
cisco Live!
Let's go

The bridge to possible

Mastering ISE Upgrades

Best Practices, Tips and Tricks

Romain PASSEREL, Security Consulting Engineer

cisco Live!

BRKSEC-2889

Agenda

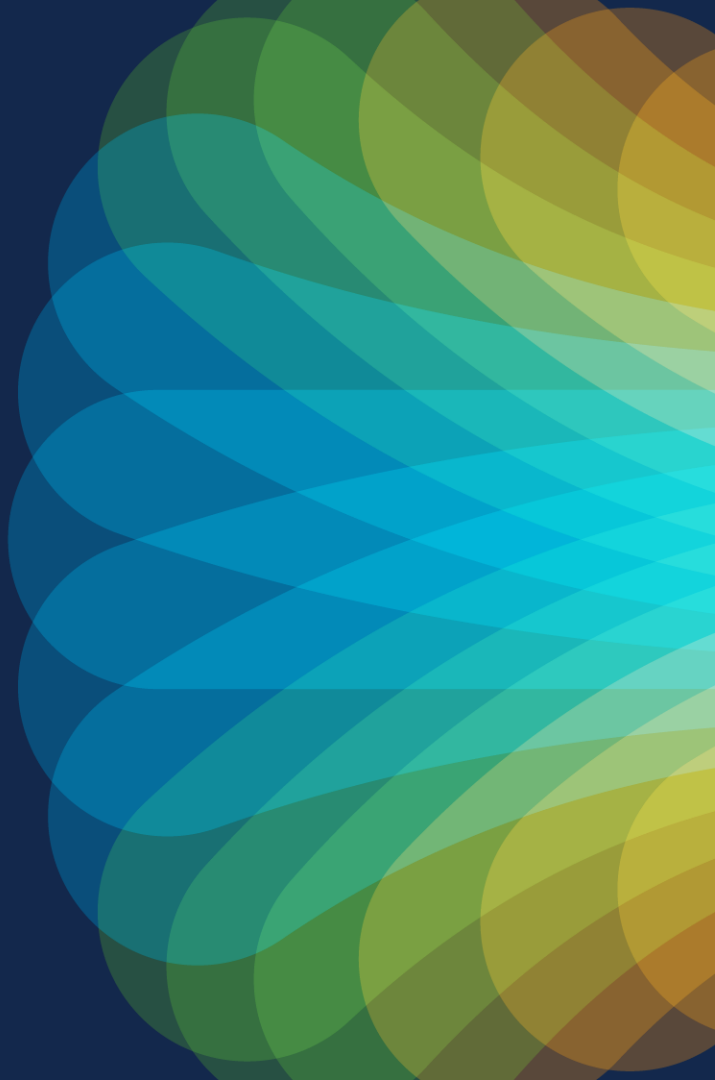
- Glossary & Reminders
- Why Upgrading ISE?
- Preparing the Upgrade
- Performing the Upgrade
- Conclusion

About Romain PASSEREL

#whoami

- Security Consulting Engineer
  - Joined Cisco in September 2020 (Graduate Program)
    - TAC rotation (4 months) in Krakow ISE Team
- Providing Security Professional Services (PS) for CX
  - Specialized on ISE, Secure Firewall (FMC, FTD), ASA and Secure Client
  - Experience in automation and cloud services (Umbrella, Duo, ..)
- Working on the Paris 2024 Olympic Project
- Fan of music and aviation!

Glossary & Reminders



Glossary

For Reference

- ISE – Identity Service Engine

- PAN – Policy Administration Node (Configuration)
  - PPAN – Primary PAN
  - SPAN – Secondary PAN

- MNT – Monitoring Node (Operational Data)
  - PMNT – Primary MNT
  - SMNT – Secondary MNT

- PSN – Policy Service Node
- SNS – Secure Network Server

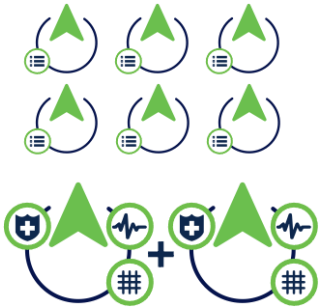
- URT – Upgrade Readiness Tool
  - EOL – End Of Life
  - VM – Virtual Machine
  - GUI – Graphical User Interface
  - CLI – Command Line Interface
  - AD – Active Directory
  - MDM – Mobile Device Management
  - AWS – Amazon Web Services
  - OCI – Oracle Cloud Infrastructure

