

Aggiorna ISE con il metodo di aggiornamento completo

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Percorsi supportati](#)

[Confronto tra l'aggiornamento completo e il metodo di aggiornamento diviso](#)

[Sequenza di aggiornamento del nodo con metodo di aggiornamento suddiviso in una distribuzione distribuita](#)

[Sequenza di aggiornamento dei nodi con il metodo di aggiornamento completo in una distribuzione distribuita](#)

[Vantaggi dell'aggiornamento completo rispetto al metodo di aggiornamento suddiviso](#)

[Flusso di aggiornamento completo](#)

[Aggiorna interfaccia utente](#)

[Pagina iniziale](#)

[Elenco di controllo](#)

[Preparazione aggiornamento](#)

[Aggiorna gestione temporanea](#)

[Aggiorna nodi](#)

[Riepilogo](#)

[Controlli integrità](#)

[Task successivi all'aggiornamento](#)

[Problemi e rimedi](#)

Introduzione

Questo documento descrive come aggiornare un'implementazione ISE esistente dalla versione 2.7 alla 3.1 utilizzando il metodo di aggiornamento completo.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE)
- Comprensione della terminologia utilizzata per descrivere i diversi tipi di implementazioni ISE

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISE, release 2.7, patch 4
- ISE, release 3.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

 Nota: la procedura è simile o identica ad altre versioni ISE. A meno che non sia specificato diversamente, questi passaggi possono essere utilizzati nella versione 2.6 per aggiornare la versione 3.1 e le versioni software ISE.

Premesse

Viene inoltre descritto come utilizzare la funzionalità Verifiche stato per rilevare e risolvere eventuali problemi di distribuzione. Il metodo di aggiornamento precedente è ora denominato Split Upgrade ed è disponibile come opzione alternativa se non si preferisce il metodo di aggiornamento completo.

Percorsi supportati

L'aggiornamento completo ad ISE 3.1 è supportato da

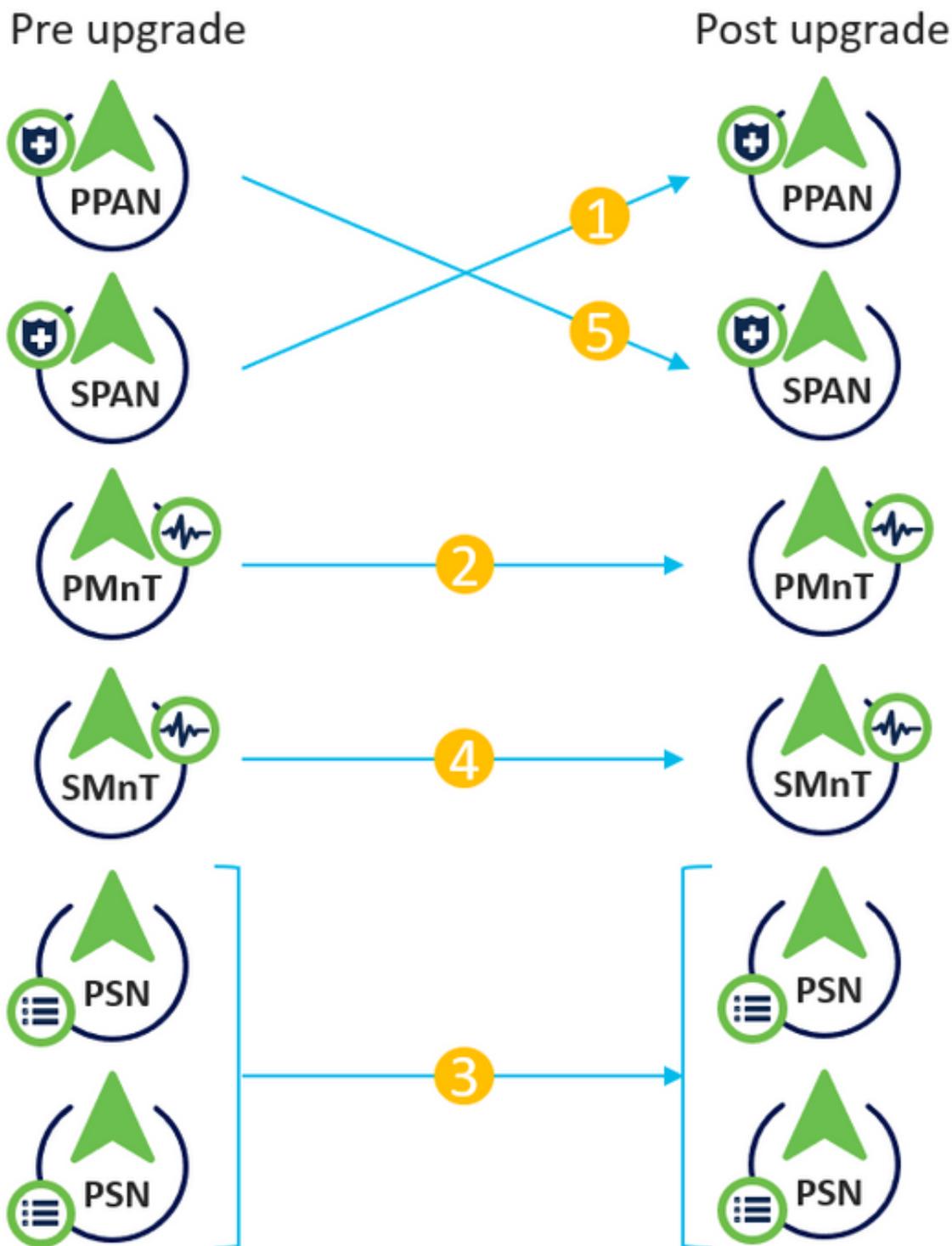
- ISE 2.6 patch 10 e versioni successive
- ISE 2.7 patch 4 e versioni successive
- ISE 3.0 patch 3 e versioni successive

