Upgrade ISE with Full Upgrade Method

Contents

Introduction

This document describes how to upgrade an existing ISE deployment from version 2.7 to 3.1 using the Full Upgrade method.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine (ISE)
- Understanding of terminology used to describe different types of ISE deployments

Components Used

The information in this document is based on these software and hardware versions:

- ISE, Release 2.7, patch 4
- ISE, Release 3.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Note: The procedure is similar or identical to other ISE versions. These steps can be used on 2.6 to upgrade to 3.1 and the ISE Software Releases unless stated otherwise.

Background Information

It also includes how to use the Health Checks feature to detect and fix any potential deployment issues. The legacy method of upgrade is now termed as Split Upgrade and is available as an alternate option if the Full Upgrade method is not preferred.

Supported Paths

Full upgrade to ISE 3.1 is supported from

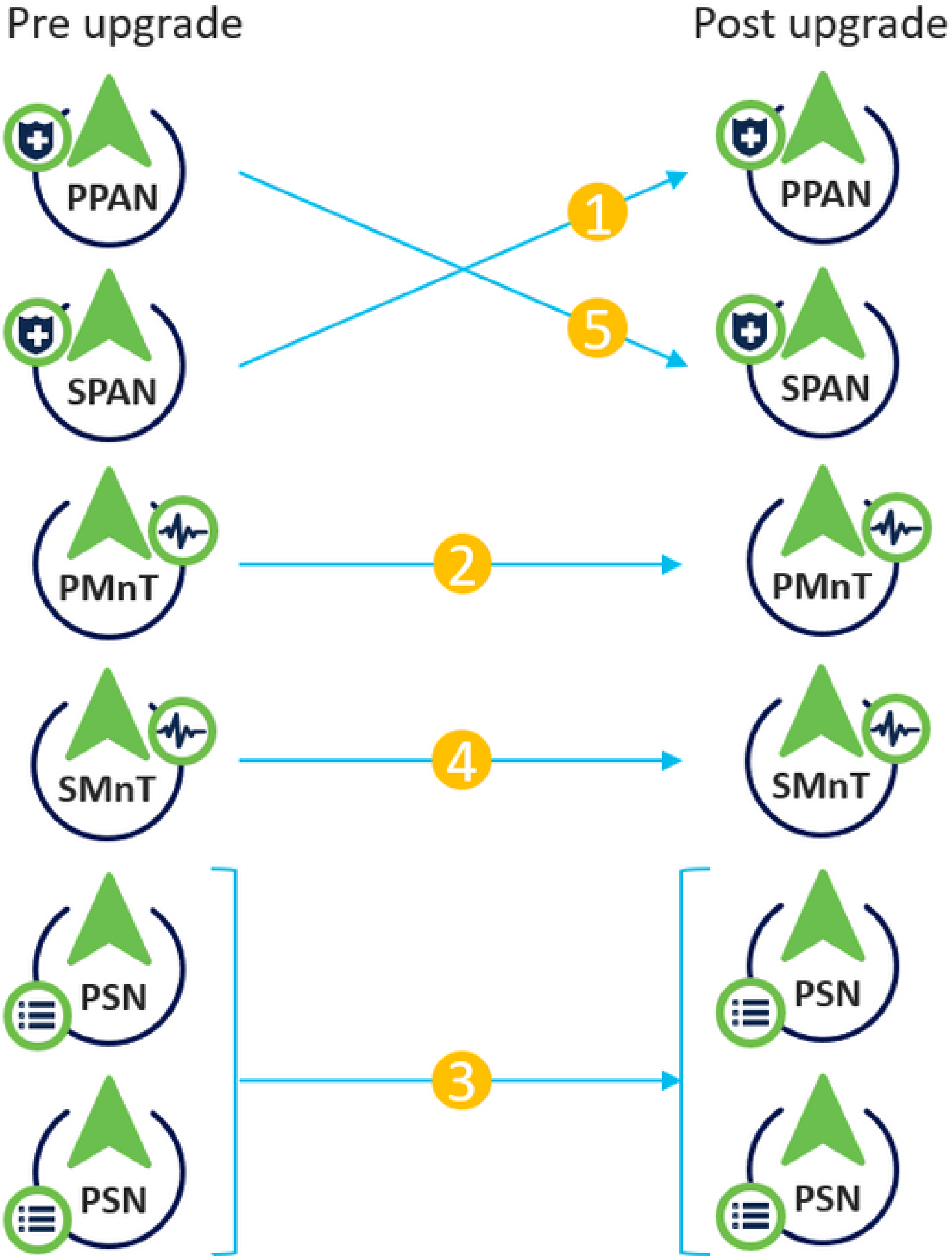
- ISE 2.6 patch 10 and later
- ISE 2.7 patch 4 and later
- ISE 3.0 patch 3 and later

Split upgrade to ISE 3.1 is supported from ISE 2.6 and later versions, with or without any patch.

Comparison of Full Upgrade with Split Upgrade Method

Sequence of Node Upgrade with Split Upgrade Method in a Distributed Deployment

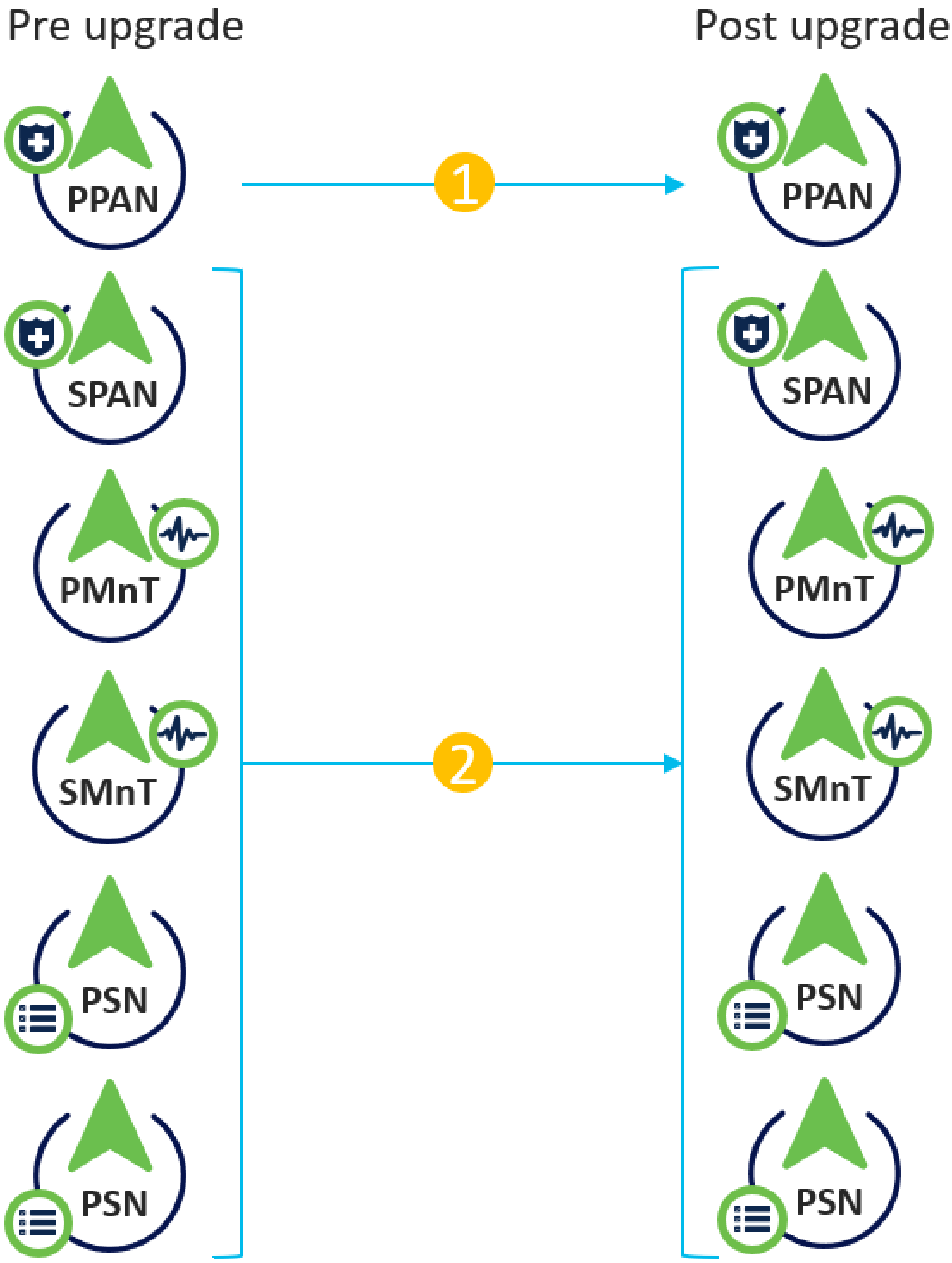
Requires a minimum of 5 steps for a fully distributed deployment to upgrade to the newer version.