Reminders

Types of Deployments

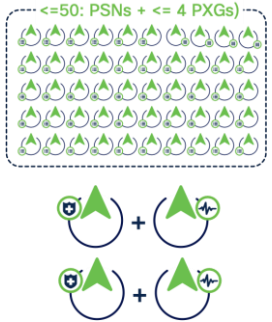
For Reference

Evaluation
Standalone
PAN + MNT + PSN



Medium Deployment
2 x PAN + MNT
5 PSN (6 since 3.0)

Small Deployment
2(.5) nodes
PAN + MNT + PSN



Large Deployment
2 x PAN
2 x MNT
50 PSN

Performance and Scalability Guide for Cisco Identity Services Engine - Cisco

Reminders

ISE platforms

SNS 3515
SNS 3595

EOL

SNS 3615
SNS 3655
SNS 3695

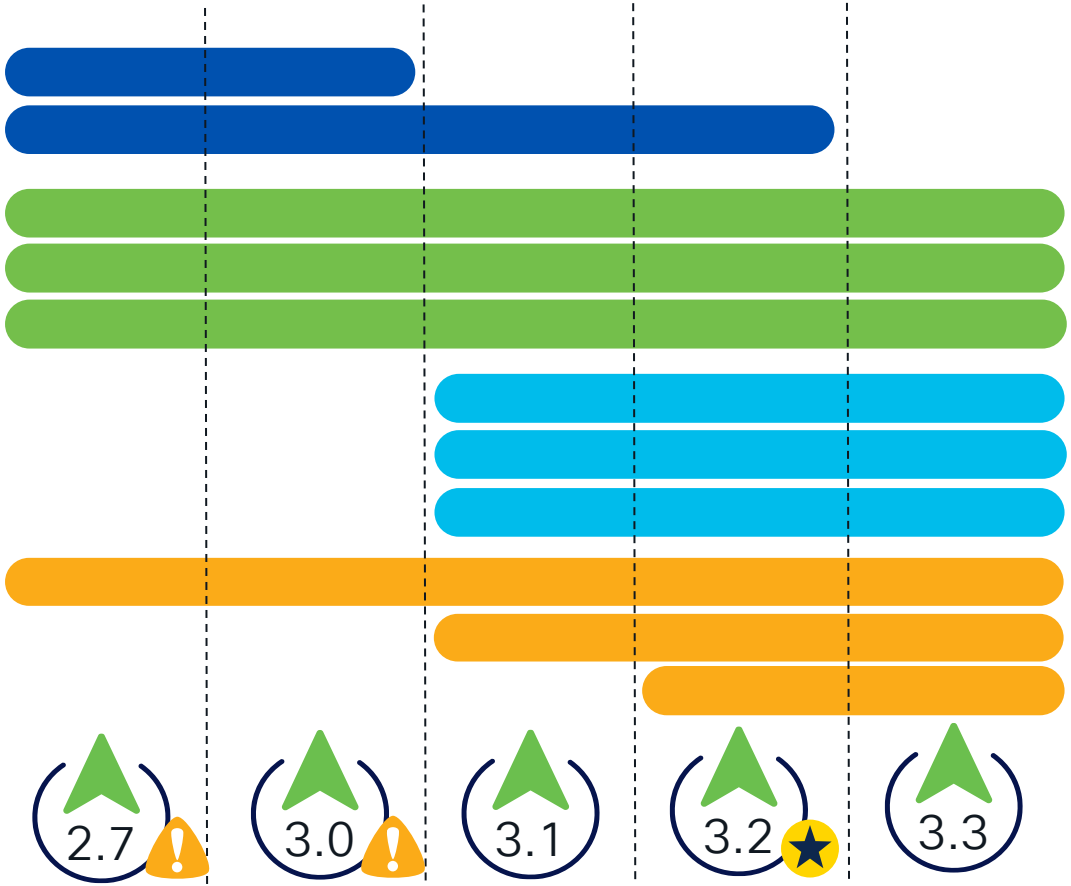
EOL

SNS 3715
SNS 3755
SNS 3795

VM

Traditional VM
AWS
Azure & OCI

For Reference



Best Practices, Tips & Tricks

This green medal icon will indicate some best practices.

The blue lightbulb is gathering Tips !

And finally, this unknown non-malicious hacker will give you some Tricks.