L'aggiornamento split ad ISE 3.1 è supportato da ISE 2.6 e versioni successive, con o senza patch.

Confronto tra l'aggiornamento completo e il metodo di aggiornamento diviso

Sequenza di aggiornamento del nodo con metodo di aggiornamento suddiviso in una distribuzione distribuita

Richiede almeno 5 passaggi per una distribuzione completamente distribuita per eseguire l'aggiornamento alla versione più recente.

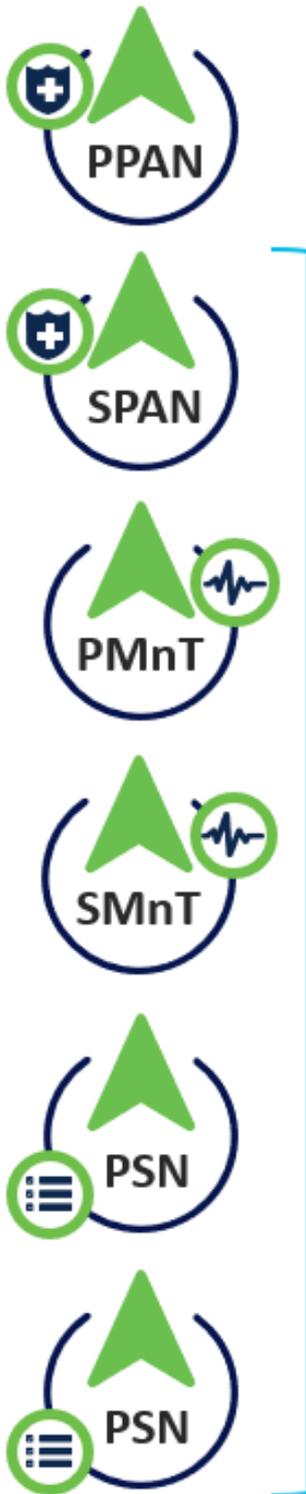


Considerando circa 240 minuti per ciascuna fase, il processo di aggiornamento totale qui richiederebbe $240 \cdot 5$ minuti = 20 ore.

