

Atualizar o ISE com o método de atualização completo

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Caminhos suportados](#)

[Comparação entre atualização completa e método de atualização dividido](#)

[Sequência de atualização de nó com método de atualização dividido em uma implantação distribuída](#)

[Sequência de atualização de nó com método de atualização completo em uma implantação distribuída](#)

[Vantagens do método de atualização completa sobre divisão](#)

[Fluxo de atualização completo](#)

[Atualizar IU](#)

[Página de boas-vindas](#)

[Lista de verificação](#)

[Preparação para o Upgrade](#)

[Preparação da atualização](#)

[Nós de atualização](#)

[Summary](#)

[Verificações de integridade](#)

[Tarefas de pós-atualização](#)

[Problemas e soluções](#)

Introduction

Este documento descreve como atualizar uma implantação de ISE existente da versão 2.7 para a 3.1 usando o método Full Upgrade. Também inclui como usar o recurso de verificações de integridade para detectar e corrigir possíveis problemas de implantação. O método herdado de atualização é agora chamado de atualização dividida e está disponível como uma opção alternativa se o método de atualização completa não for preferencial.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Identity services engine (ISE)
- Compreensão da terminologia usada para descrever diferentes tipos de implantações do ISE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ISE, versão 2.7, patch 4
- ISE, versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Note: O procedimento é semelhante ou idêntico a outras versões do ISE. Essas etapas podem ser usadas em versões 2.6 e superiores para atualizar para versões 3.1 e superiores do software ISE, a menos que declarado de outra forma.

Caminhos suportados

A atualização completa para o ISE 3.1 é suportada por

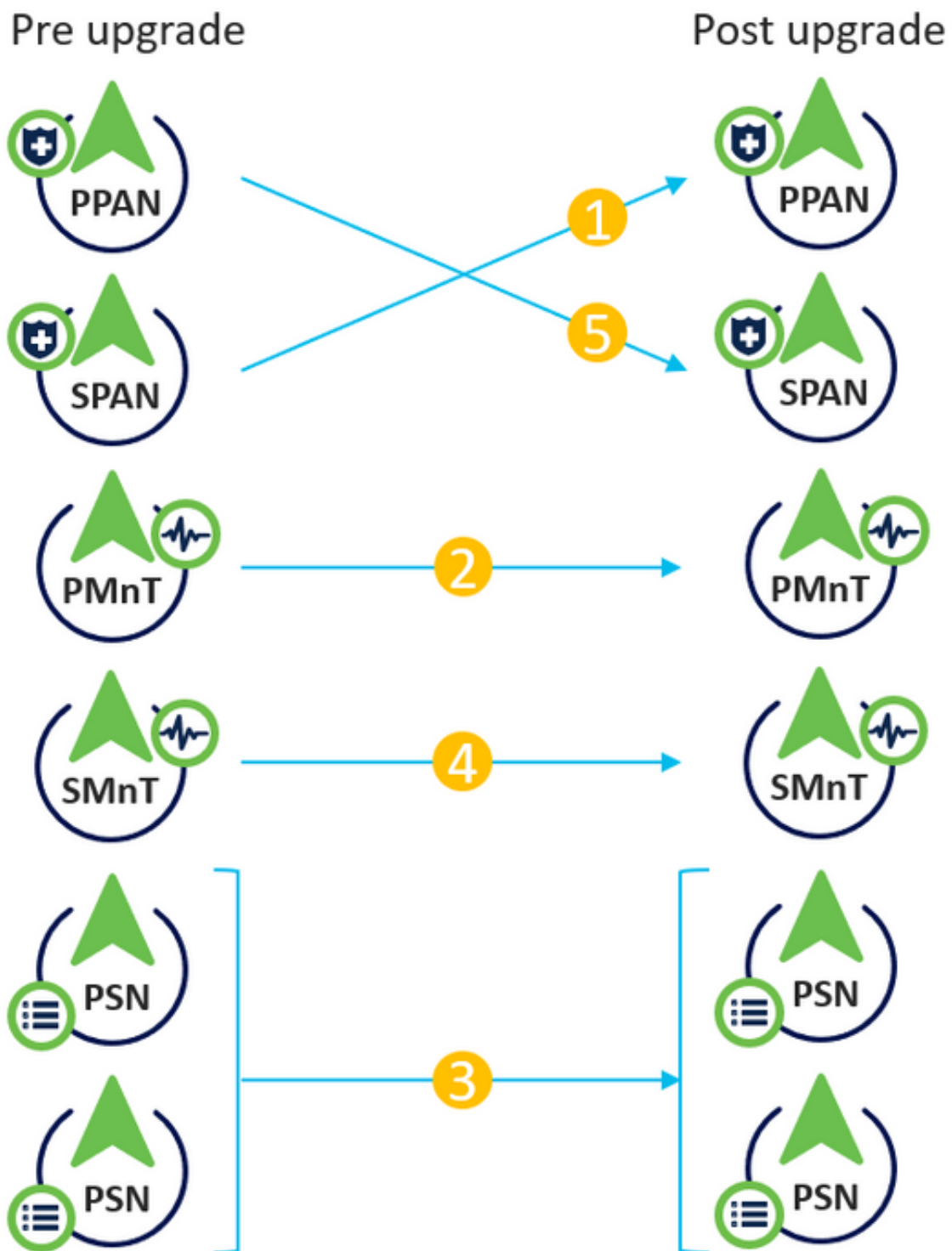
- Patch 10 e superior do ISE 2.6
- ISE 2.7 patch 4 e superior
- ISE 3.0 patch 3 e superior