Considering approximate 240 minutes for each step, the total upgrade process here would take 240*5 minutes = 20 hours.

Sequence of Node Upgrade with Full Upgrade Method in a Distributed Deployment

Requires only 2 steps for a fully distributed deployment to upgrade to the newer version.



Again, considering approximate 240 minutes for each step, the total upgrade process is now reduced to 240*2 minutes = 8 hours.

Advantages of Full Upgrade over Split Upgrade Method

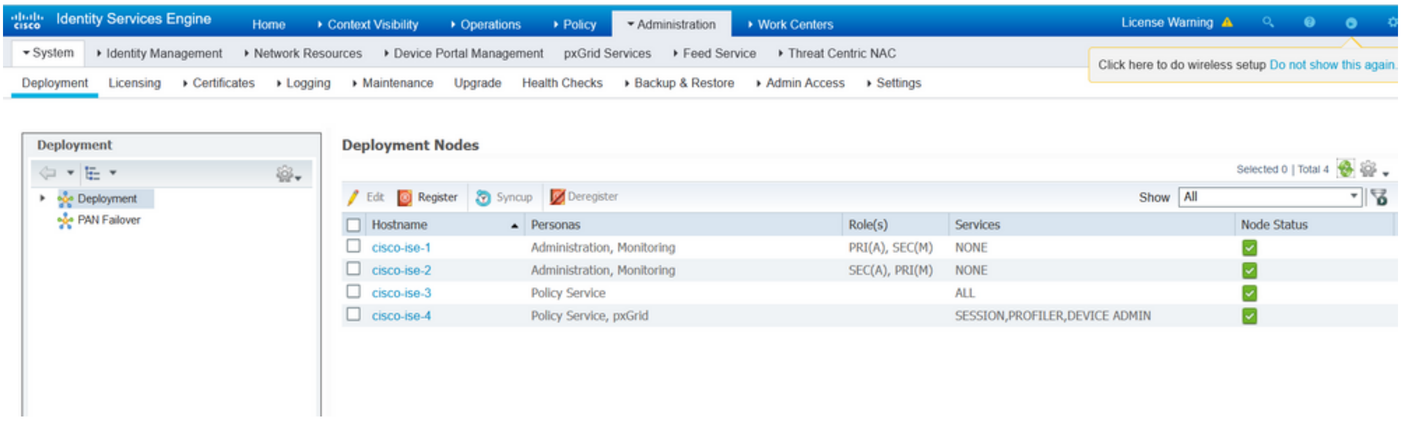
- The Full Upgrade method consumes lesser time for the overall activity because the nodes are upgraded in parallel, whereas the Split Upgrade method needs to be planned well with a longer duration of the maintenance window.

- The Full Upgrade method is hassle-free in terms of upgrade sequence as there are just 2 steps. The Split Upgrade method requires the nodes to be sequenced appropriately before starting the upgrade process.
- The Full Upgrade method retains the roles and personas as it was prior to the upgrade. The Split Upgrade method switches the primary and secondary admin roles in the upgraded version.
- The points of failures have been reduced in the Full Upgrade method by eliminating the API dependency with deployment-related changes during the upgrade process.
- The Full Upgrade method allows to track the upgrade status from the secondary admin node when the primary admin node goes down for an upgrade. This is not possible in the Split Upgrade method.
- Patch installation post-upgrade is automated and is provided as an option in the Full Upgrade method.

⚠ **Caution**: Full upgrade requires a complete downtime because all the PSNs go down for upgrade at the same time. Ensure that the activity is planned during a scheduled maintenance window.

Full Upgrade Flow

This document demonstrates the upgrade flow of a 4 node deployment. The overall process remains the same for two-node or other multi-node deployments.



Deployment Nodes

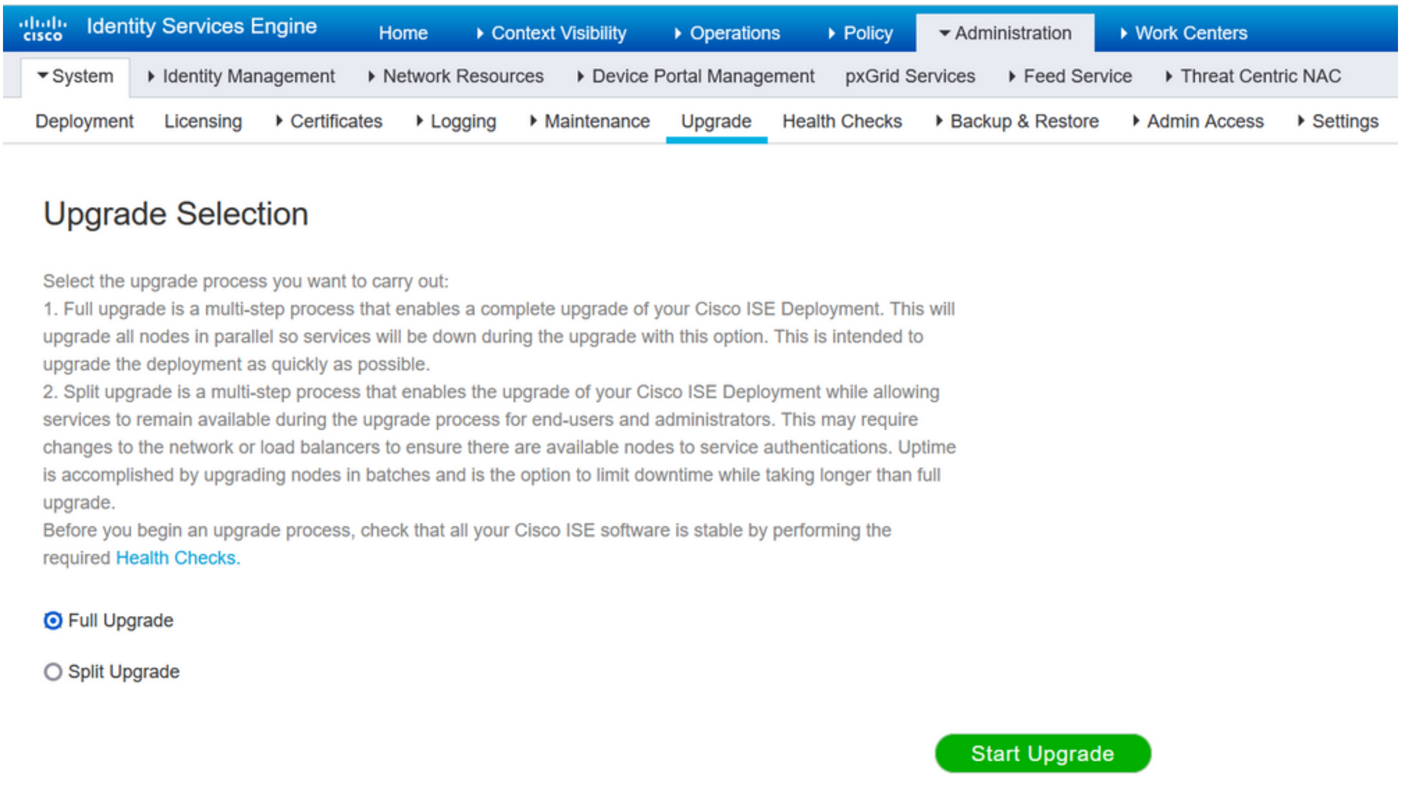
Selected 0 | Total 4

Show All

Hostname	Personas	Role(s)	Services	Node Status
cisco-ise-1	Administration, Monitoring	PRI(A), SEC(M)	NONE	✓
cisco-ise-2	Administration, Monitoring	SEC(A), PRI(M)	NONE	✓
cisco-ise-3	Policy Service		ALL	✓
cisco-ise-4	Policy Service, pxGrid		SESSION,PROFILER,DEVICE ADMIN	✓

Upgrade UI

Navigate to **Administration** > **System** > **Upgrade** in order to begin the activity as shown in the image.



