info:[application:operation:preinstall.sh] STEP 2: Verifying files in bundle...
info:[application:operation:isedbupgrade-newmodel.sh] STEP 3: Validating data before upgrade...
info:[application:operation:isedbupgrade-newmodel.sh] STEP 4: De-registering node from current deployment.
info:[application:operation:isedbupgrade-newmodel.sh] STEP 5: Taking backup of the configuration data...
info:[application:operation:isedbupgrade-newmodel.sh] STEP 6: Registering this node to primary of new deployment...
info:[application:operation:isedbupgrade-newmodel.sh] STEP 7: Downloading configuration data from primary of new deployment...
info:[application:operation:isedbupgrade-newmodel.sh] STEP 8: Importing configuration data...
info:[application:operation:isedbupgrade-newmodel.sh] STEP 9: Running ISE configuration data upgrade for node specific data...
info:[application:operation:isedbupgrade-newmodel.sh] STEP 10: Running ISE M&T database upgrade...
info:[application:install:upgrade:post-osupgrade.sh] POST ADEOS UPGRADE STEP 1: Upgrading Identity Services Engine software...
info:[application:operation:post-osupgrade.sh] POST ADEOS UPGRADE STEP 2: Importing upgraded data to 64 bit database...
```

# Failures Remediation using upgrade



## SPAN Upgrade Failure :

- Failure before reboot :

→ Node will automatically join back the old deployment. Do not continue the upgrade

- Failure after reboot :

→ Reimage the node and join back the old deployment

## Non-PAN Upgrade Failure :

- Failure before reboot :

→ Automatically joins back the old deployment.

Check with TAC or Reimage and join the **NEW** deployment

- Failure after reboot :

→ Reimage the node and join the **NEW** deployment

## PPAN Upgrade Failure :

- Failure before/after reboot :

→ Reimage and join the new deployment as SPAN



# Post Upgrade – Checklist



- Review the Post-Upgrade Task – [link](#) :

(each task is optional depending on your environment)

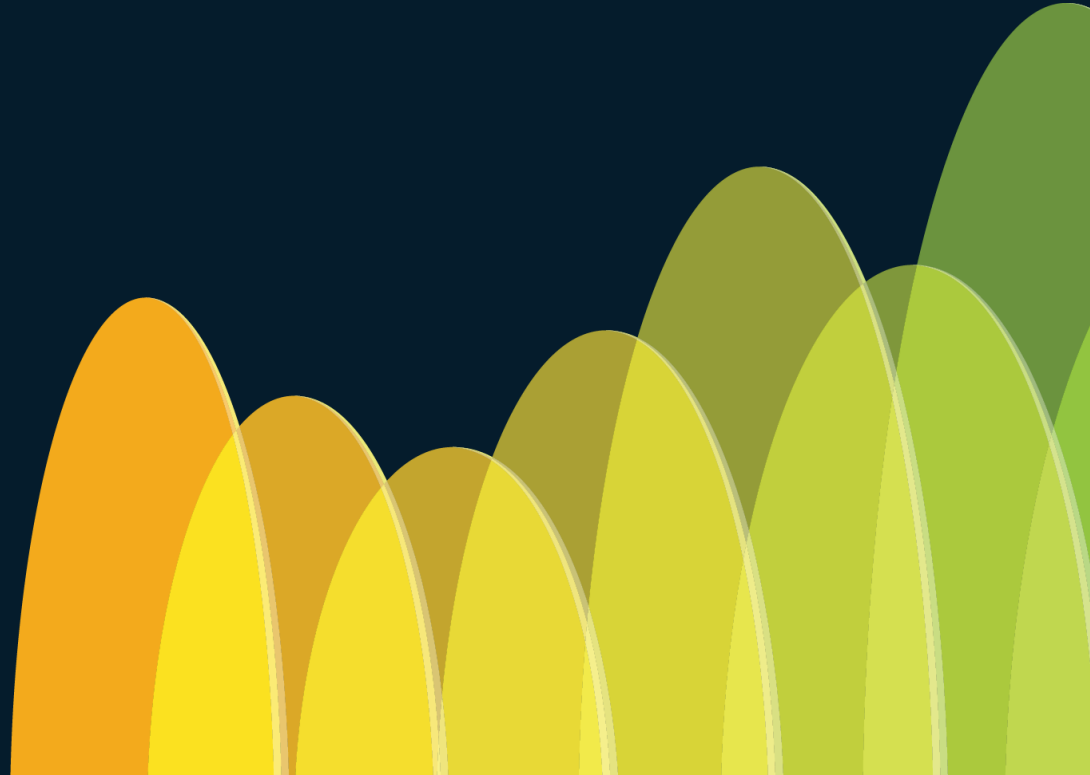
- Re-Join Active Directory
  - Check / Regenerate Root CA
  - Update virtual machine guest operating system / Upgrade BIOS and CIMC for SNS appliances
  - Restore Operational Data
  - Update Profiler Feed Service
  - Verify Licenses are valid
  - Refresh DB Statistics on MNT
- If not perform yet : **Install Latest Patch** – [link](#)