A atualização dividida para ISE 3.1 é suportada a partir do ISE 2.6 e versões anteriores, com ou sem qualquer correção.

Comparação entre atualização completa e método de atualização dividido

Sequência de atualização de nó com método de atualização dividido em uma implantação distribuída

Requer um mínimo de 5 etapas para uma implantação totalmente distribuída atualizar para a versão mais recente.



Considerando aproximadamente 240 minutos para cada etapa, o processo de atualização total aqui levaria 240×5 minutos = 20 horas.

Sequência de atualização de nó com método de atualização completo em uma implantação distribuída

Requer apenas duas etapas para uma implantação totalmente distribuída atualizar para a versão mais recente.

Pre upgrade



1

Post upgrade



2

Novamente, considerando aproximadamente 240 minutos para cada etapa, o processo total de atualização agora é reduzido para 240×2 minutos = 8 horas.

Vantagens do método de atualização completa sobre divisão

- O método de atualização completa consome menos tempo para a atividade geral porque os nós são atualizados em paralelo, enquanto o método de atualização dividida precisa ser

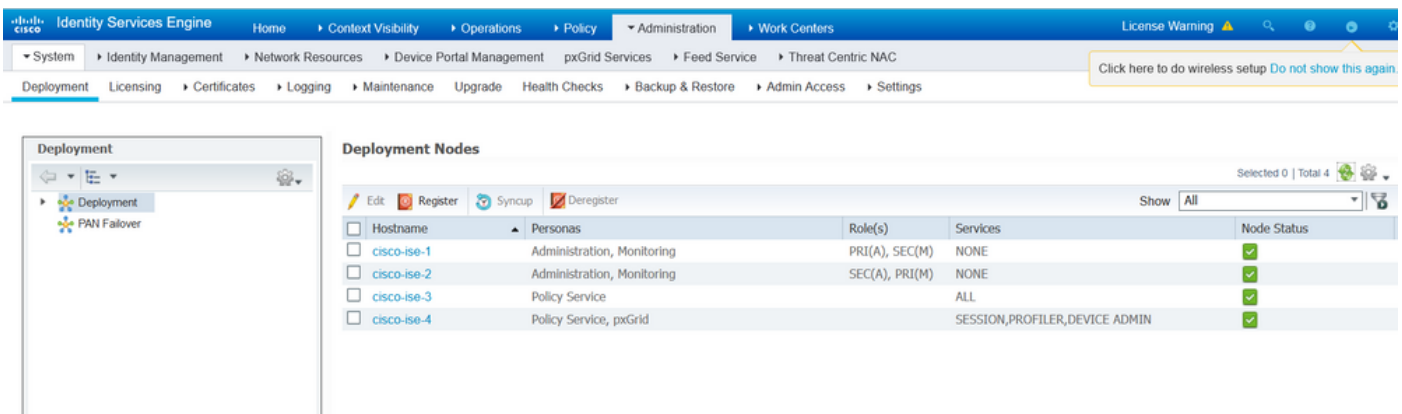
planejado bem com uma duração mais longa da janela de manutenção.