Sequenza di aggiornamento dei nodi con il metodo di aggiornamento completo in una distribuzione distribuita

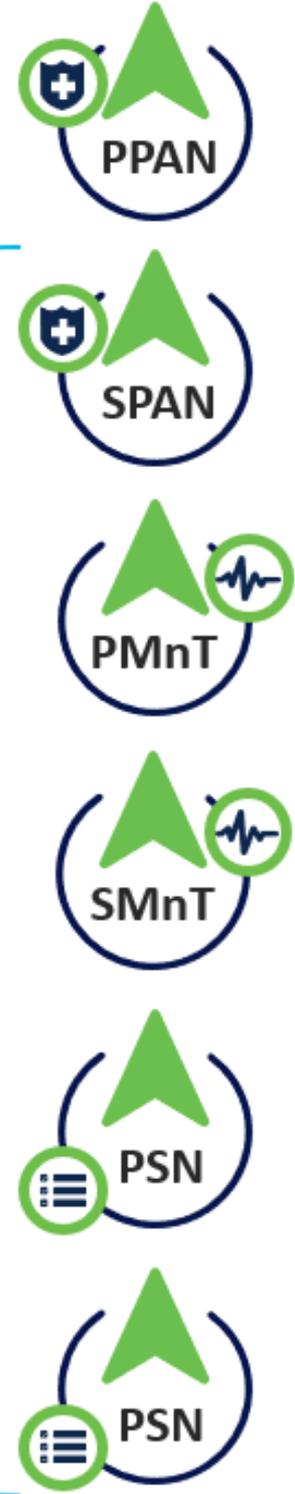
Sono necessari solo due passaggi per l'aggiornamento alla versione più recente di una distribuzione completa.

Pre upgrade



1

Post upgrade



2

Anche in questo caso, considerando circa 240 minuti per ciascuna fase, il processo di aggiornamento totale è ora ridotto a 240×2 minuti = 8 ore.

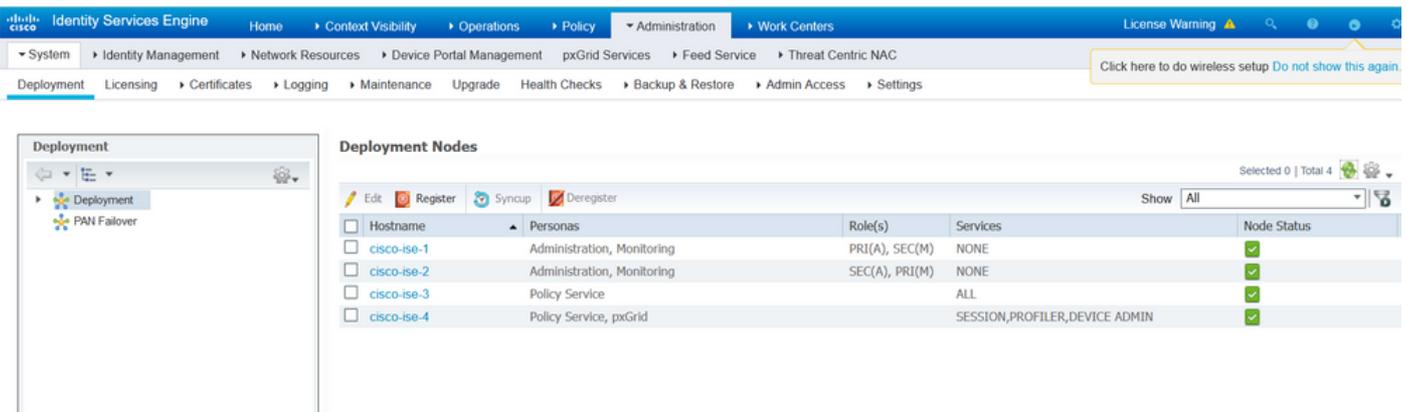
Vantaggi dell'aggiornamento completo rispetto al metodo di aggiornamento suddiviso