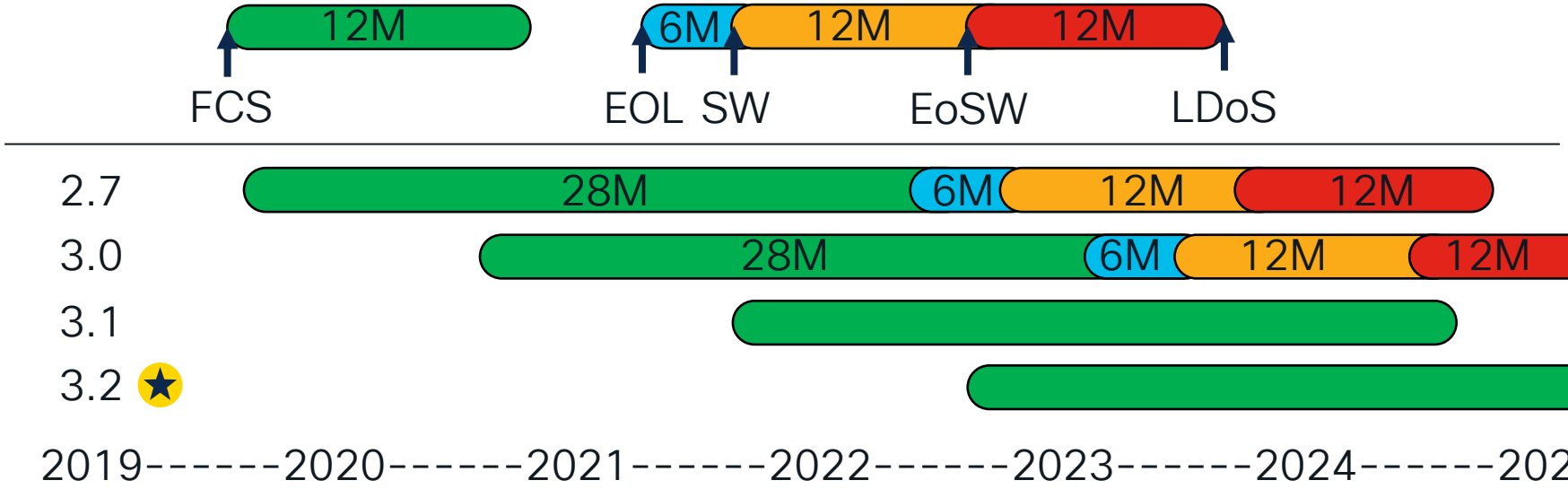
Why Upgrading ISE ?

ISE Lifecycle

Software Lifecycle Support Statement - ISE - Cisco

Since ISE 2.7, no more long/short term release

- All versions are entitled to the same lifecycle
- Plan to release a new version every 8 months



Reasons to Upgrade

- Enhance Product Stability
- Fix Security Vulnerabilities
- Integration with other solutions
- and...

New Features !

For Reference

- ISE 3.1 new features :
  - Release Notes for Cisco Identity Services Engine, Release 3.1 – Cisco

- API enhancements
- Better Posture
- Better logging and alarms
- New upgrade method

- ISE 3.2 new features :
  - Release Notes for Cisco Identity Services Engine, Release 3.2 – Cisco

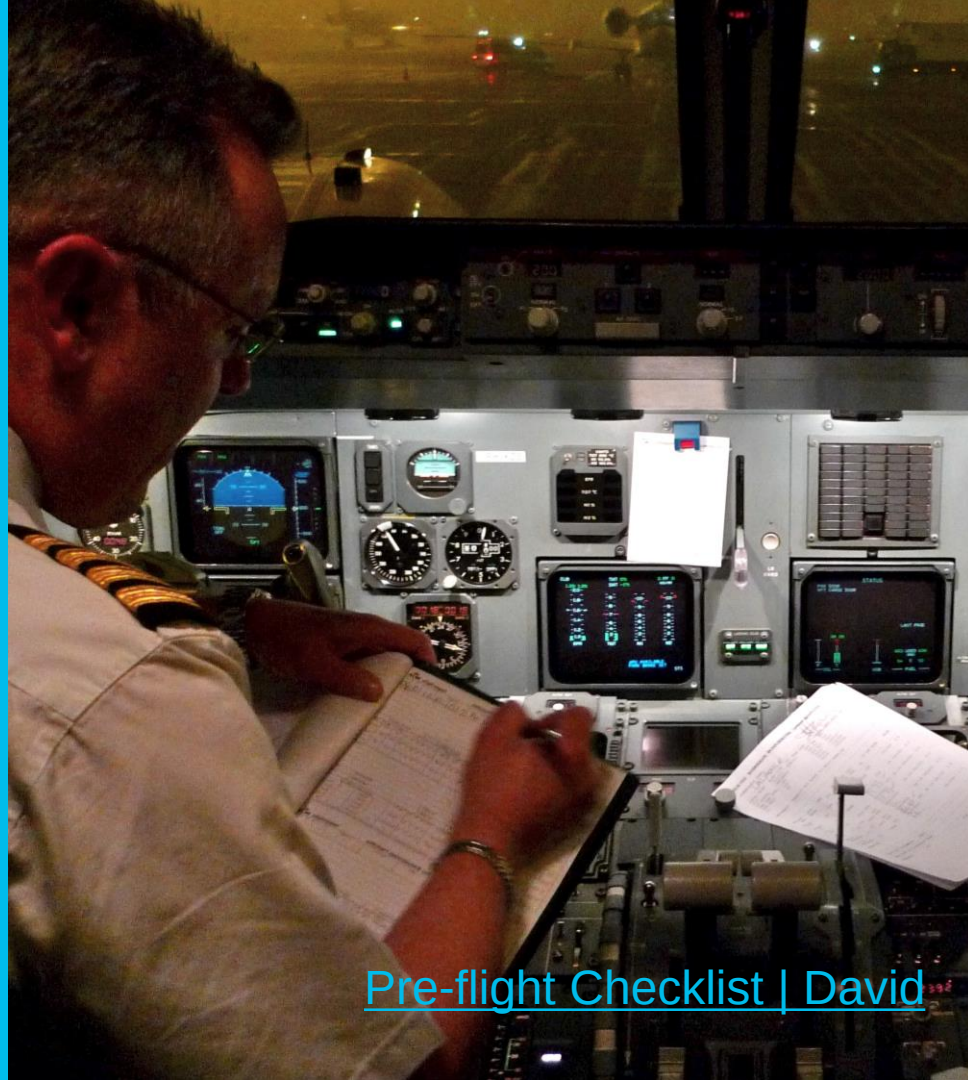
- Data Connect
- Better automation
- Cloud support
- Dark mode