- O método de atualização completa é simples em termos de sequência de atualização, pois há apenas 2 etapas. O método Split Upgrade exige que os nós sejam sequenciados apropriadamente antes de iniciar o processo de atualização.
- O método de atualização completa retém as funções e as pessoas como antes da atualização. O método de atualização dividida comuta as funções de administrador principal e secundária na versão atualizada.
- Os pontos de falhas foram reduzidos no método de atualização completa eliminando a dependência da API com alterações relacionadas à implantação durante o processo de atualização.
- O método Full Upgrade permite rastrear o status da atualização do nó de administrador secundário quando o nó de administrador principal fica inativo para uma atualização. Isso não é possível no método Dividir atualização.
- A pós-atualização da instalação de patches é automatizada e é fornecida como uma opção no método de atualização completa.

Caution: A atualização completa exige um tempo de inatividade completo, pois todos os PSNs são desativados para atualização ao mesmo tempo. Verifique se a atividade está planejada durante uma janela de manutenção programada.

Fluxo de atualização completo

Este documento demonstra o fluxo de atualização de uma implantação de 4 nós. O processo geral permanece o mesmo para implantações de dois nós ou de outros nós múltiplos.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The 'Deployment' section is active, showing a tree view with 'Deployment' and 'PAN Fallover'. The main area displays the 'Deployment Nodes' table with the following data:

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

Atualizar IU

Navegue até **Administration > System > Upgrade** para iniciar a atividade como mostrado na imagem.

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

Note: Somente o método de atualização dividido é suportado no ISE 2.6 patch 9 e inferior, ISE 2.7 patch 3 e inferior e ISE 3.0 patch 2 e inferior. Por padrão, a janela Dividir atualização é iniciada para essas versões. O processo de atualização dividida pode ser chamado [aqui](#). Selecione o botão de opção **Atualização completa** e clique em **Iniciar atualização**.

Página de boas-vindas

Cisco Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

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


Click here to do wireless setup Do not show this again

Upgrade

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

No assistente de página de boas-vindas, clique em **Avançar** para continuar.

Lista de verificação

Revise a lista de verificação e certifique-se de concluir as tarefas antes de prosseguir.

Marque a caixa de seleção que indica que **eu revisei a lista de verificação** e clique em **Avançar**.

Preparação para o Upgrade

Uma pré-verificação é executada na implantação completa antes da atualização e os resultados são exibidos nesta página. Além das verificações, nesta etapa, o pacote de atualização é baixado em todos os nós, a atualização de dados off-line (ODU) é executada no nó de administração secundário (isso é análogo à simulação da ferramenta de preparação para atualização (URT) do método de atualização dividido) e, finalmente, também exibe a estimativa de tempo para a atividade.

O pacote de atualização deve ser baixado da [página Download de software da Cisco](#).

Para executar a verificação de pré-atualização, selecione o nome do repositório no qual o pacote de atualização é colocado. Selecione o nome do arquivo do pacote de atualização na caixa suspensa Pacote.

Note: O método de atualização completa também introduz a instalação automática de patches após a atualização. O arquivo de patch deve ser colocado no mesmo repositório junto com o pacote de atualização e o nome do arquivo de patch pode ser selecionado no menu suspenso se a instalação automática de patch for desejada.