- Il metodo di aggiornamento completo richiede meno tempo per l'attività complessiva in quanto i nodi vengono aggiornati in parallelo, mentre il metodo di aggiornamento diviso deve essere pianificato correttamente con una durata maggiore della finestra di manutenzione.
- Il metodo di aggiornamento completo non presenta problemi in termini di sequenza di aggiornamento, poiché prevede solo 2 passaggi. Il metodo Split Upgrade richiede che i nodi siano disposti in sequenza in modo appropriato prima di avviare il processo di aggiornamento.
- Il metodo Full Upgrade conserva i ruoli e le persone così come erano prima dell'aggiornamento. Il metodo Split Upgrade cambia i ruoli di amministratore primario e secondario nella versione aggiornata.
- I punti di errore sono stati ridotti nel metodo di aggiornamento completo eliminando la dipendenza dell'API dalle modifiche relative alla distribuzione durante il processo di aggiornamento.
- Il metodo Full Upgrade consente di tenere traccia dello stato di aggiornamento dal nodo di amministrazione secondario quando il nodo di amministrazione principale diventa inattivo per un aggiornamento. Ciò non è possibile nel metodo Split Upgrade.
- L'installazione delle patch dopo l'aggiornamento è automatizzata e viene fornita come opzione nel metodo di aggiornamento completo.

 **Attenzione:** l'aggiornamento completo richiede un tempo di inattività completo perché tutti i PSN non sono disponibili per l'aggiornamento contemporaneamente. Verificare che l'attività sia pianificata durante un intervento di manutenzione pianificato.

Flusso di aggiornamento completo

Questo documento illustra il flusso di aggiornamento di una distribuzione a 4 nodi. Il processo complessivo rimane lo stesso per le distribuzioni a due nodi o a più nodi.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main content area displays the 'Deployment Nodes' table, which lists the status of four nodes (cisco-ise-1 to cisco-ise-4). The table includes columns for Hostname, Personas, Role(s), Services, and Node Status. All nodes show a green checkmark in the Node Status column, indicating they are successfully updated.

Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/> cisco-ise-1	Administration, Monitoring	PRI(A), SEC(M)	NONE	<input checked="" type="checkbox"/>
<input type="checkbox"/> cisco-ise-2	Administration, Monitoring	SEC(A), PRI(M)	NONE	<input checked="" type="checkbox"/>
<input type="checkbox"/> cisco-ise-3	Policy Service		ALL	<input checked="" type="checkbox"/>
<input type="checkbox"/> cisco-ise-4	Policy Service, pxGrid		SESSION,PROFILER,DEVICE ADMIN	<input checked="" type="checkbox"/>

Aggiorna interfaccia utente

Passare a Amministrazione > Sistema > Aggiorna per avviare l'attività come mostrato nell'immagine.

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

Start Upgrade

 Nota: solo il metodo Split Upgrade è supportato su ISE 2.6 patch 9 e versioni successive, ISE 2.7 patch 3 e versioni successive e ISE 3.0 patch 2 e versioni successive. Per impostazione predefinita, per queste versioni viene visualizzata la finestra Dividi aggiornamento. [Qui](#) è possibile fare riferimento al processo di aggiornamento suddiviso. Selezionare il pulsante di opzione Aggiornamento completo e fare clic su Avvia aggiornamento.

Pagina iniziale

Upgrade

Welcome Checklist Prepare to Upgrade Upgrade Staging Upgrade Nodes Summary

Exit Wizard

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.



Next

Nella procedura guidata della pagina di benvenuto, fare clic su Avanti per continuare.

Elenco di controllo

Esaminare l'elenco di controllo e assicurarsi di completare le attività prima di procedere.

The screenshot shows the Cisco Identity Services Engine (ISE) Upgrade Checklist page. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The Upgrade section is active, showing a progress bar with steps: 1 Welcome, 2 Checklist, 3 Prepare to Upgrade, 4 Upgrade Staging, 5 Upgrade Nodes, and 6 Summary. The Checklist section contains the following tasks:

- 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.

At the bottom, there is a checked checkbox "I have reviewed the checklist", a "Print Checklist" button, and "Back" and "Next" navigation buttons.