Upgrade Selection

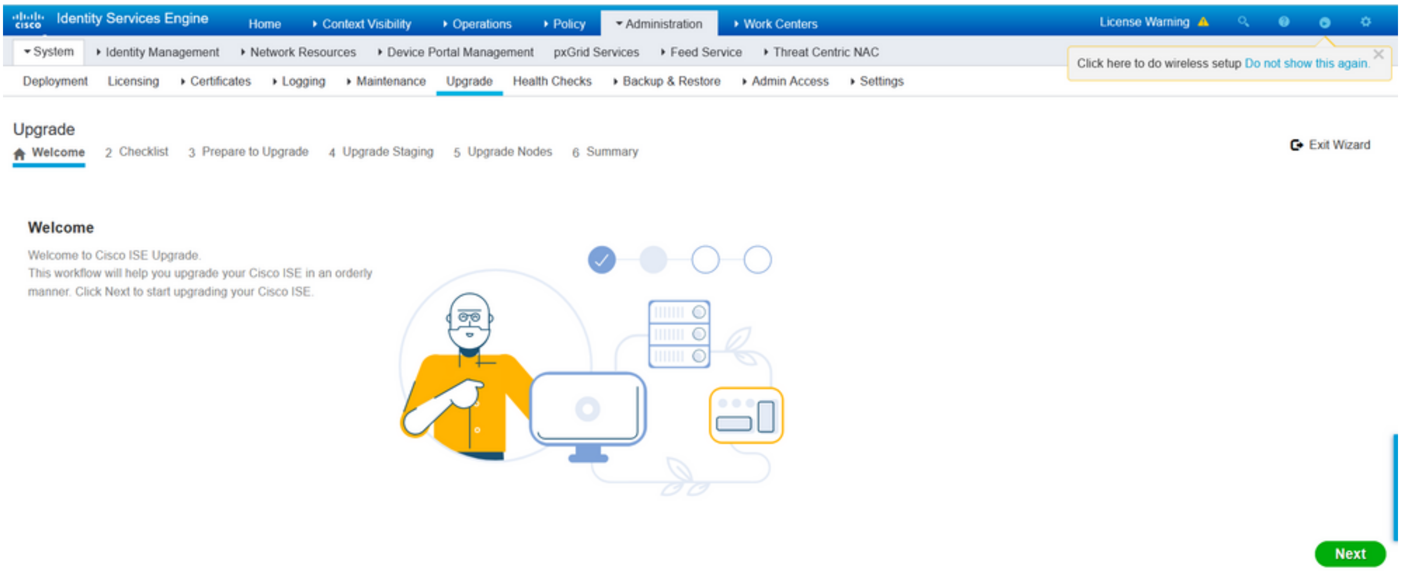
Select the upgrade process you want to carry out:
1. Full upgrade is a multi-step process that enables a complete upgrade of your Cisco ISE Deployment. This will upgrade all nodes in parallel so services will be down during the upgrade with this option. This is intended to upgrade the deployment as quickly as possible.
2. Split upgrade is a multi-step process that enables the upgrade of your Cisco ISE Deployment while allowing services to remain available during the upgrade process for end-users and administrators. This may require changes to the network or load balancers to ensure there are available nodes to service authentications. Uptime is accomplished by upgrading nodes in batches and is the option to limit downtime while taking longer than full upgrade.
Before you begin an upgrade process, check that all your Cisco ISE software is stable by performing the required Health Checks.

● Full Upgrade

○ Split Upgrade

Note: Only the Split Upgrade method is supported on ISE 2.6 patch 9 and below, ISE 2.7 patch 3 and below, and ISE 3.0 patch 2 and below. By default, the Split Upgrade window is launched for these versions. The Split Upgrade process can be referred from here. Select the **Full Upgrade** radio button and click **Start Upgrade**.

Welcome Page



Click here to do wireless setup Do not show this again

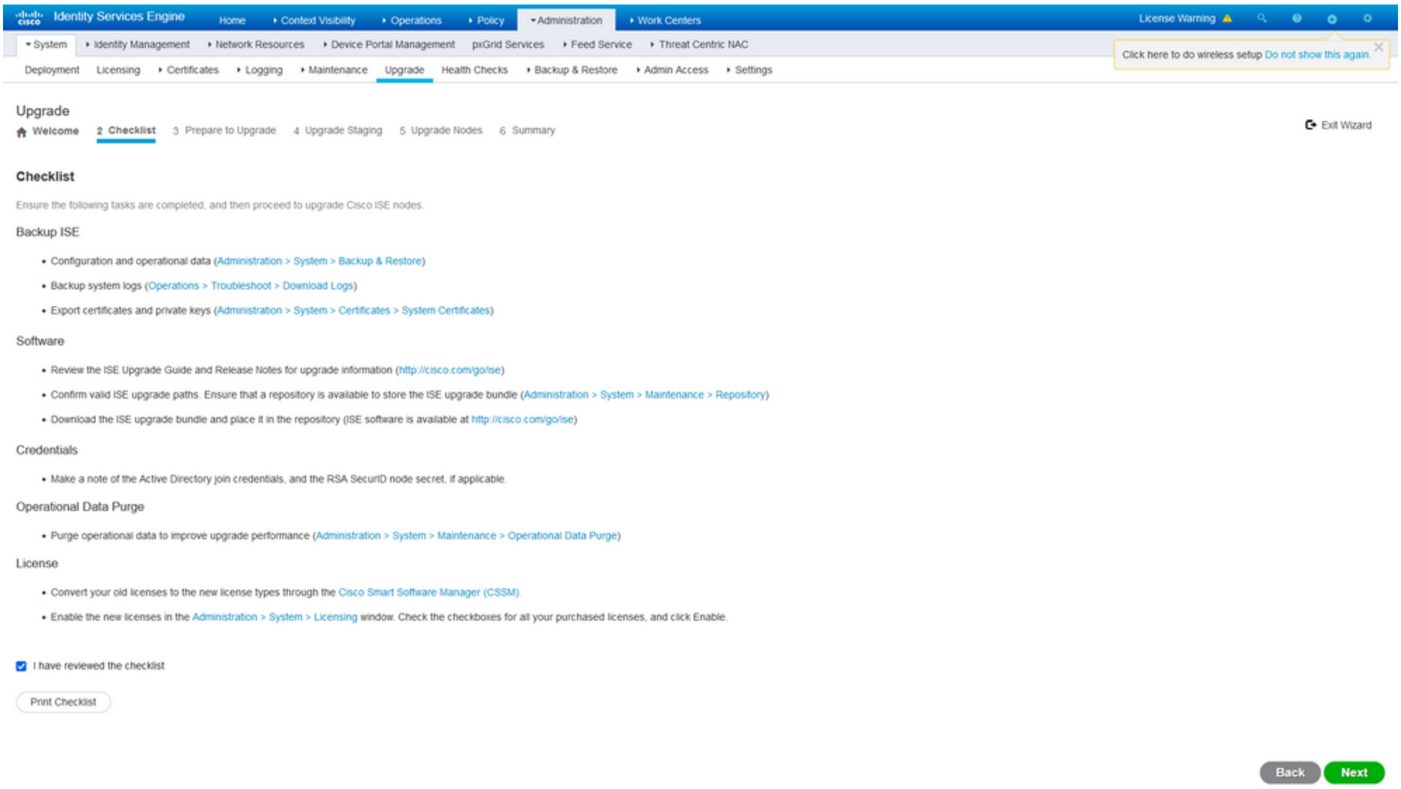
Welcome

Welcome to Cisco ISE Upgrade.
This workflow will help you upgrade your Cisco ISE in an orderly manner. Click Next to start upgrading your Cisco ISE.

On the welcome page wizard, click **Next** in order to proceed further.

Checklist

Review the checklist and ensure to complete the tasks before you proceed further.



Upgrade

Checklist

Ensure the following tasks are completed, and then proceed to upgrade Cisco ISE nodes.

Backup ISE

- Configuration and operational data (Administration > System > Backup & Restore)
- Backup system logs (Operations > Troubleshoot > Download Logs)
- Export certificates and private keys (Administration > System > Certificates > System Certificates)

Software

- Review the ISE Upgrade Guide and Release Notes for upgrade information (http://cisco.com/go/ise)
- Confirm valid ISE upgrade paths. Ensure that a repository is available to store the ISE upgrade bundle (Administration > System > Maintenance > Repository)
- Download the ISE upgrade bundle and place it in the repository (ISE software is available at http://cisco.com/go/ise)

Credentials

- Make a note of the Active Directory join credentials, and the RSA SecurID node secret, if applicable.

Operational Data Purge

- Purge operational data to improve upgrade performance (Administration > System > Maintenance > Operational Data Purge)

License

- Convert your old licenses to the new license types through the Cisco Smart Software Manager (CSSM).
- Enable the new licenses in the Administration > System > Licensing window. Check the checkboxes for all your purchased licenses, and click Enable.