- ISE 3.3 new features :
  - Release Notes for Cisco Identity Services Engine, Release 3.3 – Cisco

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

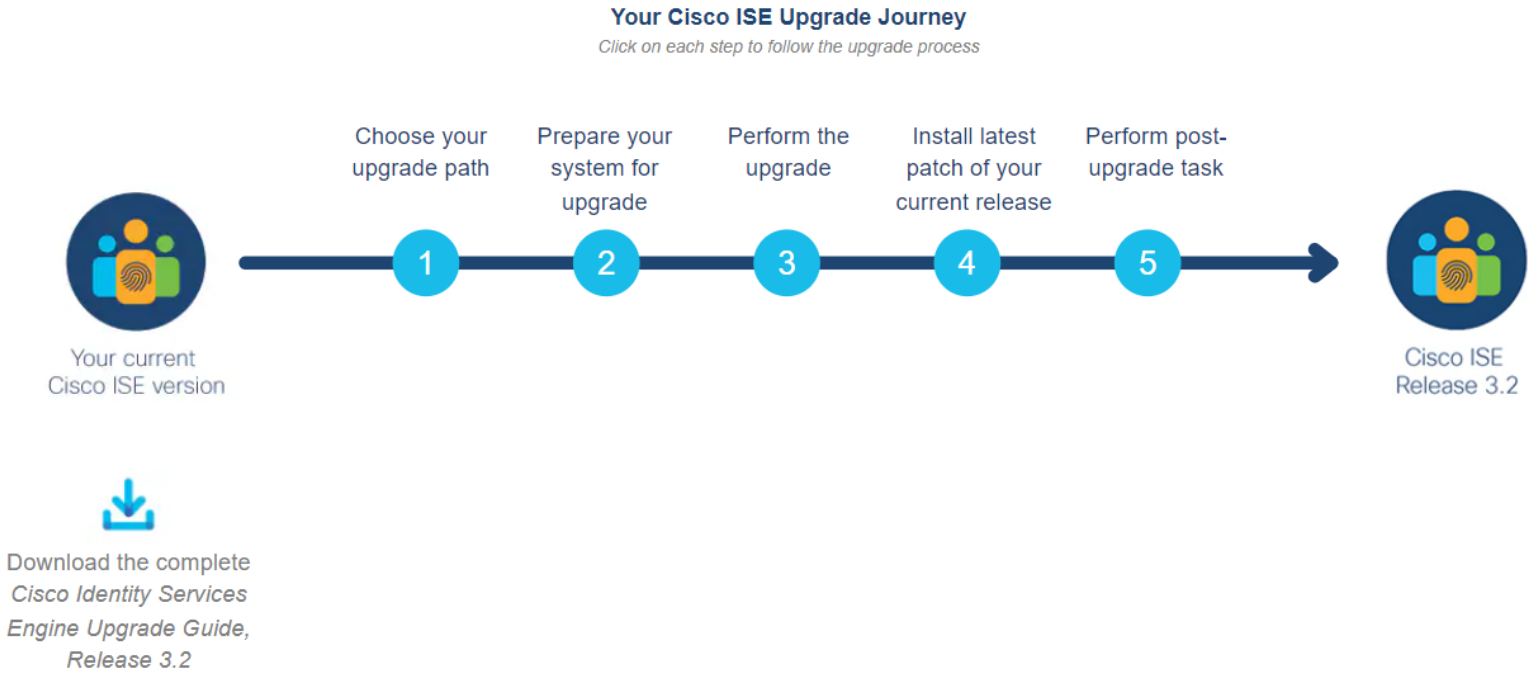
Preparing the Upgrade

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



Pre-flight Checklist | David

Cisco Official Documentation



[Cisco Identity Services Engine Upgrade Journey, Release 3.2 - Cisco]