Selezionare la casella di controllo che indica che l'elenco di controllo è stato rivisto e fare clic su Avanti.

Preparazione aggiornamento

Un controllo preliminare viene eseguito sull'intera distribuzione prima dell'aggiornamento e i risultati vengono visualizzati in questa pagina. A parte i controlli, in questa fase il bundle di aggiornamento viene scaricato su tutti i nodi, l'aggiornamento dei dati offline (ODU) viene eseguito sul nodo di amministrazione secondario (in modo analogo alla simulazione dello strumento di preparazione all'aggiornamento (URT, Upgrade Readiness Tool) del metodo Split Upgrade) e, infine, visualizza anche la stima del tempo per l'attività.

Il bundle di aggiornamento deve essere scaricato dalla [pagina di download del software Cisco](#).

The screenshot shows a software bundle download page. The bundle is titled "Upgrade bundle for upgrading ISE version 2.6, 2.7, 3.0 to 3.1. This is a signed bundle for image integrity." The date is "11-Aug-2021" and the size is "12607.68 MB". There is a download button (downward arrow) and a shopping cart icon. The bundle name is "ise-upgradebundle-2.6.x-3.0.x-to-3.1.0.518.SPA.x86_64.tar.gz". There is also a link to "Advisories" with an external link icon.

Per eseguire il controllo pre-aggiornamento, selezionare il nome del repository in cui è posizionato il bundle di aggiornamento. Selezionare il nome del file del bundle di aggiornamento dalla casella a discesa Bundle.



Nota: il metodo Full Upgrade introduce anche l'installazione automatica delle patch dopo l'aggiornamento. Il file patch deve essere posizionato nello stesso repository insieme al bundle di aggiornamento e il nome del file patch può essere selezionato dall'elenco a discesa se si desidera l'installazione automatica delle patch.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

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

Upgrade

Home Welcome 2 Checklist 3 Prepare to Upgrade 4 Upgrade Staging 5 Upgrade Nodes 6 Summary

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.xl

Patch None

Start Preparation

Fare clic su Start Preparation (Avvia preparazione) per avviare l'esecuzione dei controlli preliminari. Tutti i controlli preliminari, ad eccezione del controllo Download bundle e Aggiornamento dati di configurazione, scadono automaticamente dopo 4 ore dall'avvio della convalida del sistema. L'aggiornamento dei dati di configurazione, che è solo l'ODU, scade dopo 12 ore.

 Nota: disabilitare l'impostazione di failover PAN prima dell'attività di aggiornamento. Se non viene eseguito manualmente, viene disattivato automaticamente una volta attivato l'aggiornamento.

 Nota: ISE 3.0 e le versioni elencate richiedono l'uso di Smart Licensing. Non supporta le licenze tradizionali. Se le licenze Smart non sono abilitate o registrate prima dell'aggiornamento, ISE termina il periodo di valutazione delle licenze Smart per impostazione predefinita dopo l'aggiornamento. Link di riferimento per la migrazione delle licenze: [Prodotti - ISE Licensing Migration Guide - Cisco](#). L'aggiornamento di ISE da 2. x a 3.x comporta la modifica del livello di licenza.

 Attenzione: una volta attivato l'aggiornamento dei dati di configurazione, è necessario evitare tutti i tipi di modifiche alla configurazione di ISE. Eventuali modifiche apportate andranno perse dopo l'aggiornamento.