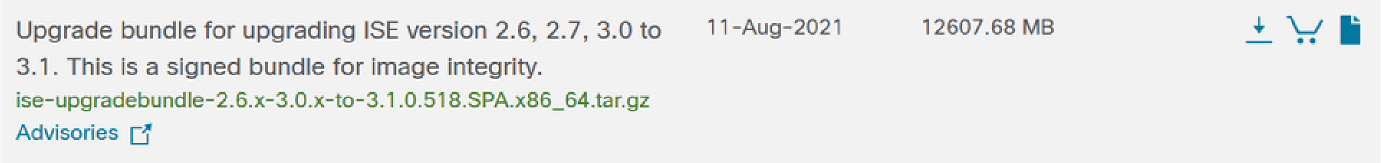
☑ I have reviewed the checklist

Tick the checkbox that states **I have reviewed the checklist** and click **Next**.

Prepare to Upgrade

A pre-check is run on the complete deployment prior to the upgrade and the results are displayed on this page. Apart from the checks, at this step the upgrade bundle is downloaded on all the nodes, offline data upgrade (ODU) is run on the secondary admin node (this is analogous to the Upgrade Readiness Tool (URT) simulation of the Split Upgrade method) and finally, it also displays the time estimate for the activity.

Upgrade bundle is to be downloaded from the Cisco Software Download page.



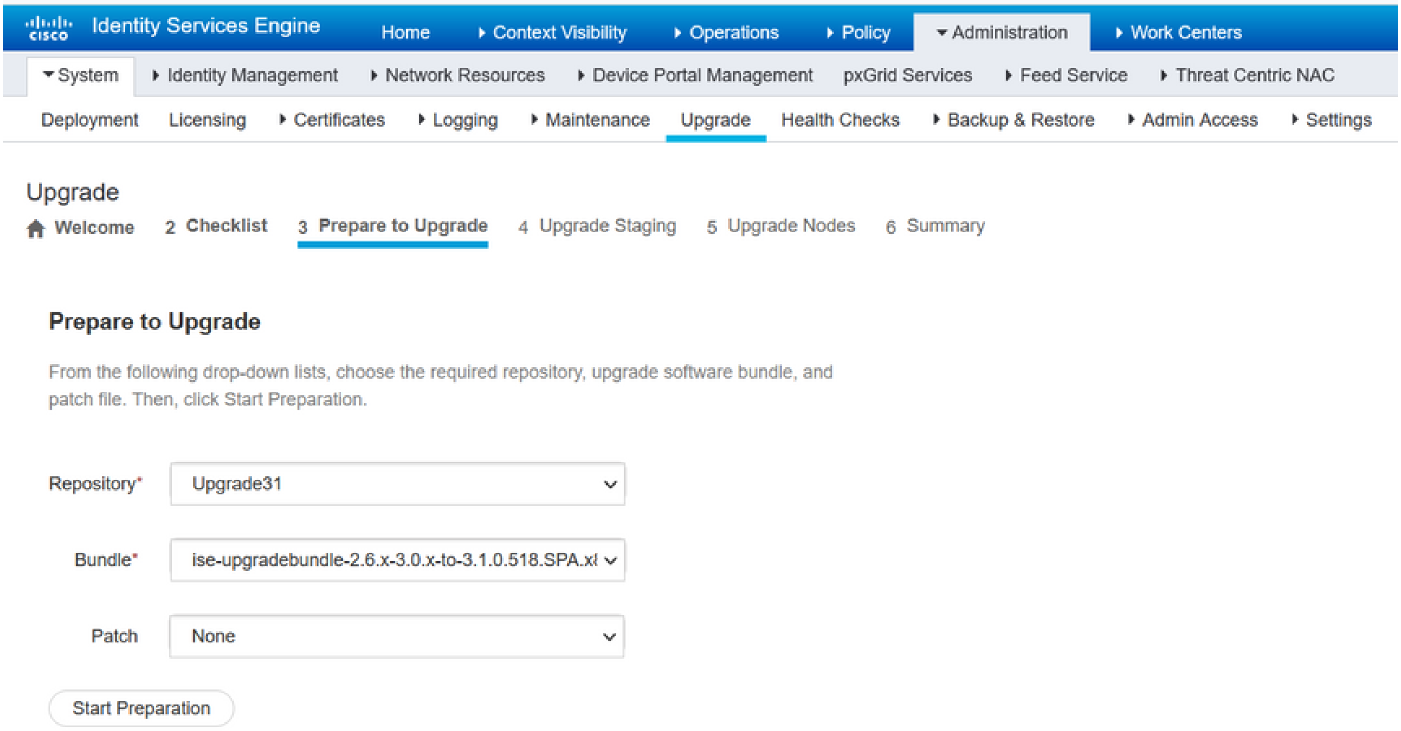
Upgrade bundle for upgrading ISE version 2.6, 2.7, 3.0 to 3.1. This is a signed bundle for image integrity. 11-Aug-2021 12607.68 MB

ise-upgradebundle-2.6.x-3.0.x-to-3.1.0.518.SPA.x86_64.tar.gz

Advisories

In order to run the pre-upgrade check, select the Repository name in which the upgrade bundle is placed. Select the upgrade bundle file name from the Bundle dropdown box.

Note: Full Upgrade method also introduces automatic patch installation post-upgrade. The patch file is to be placed in the same repository along with the upgrade bundle and the patch file name can be selected from the dropdown if automatic patch installation is desired.



Prepare to Upgrade

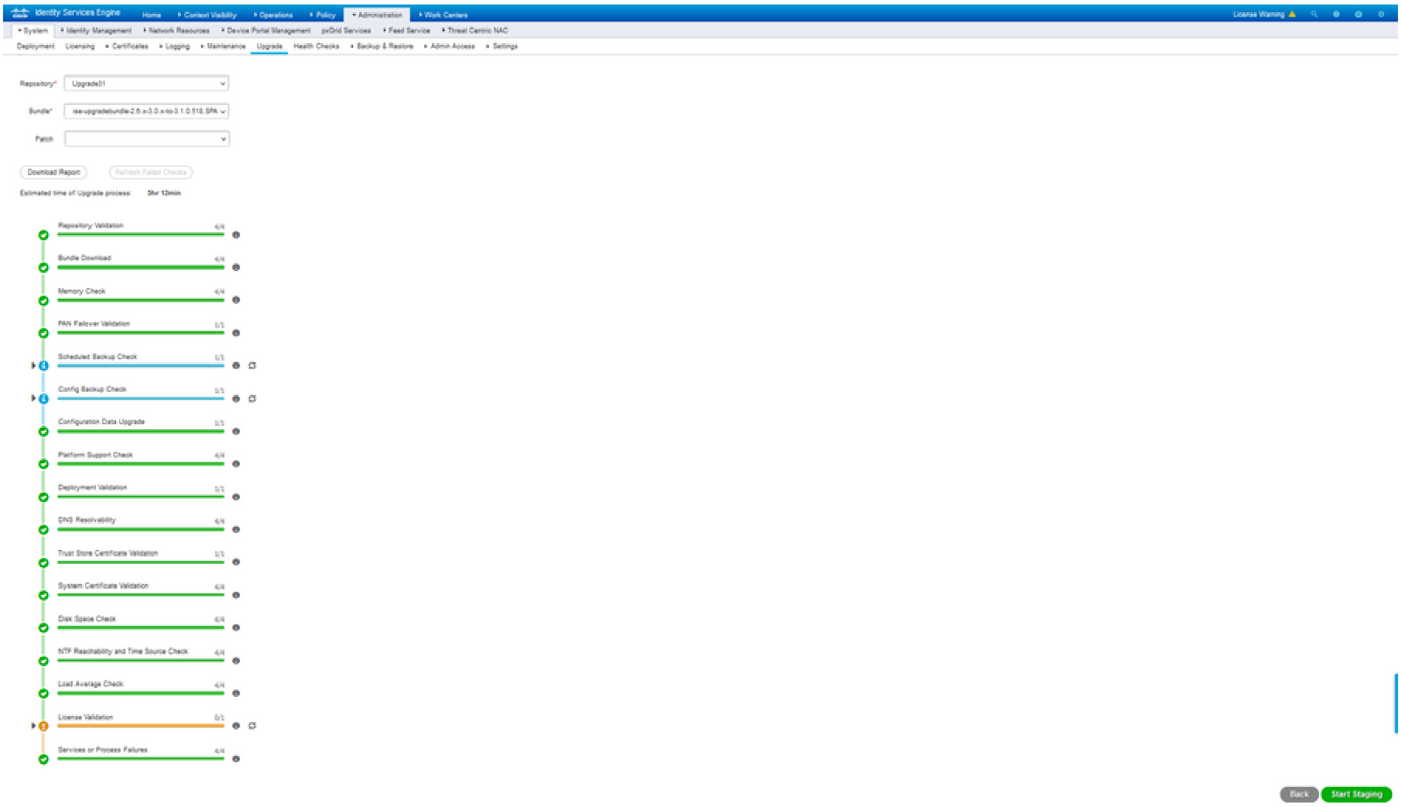
From the following drop-down lists, choose the required repository, upgrade software bundle, and patch file. Then, click Start Preparation.