Upgrade

[Home](#)
[2 Checklist](#)
[3 Prepare to Upgrade](#)
[4 Upgrade Staging](#)
[5 Upgrade Nodes](#)
[6 Summary](#)

Prepare to Upgrade

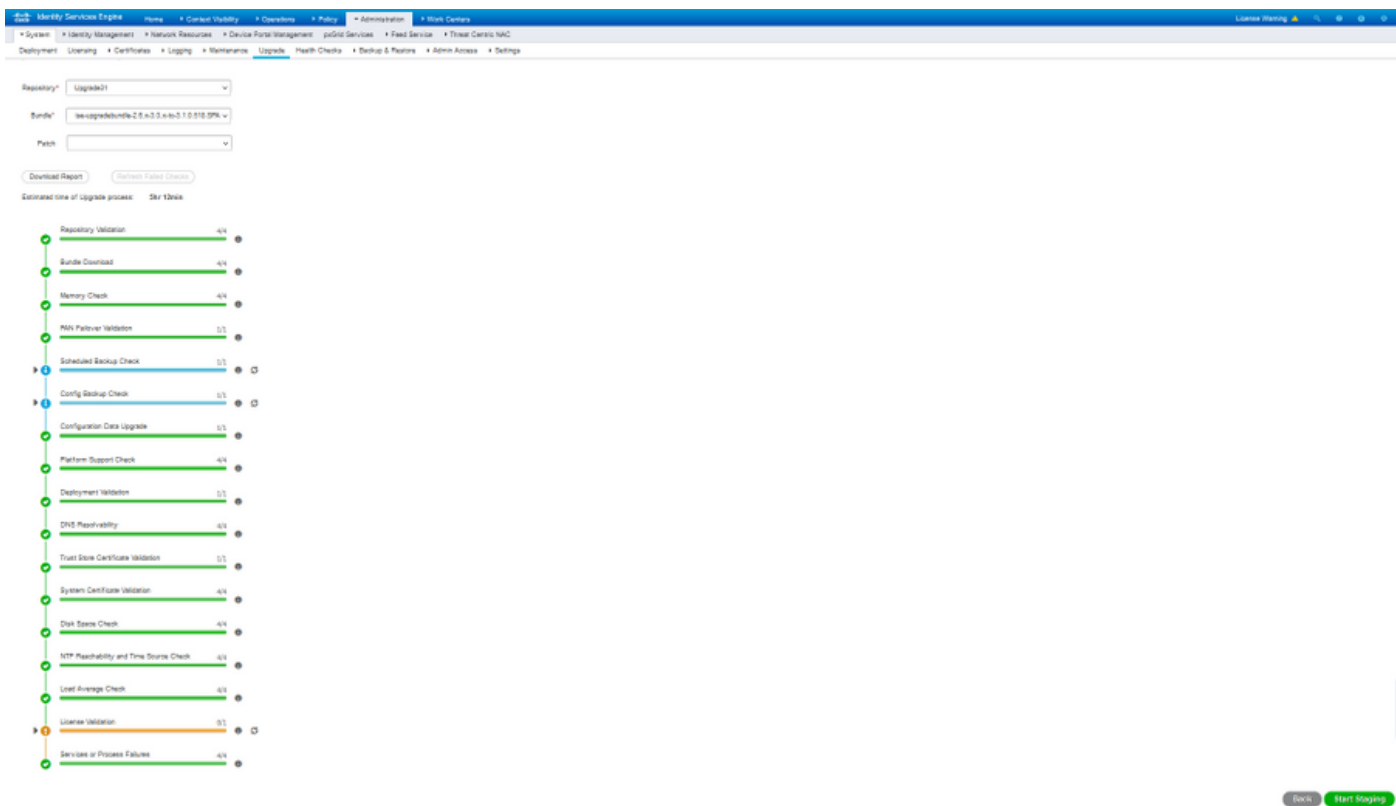
From the following drop-down lists, choose the required repository, upgrade software bundle, and patch file. Then, click Start Preparation.

Repository*

Bundle*

Patch

Clique em **Iniciar preparação** para começar a executar as verificações prévias. Todas as verificações prévias, exceto a verificação de Download de pacote e Atualização de dados de configuração, expiram automaticamente após 4 horas do início da validação do sistema. O Configuration Data Upgrade, que não é mais do que o ODU, expira após 12 horas.



Note: A configuração de failover de PAN deve ser desabilitada antes da atividade de atualização. Se não for feito manualmente, ele será automaticamente desabilitado assim que a atualização for acionada.