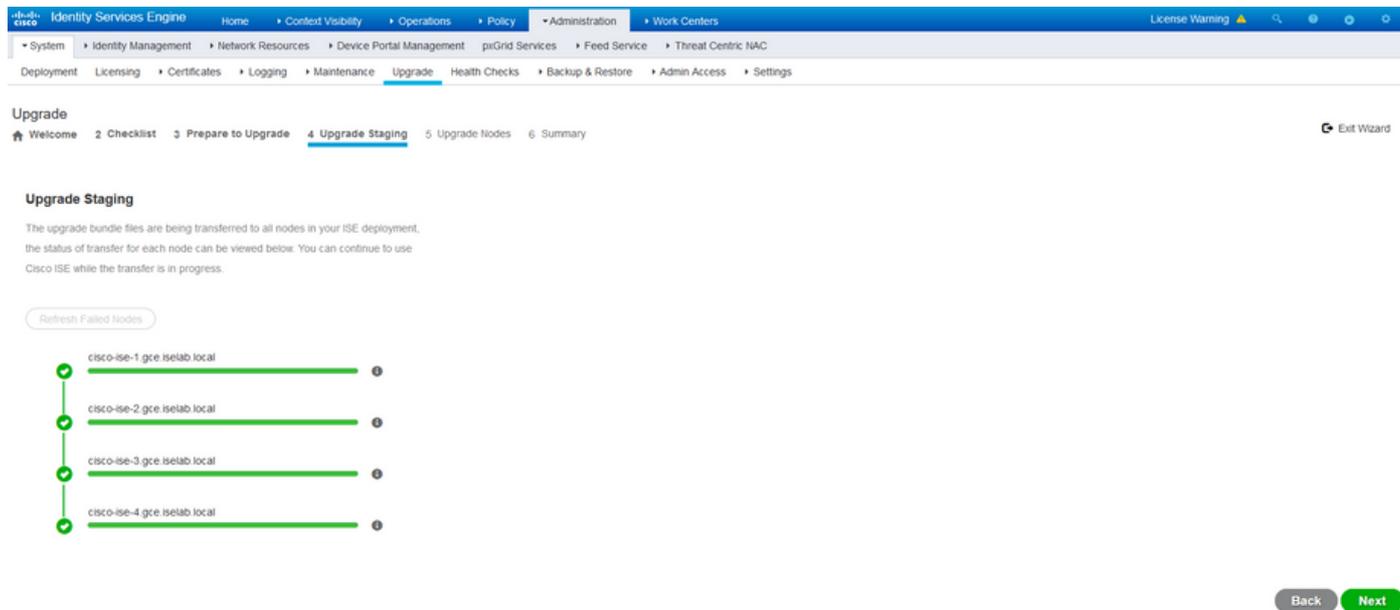
Se i controlli preliminari di uno dei componenti hanno esito negativo, vengono visualizzati in rosso o arancione in base alla criticità. Le carenze evidenziate in rosso devono essere obbligatoriamente corrette prima di procedere ulteriormente. Gli avvisi evidenziati in arancione non possono interrompere il processo di aggiornamento. È tuttavia consigliabile correggerli come procedura ottimale ed evitare di compromettere le funzionalità e le caratteristiche di installazione future.

Una volta corretti gli errori, fare clic su Avvia staging per continuare.

Aggiorna gestione temporanea

Durante la gestione temporanea dell'aggiornamento, il file di database aggiornato viene copiato in tutti i nodi della distribuzione e viene eseguito il backup dei file di configurazione in tutti i nodi della distribuzione.

Il file di dump è già presente nel nodo amministrativo secondario come parte dell'ODU. Pertanto, in questo passaggio il nodo di amministrazione secondario crea solo file di backup per il database CA NSS, le licenze Smart e la configurazione DHCP/DNS. Anche tutti gli altri nodi creano questi file, ma devono copiare il file di dump dal nodo di amministrazione secondario.



Fare clic su Avanti al termine della gestione temporanea per tutti i nodi.

Aggiorna nodi

Per avviare l'aggiornamento, fare clic su Start.

Upgrade

Home Welcome 2 Checklist 3 Prepare to Upgrade 4 Upgrade Staging 5 Upgrade Nodes 6 Summary

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**

Start

Un messaggio popup conferma che l'aggiornamento è attivato e tutti i nodi sono visualizzati in una coda con lo stato di aggiornamento. Poiché l'aggiornamento viene avviato prima sul nodo di amministrazione principale, il sistema si disconnette da questo nodo e ora lo stato dell'aggiornamento può essere monitorato dalla GUI del nodo di amministrazione secondario. Per continuare a visualizzare lo stato, selezionare Amministrazione > Sistema > Aggiorna nella GUI del nodo di amministrazione secondario.