Repository* Upgrade31

Bundle* ise-upgradebundle-2.6.x-3.0.x-to-3.1.0.518.SPA.x

Patch None

Click on **Start Preparation** in order to start running the pre-checks. All the prechecks, except the Bundle Download and Configuration Data Upgrade check expire automatically after 4 hours of initiating the system validation. Configuration Data Upgrade, which is nothing but the ODU, expires after 12 hours.



Repository* Upgrade31

Bundle* ise-upgradebundle-2.6.x-3.0.x-to-3.1.0.518.SPA

Patch

Estimated time of Upgrade process 5hr 12min

Repository Validation 4/4
Bundle Download 4/4
Memory Check 4/4
PAN Failover Validation 1/1
Scheduled Backup Check 1/1
Config Backup Check 1/1
Configuration Data Upgrade 1/1
Platform Support Check 4/4
Deployment Validation 1/1
DNS Resolvability 4/4
Trust Store Certificate Validation 1/1
System Certificate Validation 4/4
Disk Space Check 4/4
NTP Reachability and Time Source Check 4/4
Load Average Check 4/4
License Validation 0/1
Services or Process Failures 4/4

Note: Disable PAN failover setting before upgrade activity. If not done manually, it gets automatically disabled once the upgrade is triggered.

Note: ISE 3.0 and listed mandates the use of Smart Licensing. It does not support Traditional Licensing. In case Smart Licensing is not enabled or registered prior to the upgrade, ISE lands on Smart Licensing Evaluation period by default post-upgrade. License Migration reference link: Products - ISE Licensing Migration Guide - Cisco. When you upgrade ISE from 2. x to 3.x, it involves licensing tier changes.

Caution: All types of configuration changes on ISE are to be avoided once the Configuration Data Upgrade is triggered. Any changes made would be lost after the upgrade.

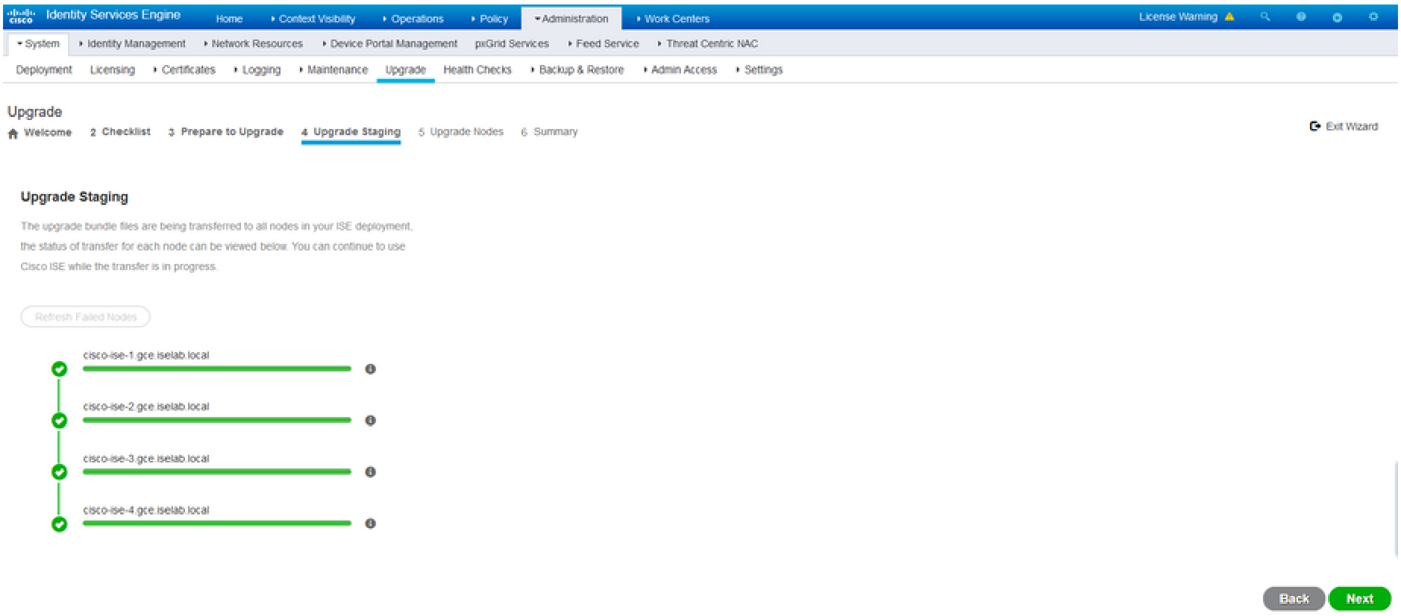
If any of the component pre-checks fail, they are displayed in red or orange colour based on their criticality. The failures highlighted in red need to be mandatorily rectified before proceeding further. The warnings highlighted in orange cannot stop the upgrade process, however, it is good to fix them as best practice and to avoid impacting the deployment features and functionalities in future.

Once the errors are rectified, click on Start Staging to proceed further.

Upgrade Staging

During upgrade staging, the upgraded database file is copied to all the nodes in the deployment and the configuration files are backed up on all nodes of the deployment.

The dump file is already present on the Secondary admin node as part of the ODU. Hence, in this step, the secondary admin node only creates backup files for CA NSS DB, Smart Licensing and DHCP/DNS configuration. All other nodes also create these files but need to additionally copy the dump file from the secondary admin node.



Upgrade Staging

The upgrade bundle files are being transferred to all nodes in your ISE deployment. the status of transfer for each node can be viewed below. You can continue to use Cisco ISE while the transfer is in progress.

cisco-ise-1.gce.iselab.local

cisco-ise-2.gce.iselab.local

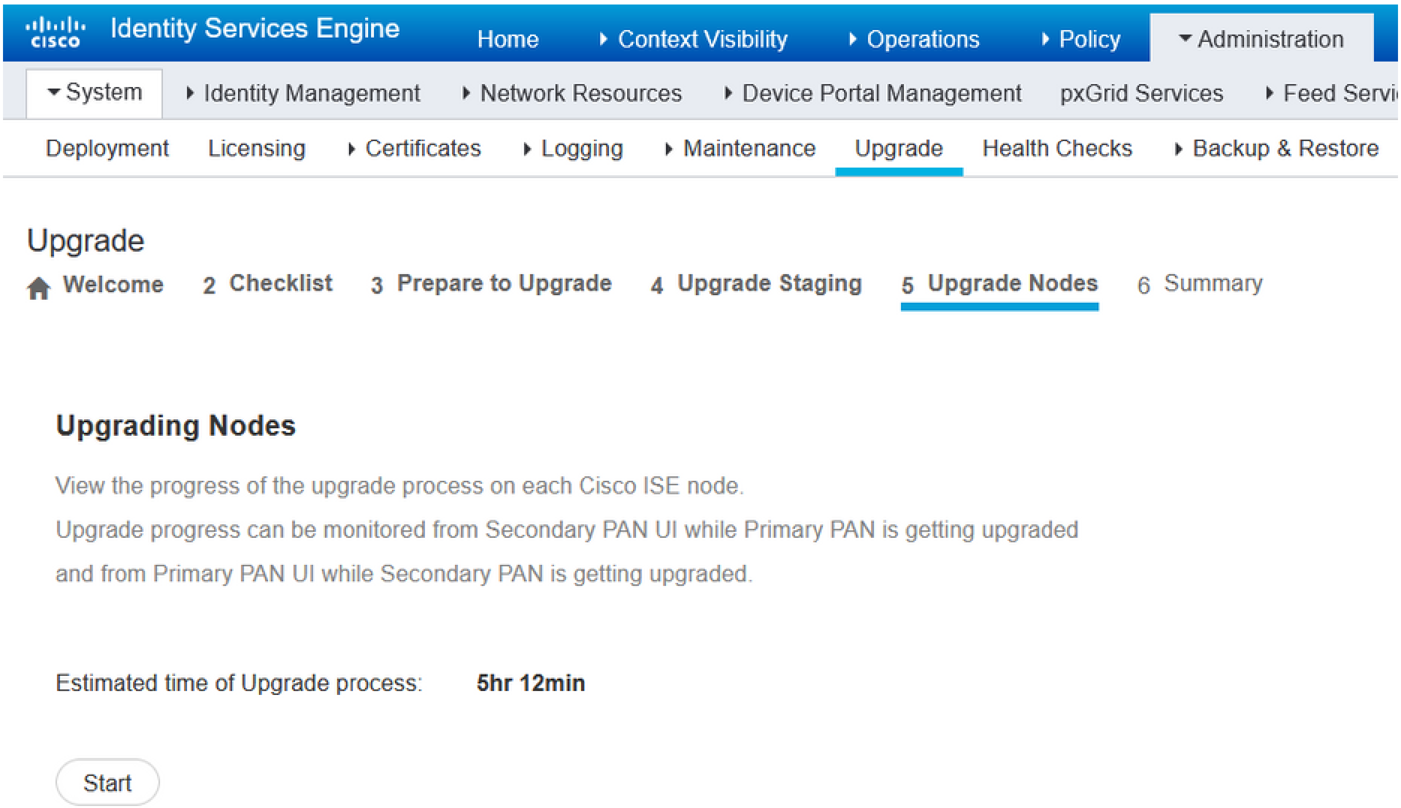
cisco-ise-3.gce.iselab.local

cisco-ise-4.gce.iselab.local

Click **Next** when the staging completes for all the nodes.