Note: O ISE 3.0 e posterior exige o uso do Smart Licensing. Não oferece suporte ao licenciamento tradicional. Caso o Smart Licensing não esteja habilitado ou registrado antes da atualização, o ISE pausa no período de avaliação do Smart Licensing por padrão após a atualização. Link de referência de migração de licença: [Produtos - Guia de Migração de Licenciamento do ISE - Cisco](#). Quando você atualiza o ISE de 2. x a 3.x, envolve alterações de nível de licenciamento. Detalhes disponíveis aqui: [Cisco Identity Services Engine - Perguntas frequentes sobre licença do Cisco ISE - Cisco](#).

Caution: Todos os tipos de alterações de configuração no ISE devem ser evitados quando a atualização de dados de configuração for acionada. Quaisquer alterações feitas seriam perdidas após a atualização.

Se algum dos pré-cheques do componente falhar, eles serão exibidos em vermelho ou laranja com base em sua importância. As falhas destacadas em vermelho precisam ser corrigidas obrigatoriamente antes de prosseguir. Os avisos destacados em laranja não interromperão o processo de atualização, no entanto, é bom corrigi-los como melhores práticas e evitar afetar os recursos e funcionalidades de implantação no futuro.

Depois que os erros forem corrigidos, clique em Start Staging para continuar.

Preparação da atualização

Durante a preparação da atualização, o arquivo de banco de dados atualizado é copiado para todos os nós na implantação e o backup dos arquivos de configuração é feito em todos os nós da implantação.

O arquivo de despejo já está presente no nó de administrador secundário como parte da ODU. Assim, nesta etapa, o nó de administração secundário cria somente arquivos de backup para CA NSS DB, Smart Licensing e configuração DHCP/DNS. Todos os outros nós também criam esses arquivos, mas precisam também copiar o arquivo de despejo do nó de administração secundário.

The screenshot displays the Cisco Identity Services Engine (ISE) administration interface during the upgrade process. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, piGrid Services, Feed Service, Threat Centric NAC, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The 'Upgrade' section is active, showing a progress bar with steps: 1. Welcome, 2. Checklist, 3. Prepare to Upgrade, 4. Upgrade Staging (current), 5. Upgrade Nodes, 6. Summary. Below the progress bar, there is a section titled 'Upgrade Staging' with a message: '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.' A table shows the status of four nodes: cisco-ise-1.gce.iselab.local, cisco-ise-2.gce.iselab.local, cisco-ise-3.gce.iselab.local, and cisco-ise-4.gce.iselab.local. Each node has a green checkmark and a progress bar, indicating successful transfer. At the bottom right, there are 'Back' and 'Next' buttons.

Clique em **Avançar** quando a preparação for concluída para todos os nós.

Nós de atualização

Clique em **Iniciar** para disparar a atualização.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. Under 'Administration', there is a sub-menu with 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Services'. The 'System' sub-menu is expanded, showing 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', and 'Backup & Restore'. The 'Upgrade' option is highlighted. Below the navigation, the 'Upgrade' section is active, showing a breadcrumb trail: 'Welcome', '2 Checklist', '3 Prepare to Upgrade', '4 Upgrade Staging', '5 Upgrade Nodes', and '6 Summary'. The '5 Upgrade Nodes' step is highlighted. The main content area is titled 'Upgrading Nodes' and contains the following text: '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.' Below this text, it states 'Estimated time of Upgrade process: 5hr 12min'. At the bottom of the section, there is a 'Start' button.

Uma mensagem pop-up confirma que a atualização é acionada e todos os nós são exibidos em uma fila com o status da atualização. Como a atualização é iniciada primeiro no nó de administrador principal, o sistema faz logoff desse nó e agora o status da atualização pode ser monitorado na GUI do nó de administrador secundário. Navegue até **Administration > System > Upgrade** na GUI do nó de administrador secundário para continuar a visualizar o status.