Upgrade

Upgrade Nodes

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

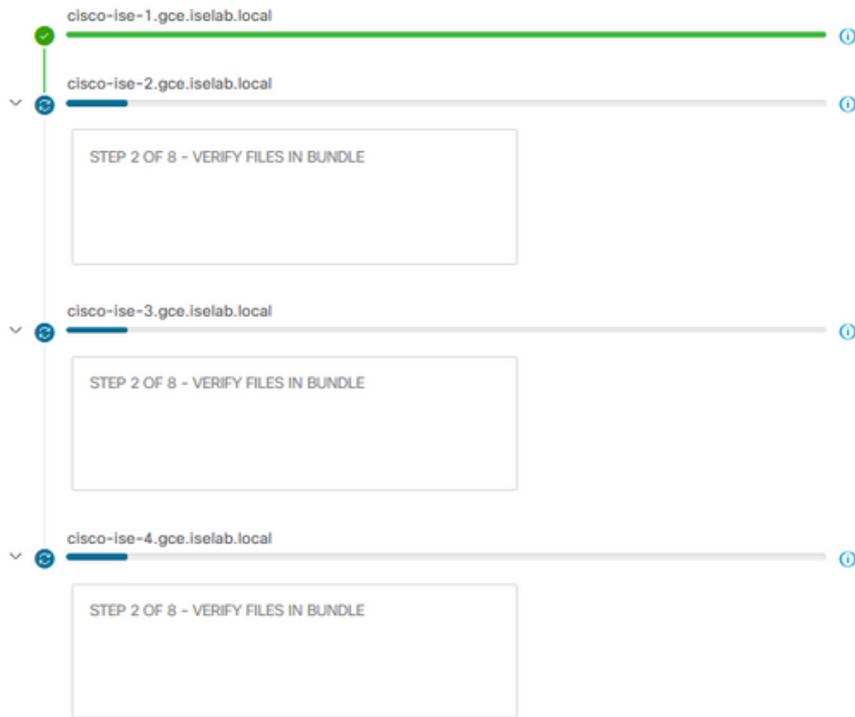


Una volta aggiornato il nodo di amministrazione principale e attivati i servizi, il sistema si disconnette dalla GUI del nodo di amministrazione secondario. Gli utenti possono ora tornare al monitoraggio dello stato dalla GUI del nodo di amministrazione principale mentre tutti gli altri nodi dell'installazione sono inattivi per l'aggiornamento contemporaneamente.



Estimated time of Upgrade process: 5hr 12min

Overall Upgrade Progress 2hr 34min



[Exit Wizard](#)

Una volta completato l'aggiornamento di tutti i nodi, lo stato diventa verde.

Se sono presenti nodi con errori, viene visualizzata una finestra popup con le informazioni sul nodo con errori. Fare clic su OK nella finestra popup per annullare la registrazione dei nodi con errori dalla distribuzione. Questi elementi devono essere aggiornati/re-imaging singolarmente e, se presenti, uniti all'installazione.

Fare clic su Avanti per visualizzare i report riepilogativi complessivi dell'aggiornamento.

Riepilogo

Al termine del processo di aggiornamento, i report di aggiornamento diagnostici per la distribuzione possono essere visualizzati e scaricati da questa pagina.

Controlli integrità

Per convalidare lo stato della distribuzione dopo l'aggiornamento, viene eseguito automaticamente un controllo di integrità per verificare lo stato della distribuzione. Questo report può essere scaricato dalla pagina Riepilogo del flusso di aggiornamento. Se è richiesta una verifica dello stato su richiesta in qualsiasi momento, selezionare Amministrazione > Sistema > Verifiche dello stato, quindi fare clic su Avvia verifiche dello stato.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration · System'. Below this is a menu with options: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, **Health Checks**, Backup & Restore, Admin Access, and Settings. The main heading is 'Health Checks'. Below the heading is a paragraph: '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 successful checking you can go to [Upgrade Workflow](#).' The main content is a list of 13 health checks, each with a progress bar and a status icon. The checks are: 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), and I/O Bandwidth Performance Check (4/4). A message at the bottom says 'Health Checks completed. You can go to Upgrade Workflow.' and there is a 'Download report' button.