Choose the appropriate target version

- Check the suggested release (golden star) 
- Check compatibility (Hardware requirements, Integrations)
- Validate your licenses

Cisco ISE Licensing Guide - Cisco

- Open bugs review :
  - Use Bug Search Tool (cisco.com))
  - Engage with Cisco PS for Software Analysis

Target Version : Do not forget

- Validate your upgrade path

Two-step upgrade : Perform the biggest jump first

- Target the latest patch
  - Avoid running ISE in production without a patch
  - Patch are cumulative
  - Allow a 2-3-week delay post-patch release before production installation

Install Patch on ISE - Cisco

Choose your Upgrade Method

- Backup and Restore
  - Recommended method
- Fast but more administration required
- Difficult to perform

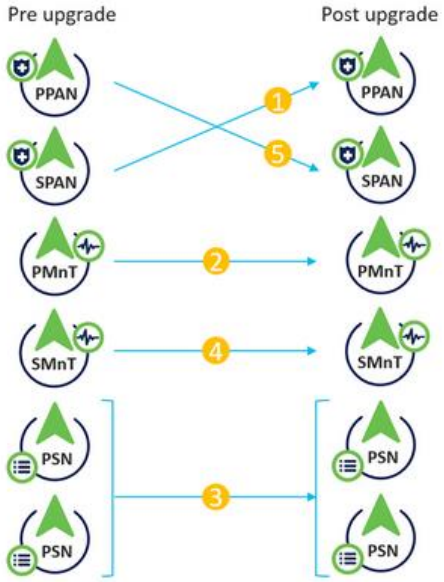
- GUI
- Long but less administration required
- Easy

- CLI
- Longer and more administration required
- Moderate difficulty

Which method is the right for you ?

Difference between Upgrade Method and Upgrade Sequence

- Upgrade Sequence : In which order the ISE nodes are upgraded
- **Common upgrade sequence steps: (except GUI Full Upgrade Method)**



Upgrading the PMNT before the SMNT avoids a persona change.

GUI Upgrade Methods

Split Upgrade

- Step-by-step guide
- Node upgrade sequence: One at a time (Exception - up to 4 PSNs simultaneously)

- Basic knowledge about the ISE installation and configuration
- Great for small / medium deployment

Full Upgrade

(added 2.6P10, 2.7P4, 3.0P3)

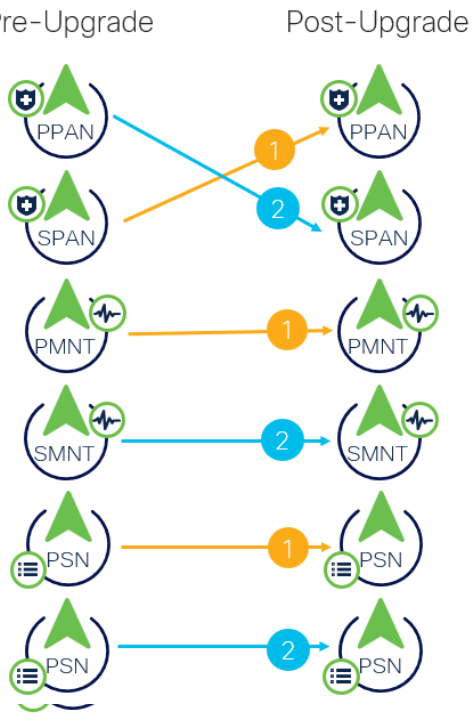
- Step-by-step guide with pre-checks
- Two steps upgrade :
  - PPAN
  - All the other nodes

- Upgrade duration: Same for all deployments
- No Persona change
- Downtime: **Required**

New Split Upgrade Method

New

- Coming with ISE 3.3 and 3.2 P3
- Nodes are now upgraded in Iterations
- Iterations can contain **15** nodes !
- Upgraded configuration is copied from SPAN to other nodes
- Patch installation is available !
- Includes common Pre-Checks!