# What commands are helpful during an upgrade process?

① Start presenting to display the poll results on this slide.

# Common Concerns




# Why Backup & Restore is recommended ?

- **Reduced Error Risk:**
  - During reimaging, the disk is completely wiped, minimizing errors.
- **Faster Upgrade Process:**
  - There is no need to wait for the SPAN upgrade before upgrading other nodes, significantly shortening the upgrade time.

## CLI or GUI upgrades steps

1. SPAN
2. Other nodes
3. PPAN

 This approach is susceptible to **human errors**, such as incorrect IP addresses or hostnames during setup, which can extend the upgrade duration.

# Can I upgrade ISE clusters in stages over time?

- **Yes**, you can upgrade ISE clusters in multiple operations. Here are key points to consider:
  - Patch is recommended for production :
    - Patch installation can only be done using Backup & Restore or GUI **New split upgrade method** (3.2P3+).
  - Some Operational Data generated might be lost after upgrade :
    - You can configure external syslog servers on ISE to redirect logs to 3rd party solution like Splunk : [Cisco ISE Integration with Splunk](#)



# Is it possible to mix CLI and Backup & Restore ?

- Yes it is possible to mix some upgrade methods.
- One common scenario seen is :
  - SPAN and PMNT are upgraded
  - PSNs and the rest of the nodes are reimaged and added to the cluster.



# Upgrading with Catalyst Center Integration ?

- Catalyst Center is integrated with PPAN so it will stay integrated to the old cluster until the last node is upgraded.
- You may need to configure static AAA servers in Catalyst Center to point to IPs of your upgraded PSNs to test them on specific sites.

Settings / External Services