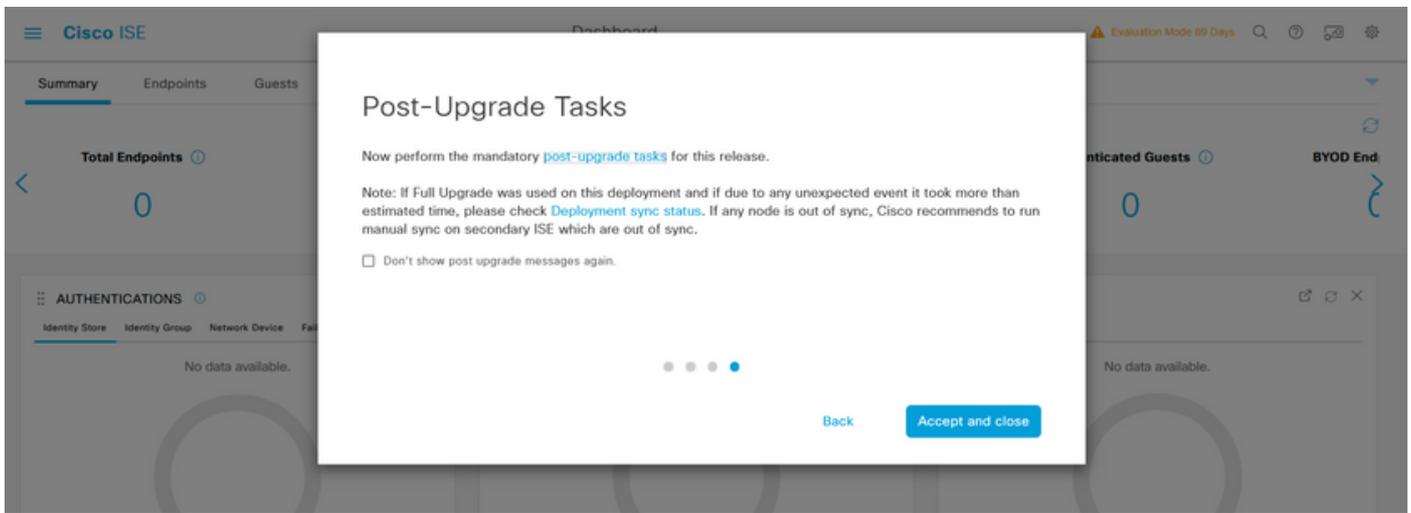
Health Check	Status
Platform Support Check	4/4
Deployment Validation	1/1
DNS Resolvability	4/4
Trust Store Certificate Validation	1/1
System Certificate Validation	4/4
Disk Space Check	4/4
NTP Reachability and Time Source Check	4/4
Load Average Check	4/4
MDM Validation	1/1
License Validation	1/1
Services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

Health Checks completed. You can go to Upgrade Workflow.

[Download report](#)

Task successivi all'aggiornamento

Quando un utente accede alla GUI del nodo di amministrazione principale dopo aver completato l'aggiornamento, viene visualizzato un messaggio popup relativo alle operazioni successive all'aggiornamento.



Fare clic sul collegamento ipertestuale delle attività successive all'aggiornamento nel messaggio popup per esaminare i dettagli delle attività e completarle.

Problemi e rimedi

1. Se l'aggiornamento del nodo di amministrazione primario ha esito negativo, promuovere l'amministratore secondario all'amministratore primario, quindi riprovare a eseguire l'aggiornamento.
2. Se l'aggiornamento ha esito negativo su qualsiasi altro nodo diverso dall'amministratore primario, è necessario annullare la registrazione del nodo dalla distribuzione. Questo nodo deve essere aggiornato singolarmente o con una nuova immagine direttamente alla versione aggiornata e può essere aggiunto nuovamente alla distribuzione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).