Upgrade Nodes

Click on **Start** in order to trigger the upgrade.



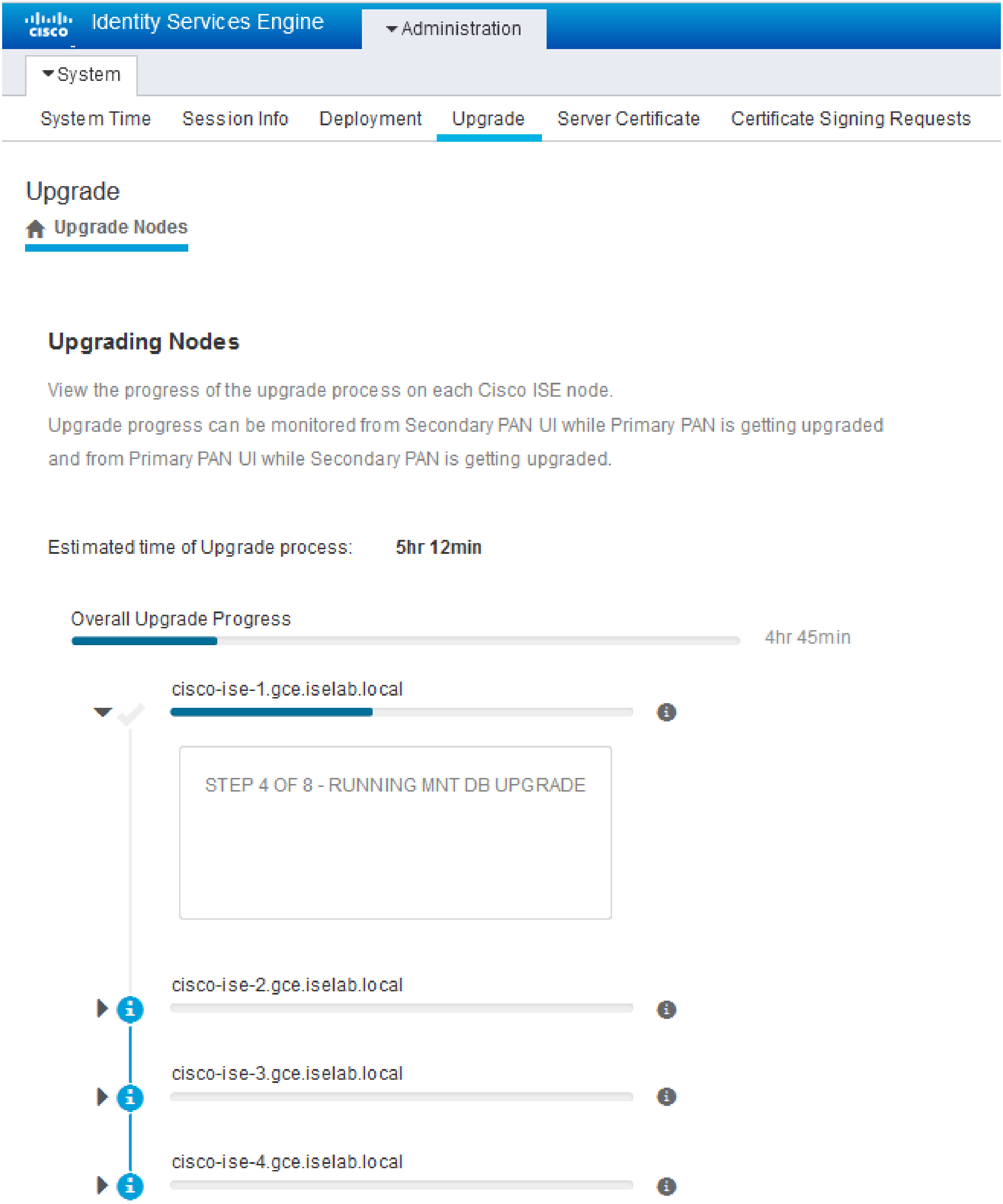
Upgrading Nodes

View the progress of the upgrade process on each Cisco ISE node.

Upgrade progress can be monitored from Secondary PAN UI while Primary PAN is getting upgraded and from Primary PAN UI while Secondary PAN is getting upgraded.

Estimated time of Upgrade process: **5hr 12min**

A pop-up message confirms that the upgrade is triggered and all the nodes are displayed in a queue with the upgrade status. Since the upgrade is initiated on the primary admin node first, the system logs out of this node and now the upgrade status can be monitored from the secondary admin node's GUI. Navigate to **Administration** > **System** > **Upgrade** on the secondary admin node's GUI in order to continue viewing the status.



Upgrading Nodes

View the progress of the upgrade process on each Cisco ISE node.

Upgrade progress can be monitored from Secondary PAN UI while Primary PAN is getting upgraded and from Primary PAN UI while Secondary PAN is getting upgraded.