Understanding new split upgrade on Cisco ISE - Cisco

Pre-Checks List

For Reference

- Repository Validation
- Bundle Download
- Memory check
- Patch Bundle download
- PAN Failover Validation
- Scheduled Backup
- Configuration Data Upgrade
- Services or Process Failures
- Platform Support
- Deployment Validation
- DNS Resolvability
- Trust Store Cert Validation
- System Cert Validation
- Disk Space Check
- NTP Validation
- Load Average Check

CLI Upgrade Method

- Better control over the upgrade
- Good the visibility on the upgrade status
- Requires a good knowledge of the upgrade process

You can shorter the upgrade duration by upgrading nodes in Parallel !

Fallback method to a failed upgrade GUI

Backup and Restore

- Not an upgrade, but node reinstallation
- Backup restoration on new PPAN (old SPAN)
- Other Nodes configuration synchronized during cluster join
- Operation and deployment knowledge level: Highest required

Only option available for Cloud deployments (AWS, Azure and OCI)

B&R can fully be automated [Upgrading ISE in the Cloud with Automation – YouTube] by Charlie Moreton

Other upgrade methods ?

- Mix of CLI Upgrade and Backup & Restore
  - Upgrading the SPAN and PMNT nodes
  - Reinstall and join PSNs

- Automated reconfiguration of ISE
  - Install a fresh new blank config
  - Use APIs to recreate the necessary configurations

How to estimate your upgrade duration ?

Disclaimer: Estimated timings subject to environment specifics

- Use the URT (Upgrade Readiness Tool) to have a better estimation !

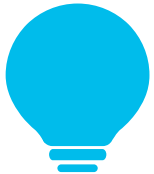
Improving the upgrade duration can be achieved by cleaning endpoints, users, and logs.

Operation	Estimated duration
Installing ISE	1- hour
Restoring a configuration backup (PPAN)	30 minutes
Synchronizing configuration from PAN	30 minutes
Upgrading a PAN	2/3 hours
Upgrading an MNT	2/3 hours + 1 hour / 15 GB of operational data
Upgrading a PSN	1+ hour

Setting up a repository

- Required files for an upgrade (Backups, URT, Installation ISO, upgrade bundle, patch). 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}
```



- If the download of the Upgrade bundle download takes more than 35 minutes, it might timeout

Using the local disk as repository

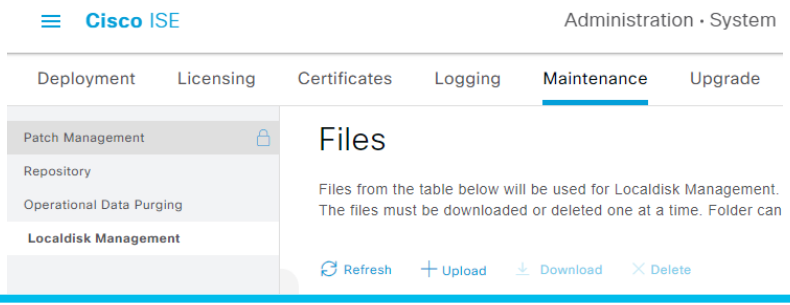
You can use the Local Disk (disk) to store URT or Upgrade bundle.
Warning : the local disk space is limited !

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

```
(config)# repository disk
(config-Repository)# url disk:

# copy ftp://{server}/{filename}
disk:/
```

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



Run the URT

Applies for all upgrade methods (except Full Upgrade and New Split Upgrade)

- Script: Run on SPAN
- Service impact: None
- Actions: Perform common checks, check database compatibility with new version
- Upgrade time estimation for each node

While the URT is running, do not perform any persona change or trigger backup.

```
> application install URT repository
[…]
Checking ISE version compatibility
- Successful
Checking ISE persona
- Successful
[…]
Running data upgrade on cloned database
- Successful
[…]
Time estimate for upgrade
(Estimates are calculated based on size of
config and mnt data only[…))
Estimated time for each node (in mins):
ise30(STANDALONE):83
```

What if the URT is unsuccessful ?

- The failure reason is clear

Fix the issue and rerun the URT to validate. Example :

```
Trust Cert Validation
The certificate has expired.
Trust certificate with friendly name 'VeriSign Class 3 Secure Server CA - G3' is invalid: The certificate has expired.
% Error: One or more trust certificates are invalid (see above), please re-import valid CA Certificate(s) before continuing. Upgrade cannot continue.
- Failed
```

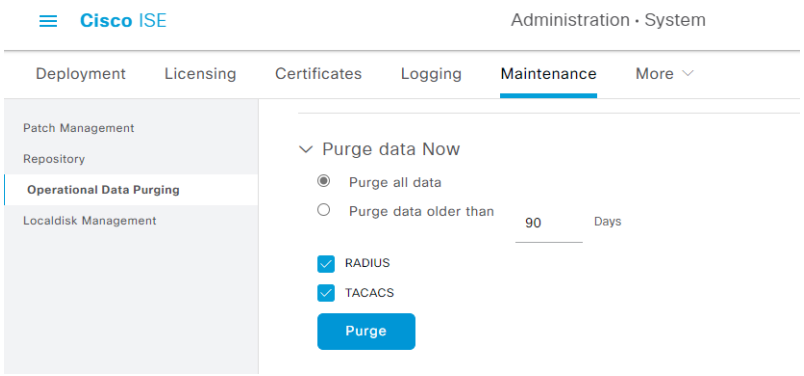
- The failure is not clear :

Logs are stored on the localdisk and should be shared with TAC for analysis