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

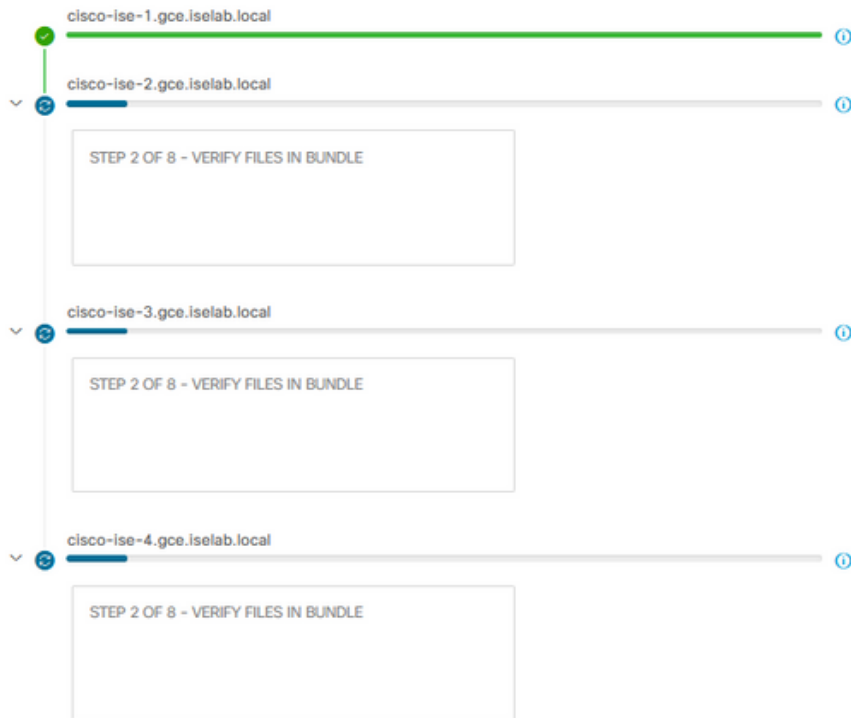
4hr 45min



Quando o nó de administrador principal é atualizado e os serviços são ativados, o sistema faz logoff da GUI do nó de administrador secundário. Agora, os usuários podem voltar para monitorar o status da GUI do nó de administrador principal enquanto todos os outros nós da implantação são desativados para a atualização simultaneamente.



Estimated time of Upgrade process: 5hr 12min



Exit Wizard

Quando todos os nós forem atualizados com êxito, o status será alterado para verde.

Se houver nós com falha, uma janela pop-up com informações sobre o nó com falha será exibida. Clique em **OK** na janela pop-up para cancelar o registro dos nós com falha da implantação. Eles devem ser atualizados/recriados individualmente e associados à implantação, se houver.

Clique em **Avançar** para exibir os relatórios de resumo de atualização geral.

Summary

Após a conclusão do processo de atualização, os relatórios de atualização de diagnóstico para a implantação podem ser exibidos e baixados desta página.

Cisco ISE Administration - System Evaluation Mode 89 Days

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

Welcome Checklist Prepare to Upgrade Upgrade Staging Upgrade Nodes Summary

Summary

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](#)

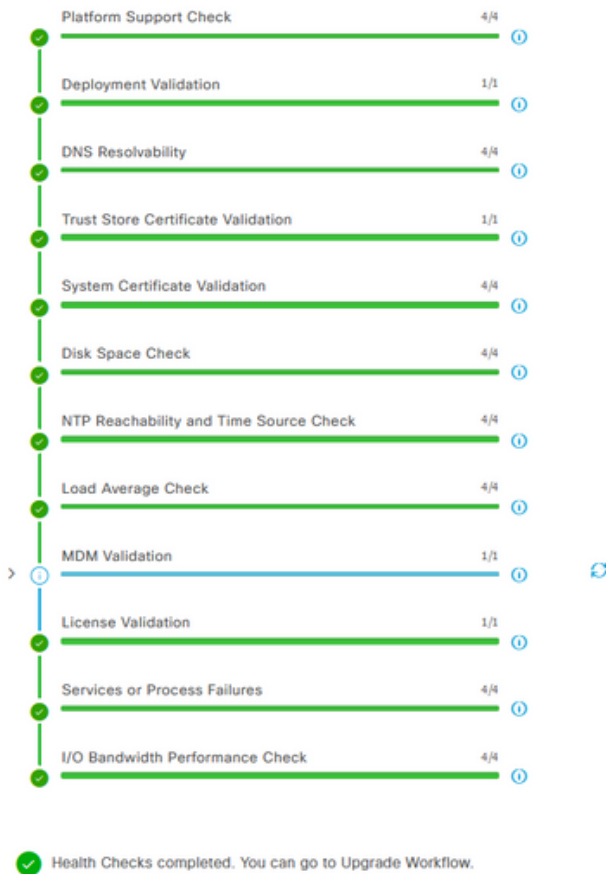
[Exit Wizard](#) [Finish](#)