Estimated time of Upgrade process: 5hr 12min

Overall Upgrade Progress 4hr 45min

cisco-ise-1.gce.iselab.local

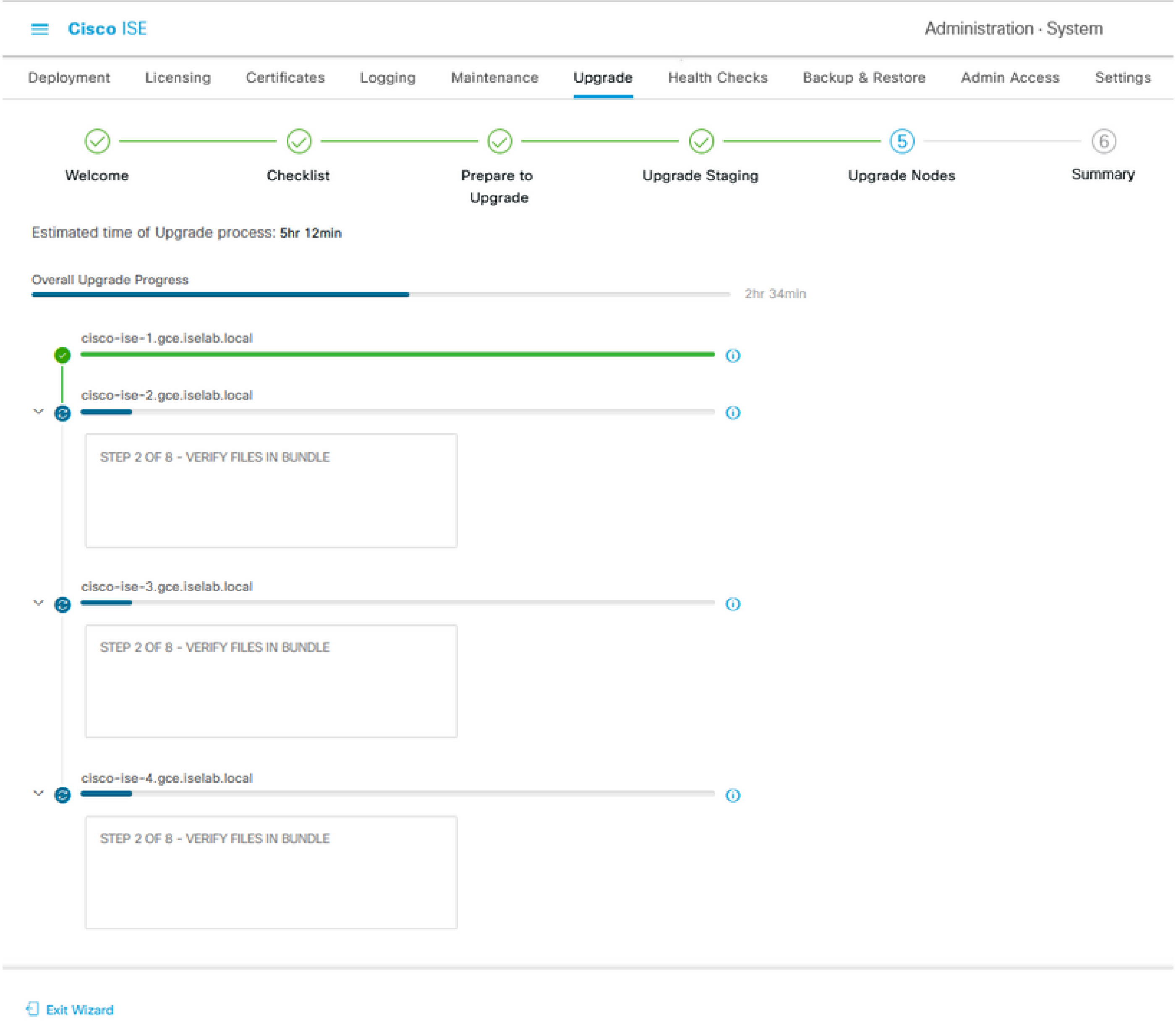
STEP 4 OF 8 - RUNNING MNT DB UPGRADE

cisco-ise-2.gce.iselab.local

cisco-ise-3.gce.iselab.local

cisco-ise-4.gce.iselab.local

Once the primary admin node gets upgraded and the services come up, the system logs out of the secondary admin node's GUI. Users can now switch back to monitoring the status from the primary admin node's GUI while all the other nodes of the deployment go down for the upgrade simultaneously.



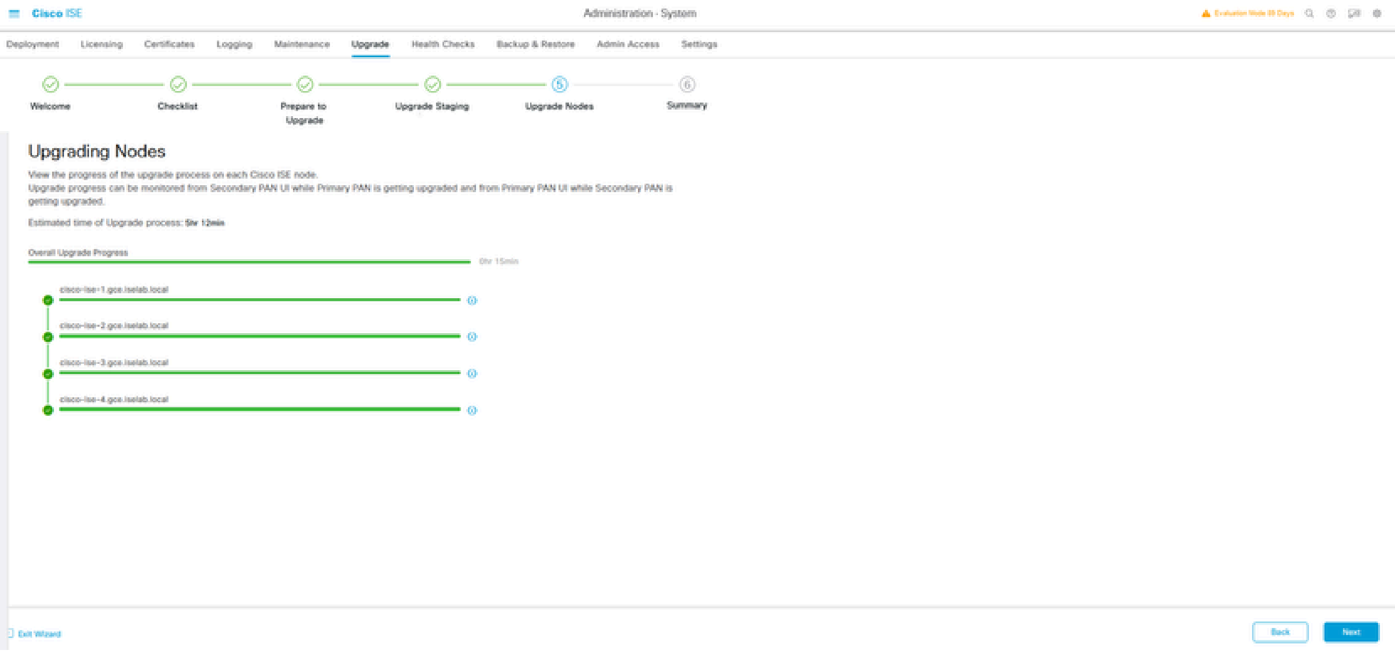
Estimated time of Upgrade process: **5hr 12min**

cisco-ise-2.gce.iselab.local: STEP 2 OF 8 - VERIFY FILES IN BUNDLE

cisco-ise-3.gce.iselab.local: STEP 2 OF 8 - VERIFY FILES IN BUNDLE

cisco-ise-4.gce.iselab.local: STEP 2 OF 8 - VERIFY FILES IN BUNDLE

Once all the nodes get upgraded successfully, the status changes to green colour.



Upgrading Nodes

View the progress of the upgrade process on each Cisco ISE node.
Upgrade progress can be monitored from Secondary PAN UI while Primary PAN is getting upgraded and from Primary PAN UI while Secondary PAN is getting upgraded.

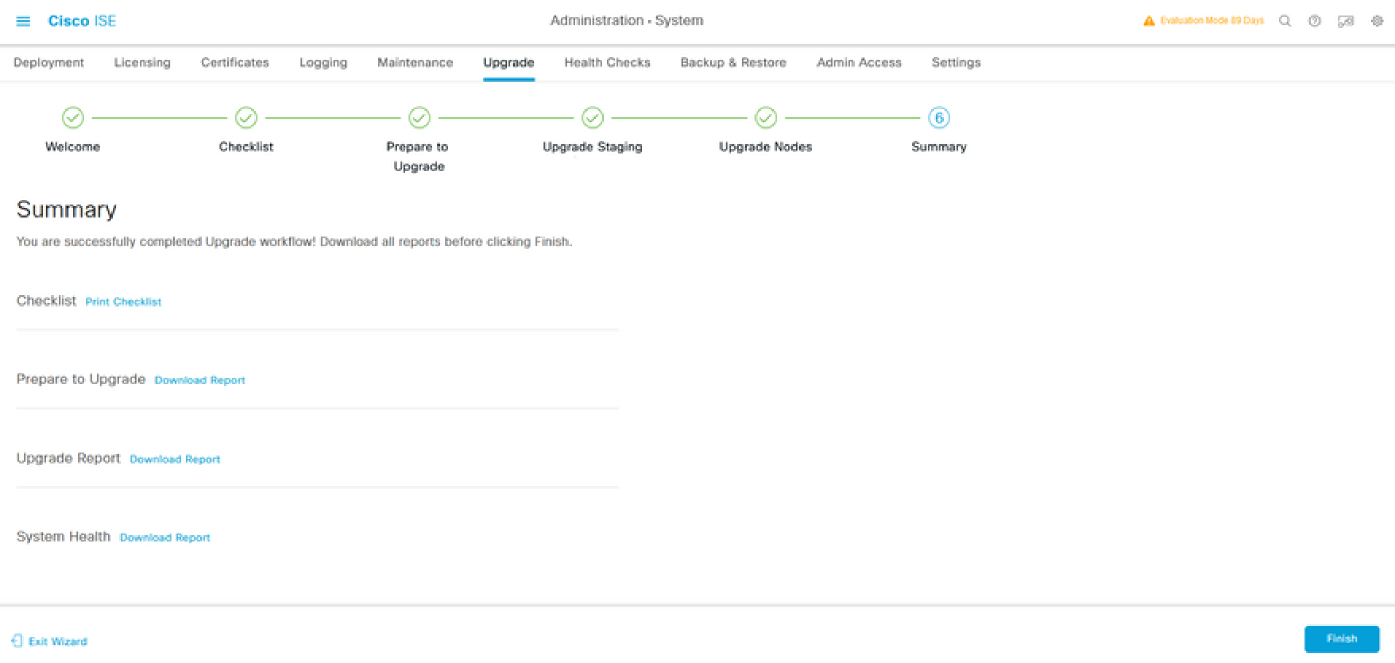
Estimated time of Upgrade process: **5hr 12min**

If there are any failed nodes, a pop-up window with information about the failed node is displayed. Click **OK** in the popup window to de-register the failed nodes from the deployment. These have to be individually upgraded/re-imaged and joined back to the deployment if any.