## Authentication and Policy Servers

Use this form to specify the servers that authenticate Catalyst Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[Add](#) [Export](#)

### Add AAA server ×

Server IP Address\*

Shared Secret\*

- You may need to refresh integration when all the ISE nodes are upgraded. ([Reintegrate Cisco ISE with Cisco Catalyst Center](#))



# Personal Advice : Test before upgrade

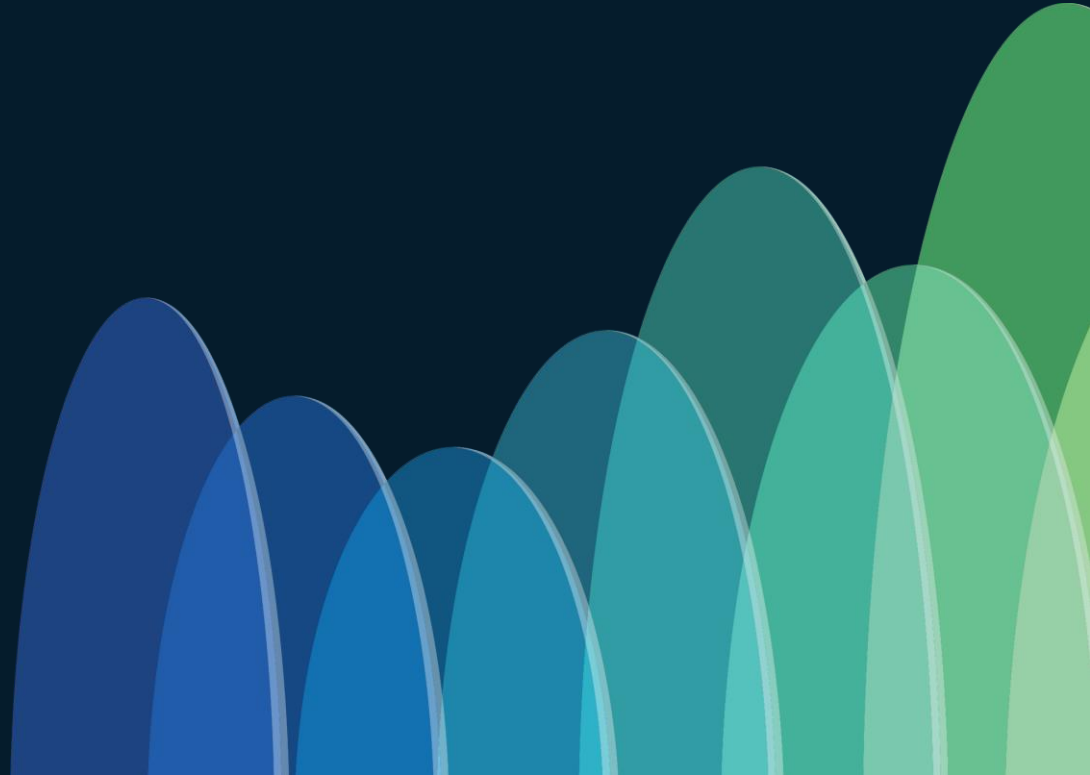
- To avoid discovering an issue after the upgrade is performed
- Test your configuration with new version
  - Generate a configuration backup
  - Set Up a new ISE or reimage a not used PSN to the targetted version
  - Install latest patch available
  - Restore your configuration on this test node.
  - Perform some authentication tests of all your use-cases.



# *Congratulations!*

You've Successfully Upgraded Your ISE Deployment.

# Conclusion & Q&A



slido

Please download and install the Slido app on all computers you use



## Audience Q&A

① Start presenting to display the audience questions on this slide.

# Conclusion

No magic trick to master an ISE Upgrade

- Plan and prepare
- Verify and test
- Utilize Cisco CX services, proactive TAC engagement

Upgrading ISE is not easy, unless you are well prepared!



Source: NASA

# Webex App

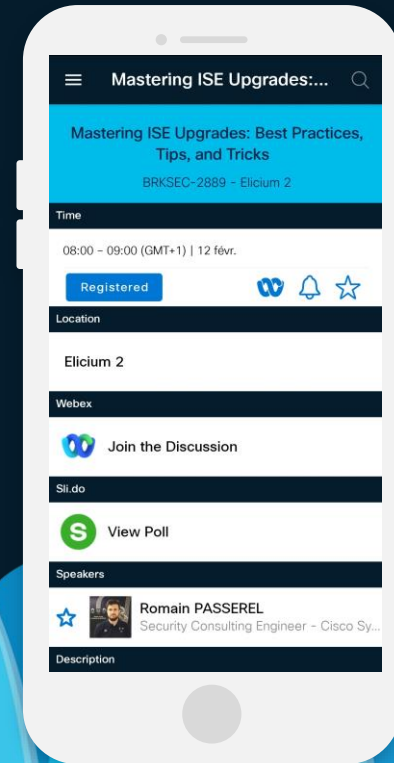
## Questions?

Use the Webex app to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Events 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 February 28, 2025.



# Continue your education

CISCO *Live!*

- Check out other ISE sessions :  
<https://www.ciscolive.com/emea/learn/learning-maps/security/ise.html>
- Book your one-on-one  
Meet the Engineer meeting
- Experience the latest ISE version  
on dCloud.
- Reach out to your Cisco Account  
team to explore CX Professional  
Services.