Verificações de integridade

Para validar o status de implantação após a atualização, uma verificação de integridade é executada automaticamente para verificar o status da implantação. Este relatório pode ser baixado da página Resumo do fluxo de atualização. Se uma verificação de integridade sob demanda for necessária a qualquer momento, navegue para **Administration > System > Health Checks (Administração > Sistema > Verificações de integridade)** e clique em **Start Health Checks (Iniciar verificações de integridade)**.

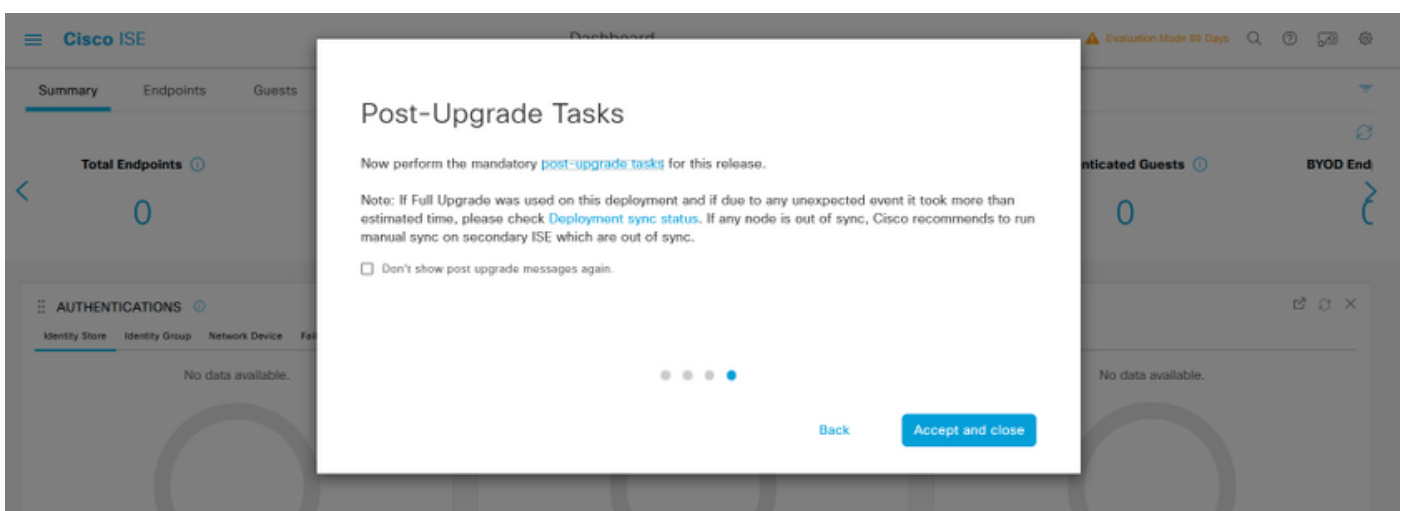
Health Checks

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 successful checking you can go to [Upgrade Workflow](#).

[Download report](#)

Tarefas de pós-atualização

Quando um usuário faz login na GUI do nó de administração principal após concluir a atualização, uma mensagem pop-up é exibida com relação às tarefas pós-atualização.



Clique no hiperlink tarefas pós-atualização na mensagem pop-up para revisar os detalhes da

tarefas e concluí-los.

Problemas e soluções

1. Se a atualização do nó de administrador principal falhar, promova o administrador secundário para o administrador principal e tente novamente a atualização.
2. Se a atualização falhar em qualquer outro nó além do administrador principal, o nó terá que ser removido do registro da implantação. Esse nó terá que ser atualizado individualmente ou recriado diretamente para a versão atualizada e poderá ser adicionado novamente à implantação.