Click **Next** in order to view the overall upgrade summary reports.

Summary

After the upgrade process is complete, the diagnostic upgrade reports for the deployment can be viewed and downloaded from this page.



You are successfully completed Upgrade workflow! Download all reports before clicking Finish.

Checklist Print Checklist

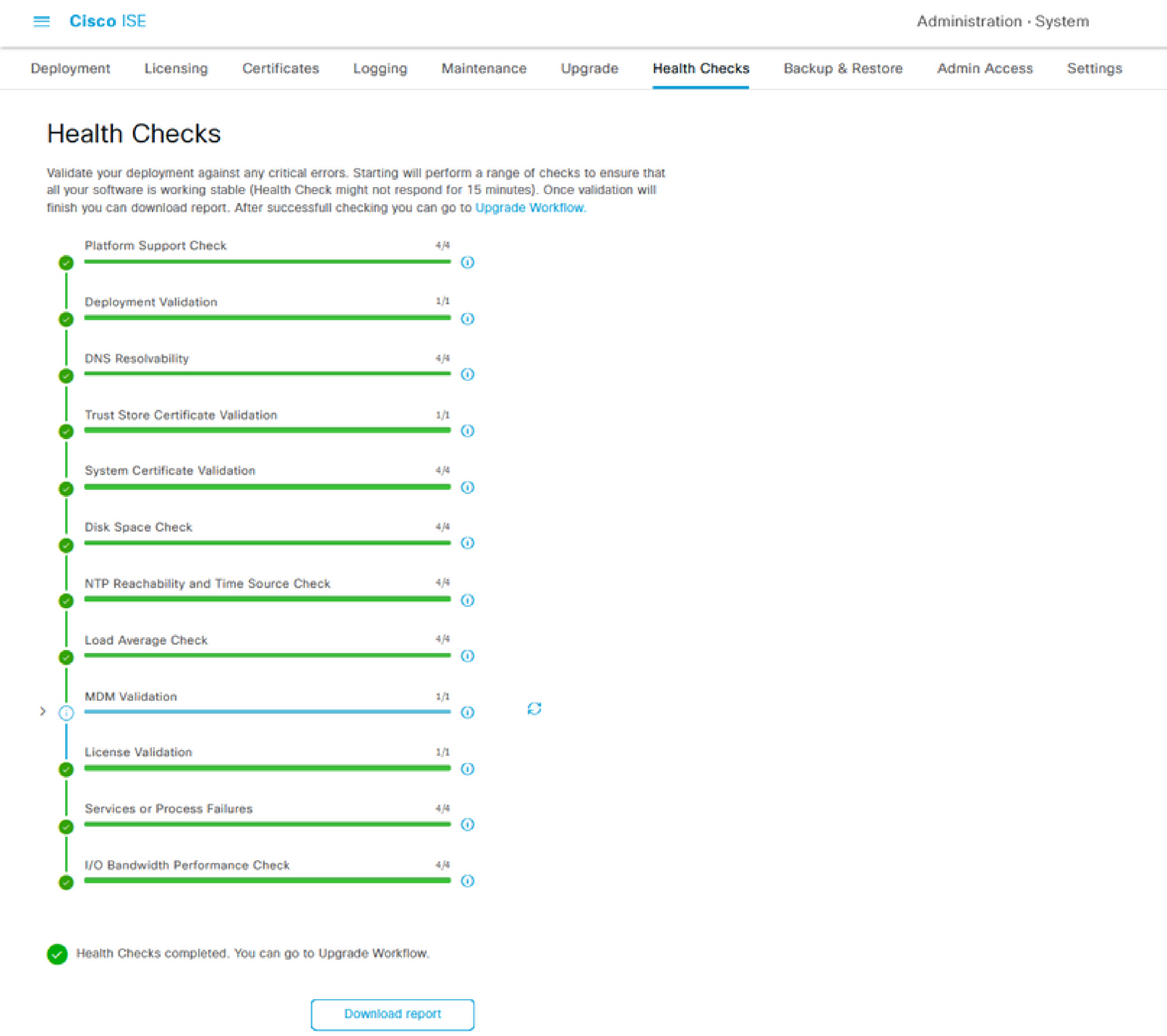
Prepare to Upgrade Download Report

Upgrade Report Download Report

System Health Download Report

Health Checks

In order to validate the deployment status post-upgrade, a health check runs automatically to verify the deployment's status. This report can be downloaded from the Summary page of the upgrade flow. If an on-demand health check is required at any point in time, navigate to **Administration > System > Health Checks** and click on **Start Health Checks**.



Health Checks

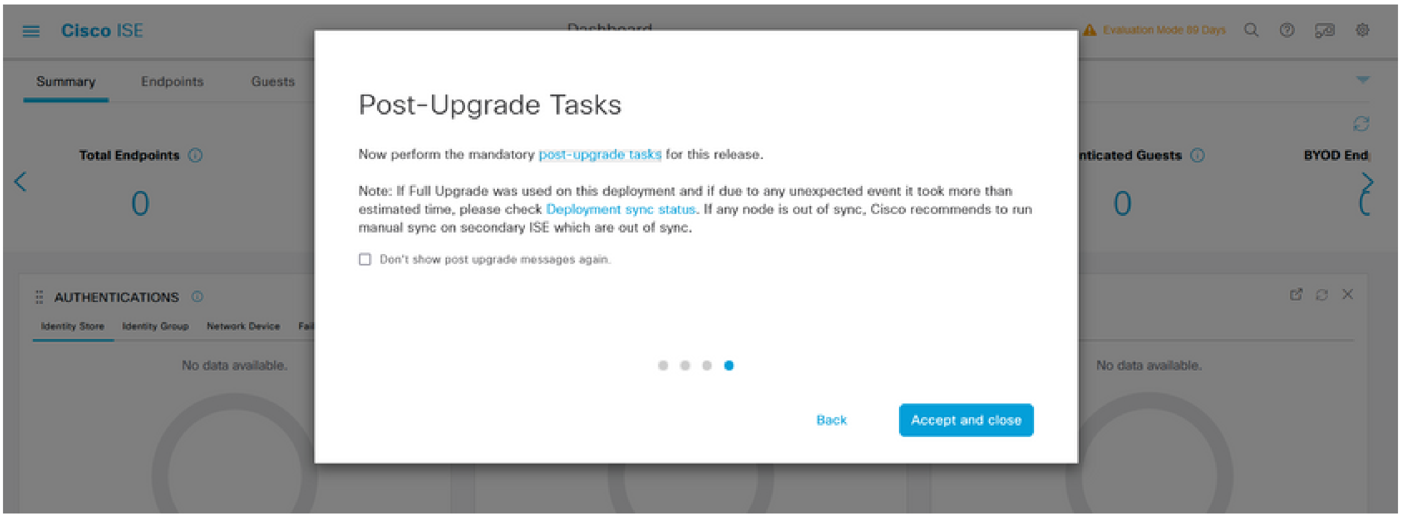
Validate your deployment against any critical errors. Starting will perform a range of checks to ensure that all your software is working stable (Health Check might not respond for 15 minutes). Once validation will finish you can download report. After successfull checking you can go to Upgrade Workflow.

Platform Support Check	4/4
Deployment Validation	1/1
DNS Resolvability	4/4
Trust Store Certificate Validation	1/1
System Certificate Validation	4/4
Disk Space Check	4/4
NTP Reachability and Time Source Check	4/4
Load Average Check	4/4
MDM Validation	1/1
License Validation	1/1
Services or Process Failures	4/4
I/O Bandwidth Performance Check	4/4

Health Checks completed. You can go to Upgrade Workflow.

Post Upgrade Tasks

When a user logs in to the primary admin node's GUI after you complete the upgrade, a pop-up message is displayed regarding post-upgrade tasks.



Post-Upgrade Tasks

Now perform the mandatory post-upgrade tasks for this release.

Note: If Full Upgrade was used on this deployment and if due to any unexpected event it took more than estimated time, please check Deployment sync status. If any node is out of sync, Cisco recommends to run manual sync on secondary ISE which are out of sync.

□ Don't show post upgrade messages again.

Click the post-upgrade tasks hyperlink on the pop-up message in order to review the task details and complete them.

Issues and Remedies

1. If the primary admin node upgrade fails, promote the secondary admin to the primary admin and then re-try the upgrade.
2. If the upgrade fails on any other node apart from primary admin, the node would have to be deregistered from the deployment. This node has to be upgraded individually or reimaged directly to the upgraded version and can be joined back to the deployment.