Contact me at: [rpassere@cisco.com](mailto:rpassere@cisco.com)

# Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog





Thank you

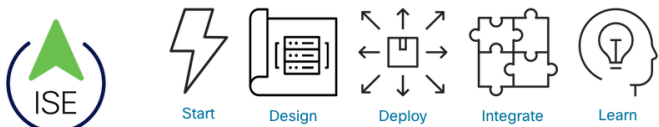
CISCO *Live!*



# ISE Resources

ISE BERG

## Cisco Identity Service Engine (ISE) Big Encyclopedic Resources Guide (BERG)



<https://cs.co/ise-berg#tag>

Use a hashtag in the shortcut URL with the name of any tag/topic you want to jump straight to it! Feature, protocol, vendor, product, anything! You may always use your browser's search feature to find all occurrences of something in the page, too. Available tags:

42Gears | AAD | Absolute | Ac  
Alef | Amazon | AMP | analytic:  
Aruba | ASA | Asimily | ASR | /  
CC | CCC | CCV | Certege | ce  
CSC | CSE | CSM | CSTA | CT/  
deployment | developer | DevN  
| errors | ExtraHop | Extreme |  
HP | Huawei | Hyper-V | IBM |  
ipsec | Ipsk | ISE | Ivanti | JAMI  
balancing | log-analytics | logg  
EntraID | MicroTik | MobileIron  
| OCI | ODBC | Okta | operation  
PIC | Ping | PKI | PNG | policy |  
cloud | pxgrid-direct | pxGrid |  
Rockwell | RSA | Ruckus | SCC  
secure-workload | security | se  
Splunk | Stealthwatch | stencils:  
Tanium | TEAP | Tenable | Terr  
UCS | Umbrella | upgrade | spl  
wireless | WLC | Workload | W



ve-policy | AIEA | AirWatch |  
ppliance | Arista | Armis |  
atalyst | Catalyst-Center |  
nitive | compliance | CSA |  
nnect | DeceptionGrid |  
vam | ELK | EntraID | Envoy  
Good | Google | guides |  
adOS | iPhone | ip-phones |  
w | LiveAction | lb | load-  
FA | Meraki | Microsoft |  
| NGFW | Nozomi | Nutanix  
AP | pSense | phones | PI |  
i | PXGC | PXGD | pxgrid-  
ipid7 | repositories | REST |  
| secure-network-analytics |  
IS | SMTP | SNA | SOTI |  
| TACACS | TACACS+ |  
xting | trustsec | TrustSec |  
oomNavigator | windows |

- ISE Big Encyclopedic Resources Guide  
[cs.co/ise-berg](https://cs.co/ise-berg)
- ISE YouTube Channel  
[cs.co/ise-youtube](https://cs.co/ise-youtube)
- ISE Webinars  
[cs.co/ise-webinars](https://cs.co/ise-webinars)
- ISE Community  
[cs.co/ise-community](https://cs.co/ise-community)
- Does ISE Support My Network Device?  
[cs.co/ise-interop](https://cs.co/ise-interop)
- ISE Troubleshooting Tech Notes  
[cs.co/ise-troubleshooting](https://cs.co/ise-troubleshooting)
- ISE Licensing & Evaluations  
[cs.co/ise-licensing](https://cs.co/ise-licensing)

# Glossary



For Reference

- ISE – Identity **S**ervice **E**ngine
- PAN – **P**olicy **A**dministration **N**ode (**C**onfiguration)
- PPAN – Primary PAN
- SPAN – Secondary PAN
- MNT – **M**onitoring Node (**O**perational Data)
- PMNT – Primary MNT
- SMNT – Secondary MNT
- PSN – **P**olicy **S**ervice **N**ode
- SNS – **S**ecure **N**etwork **S**erver



- URT – Upgrade **R**eadiness **T**ool
- EOL – End Of Life
- VM – Virtual **M**achine
- GUI – **G**raphical **U**ser **I**nterface
- CLI – **C**ommand **L**ine **I**nterface
- AD – **A**ctive **D**irectory
- MDM – **M**obile **D**evice **M**anagement
- AWS – **A**mazn **W**eb **S**ervices
- OCI – **O**racle **C**loud **I**nfrastructure

CISCO *Live!*

GO BEYOND

The background of the slide features a series of overlapping, teardrop-shaped elements in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are arranged in a way that creates a sense of depth and movement, resembling a stylized mountain range or a series of waves. The overall aesthetic is clean and modern.