```
Please enter encryption password:
Please enter encryption password again to verify:
Encrypted URT logs(urt_logs.tar.gpg) are available in localdisk. Please reach out to Cisco TAC to debug
% Post-install step failed. Please check the logs for more details.
abivamk24/admin#
```

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 !



If the node was previously MNT and still hold Operational Data logs.
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: 20
```

How to backup ?

- Backup options: Configuration (PPAN) or Operational (PMNT) from GUI or CLI
- Restoration of configuration backup: Option to restore ADE-OS
  - ADE-OS data: Hostname, IP address, NTP, running configuration, etc.

Issue: Slow or stuck backup (Config or Operational)

Solution: Try canceling via GUI or use CLI command

```
> application configure ise
[…]
[24]Force Backup Cancellation
[…]
```

Restoring your config backup in a lab !

- Consider setting up a lab VM of targeted ISE version
- Install latest patch
- Restore production environment backup (without ADE-OS)
- Successful restore indicates upgrade confidence
- Recommended: Planning some authentication tests

Pre-Upgrade validations (checklist)

For Reference

- Backup
  - Configuration, Operational Data, Network devices, endpoints (.csv)
  - Load balancers
  - Export certificates and private keys
  - Export internal CA certificates from CLI
- Take notes
  - AD Credentials and similar credentials
  - MDM 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+)
  - Install latest patch (before the upgrade)
  - Disable PAN failover
  - Disable scheduled backups

Prepare the Maintenance Windows

- Use maintenance windows
  - Yes, it is possible to upgrade in multiple maintenance windows
- Communicate about possible downtime
- Schedule extra-time ! (Estimate worst case scenario)
- Write a Method of Procedure document (MOP). Cisco CX Professional Services can help writing such a document.
- Open a proactive TAC 48 hours before the operation !

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

Performing the Upgrade

To keep in mind

- An ISE upgrade is long, but do not rush it and take your time to double check every step.

- Any mistake :

> “This little maneuver’s gonna cost us 51 years”
>
> Cooper, Interstellar

Some Upgrade Best Practices

- Start your CLI upgrade using a Remote Console !

- Pre-upgrade file upload to ISE node using the following command :

```
# application upgrade prepare {Bundle Name} {Repository}
```

When ready start the upgrade using :

```
# application upgrade proceed
```

If an upgrade launched from the GUI takes longer than 4 hours, the upgrade might fail.

In that case, It's recommended to upgrade via CLI.

Upgrading an ISE Virtual Machine

- If you need to reinstall ISE on multiple VMs in parallel, it is faster to use the an ISO image than to use an OVA.

- Do not forget to Update Guest OS version
  - Procedure (after the upgrade):
    1. Shutdown
    2. Change Guest OS
    3. Start

- ISE disk size increase: Reinstallation only supported method

Upgrading an SNS Appliance

- CIMC and BIOS upgrades: Fix bugs, secure from vulnerability, enhance hardware stability
- You can use the ISE Upgrade Maintenance window for CIMC upgrade but it's best to plan a dedicated one

- Backup and restore: ISO installation proximity to appliance/VM necessary
- The faster method : use a bootable USB key (Since ISE 3.2, the recommended software for bootable USB creation is Rufus).

How to monitor the upgrade process ?

Main ISE system logs will be included in ade/ADE.log log file.

To view the upgrade STEPs in live you can use :

```
> 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...
```

After a node is upgraded

- Verify the ISE services are up and running :
  - `#show application status ise`

Do not make any operation on the node before the having the **Application Server** running !

- Validate the version installed
  - `#show version`

What if the upgrade fails ?

The common logs to check for an error are ade/ADE.log and ise-psc.log. You can view them using :

```
# show logging system ade/ADE.log
# show logging application ise-psc.log
```

- Collect support bundle through CLI using the following command :

```
# backup-logs {Backup Name} repository {Repository Name} public-key
```

- Upload the file to your TAC case for a log analysis.

Cisco Worldwide Support Contacts - Cisco

Failures Remediation

SPAN Upgrade Failure :

- Failure before reboot :

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

- Failure after reboot :

→ Fresh install 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 Fresh install the node and join the **NEW** deployment

- Failure after reboot :

→ Fresh install the node and join the **NEW** deployment

PPAN Upgrade Failure :

- Failure before/after reboot :

→ Fresh install and join the new deployment as SPAN

One Common Mistake

- SPAN upgrade successful, but upgrade failing on other nodes

```
STEP 7: Importing configuration data...
% Error: Sanity test found some objects missing in CEPM schema...
% Warning: Sanity test found some indexes missing in CEPM schema. Please
recreate missing indexes after upgrade using app configure ise cli
% Error: Configuration database Schema Sanity failed!
```

Do not install any patch before finishing the upgrade on all nodes !

- Workarounds :
  - Deregister the node before upgrading it, re-join the cluster after upgrade
  - Use the Backup and Restore method

Warning on Field Notice FN 72499

- ISE 3.1: Supports RSA-PSS signature, incompatible with Anyconnect on Windows
- Bug impact: Anyconnect versions 4.10.04065 and earlier can't authenticate to ISE
- Fix: Upgrade to a fixed Anyconnect version
- Workaround: Disable RSA-PSS on PSNs using CLI

```
# application configure ise

[33]Enable/Disable/Current_status of RSA_PSS signature for EAP-TLS
```

Warning on URL Change for Smart Licensing

- From ISE 3.0 Patch 7, 3.1 Patch 5 and 3.2, the URL to check the ISE licenses consumption has changed
- The new URL is : https://smartreceiver.cisco.com
- Work accordingly to authorize it in your proxy or firewall.

After Upgrade Checklist

For Reference

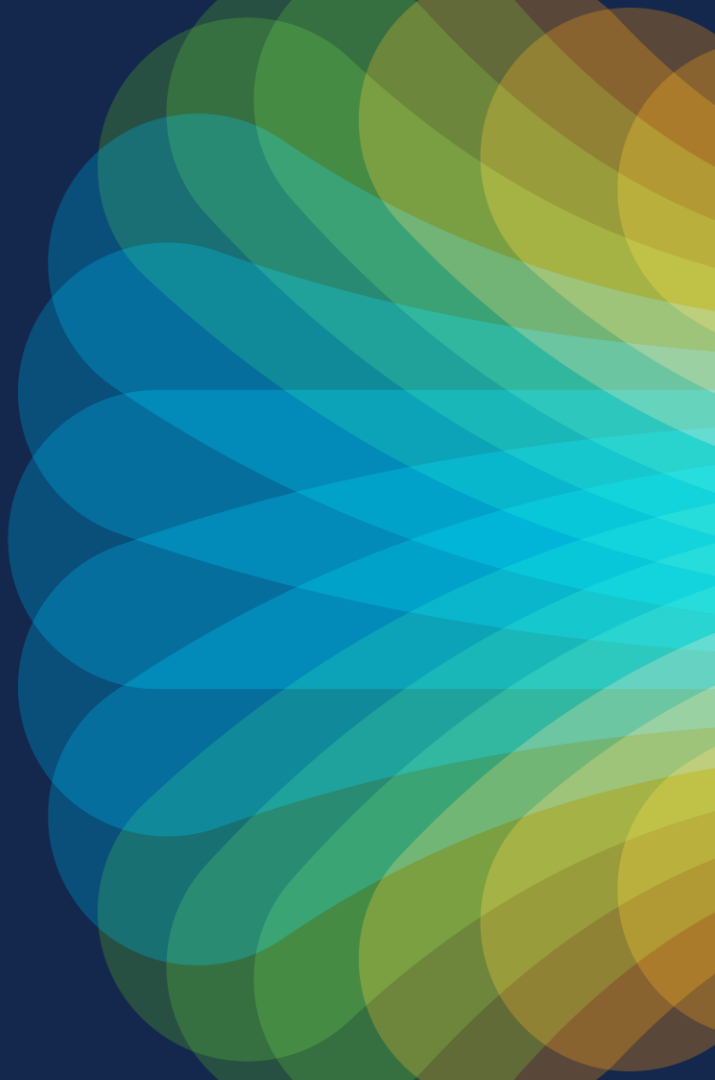
- Install latest Patch
  - Install Patch on ISE – Cisco

- Check the Post-Upgrade tasks :
  - Step 5 of the Upgrade Journey
  - Re-Join Active Directory
  - Regenerate the Root CA chain
  - Check Cipher suites
  - Update Profiler Feed Service
  - Restore Operational Data

Congratulations!

You've Successfully Upgraded Your ISE Deployment.

Conclusion



Conclusion

No magic trick to master an ISE Upgrade

- Important: Understanding ISE installation and upgrade process
- Key aspects: Proper planning, maintenance window usage, downtime communication
- Assistance: Utilize Cisco CX services, proactive TAC engagement

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


cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go