# Lo que necesita saber antes de una actualización de Cisco ISE y Secure Firewall

## Comunidad de Cisco

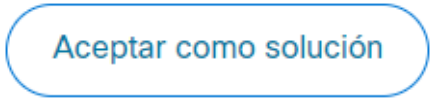
Iván Villegas – Team Captain Security
Ricardo Vera – Escalation Engineer
Michel Lepicard – Technical Consulting Engineer

Jueves 9 de mayo de 2024

# Conecte, Interactúe, ¡Colabore!

## Soluciones

Ayuda a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución” u otórgales un voto de utilidad.




## Votos de utilidad

¡Resalta el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndoles la oportunidad de ganar premios. ¡Reconoce su esfuerzo!


# Premios Spotlight Awards

¡Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros!

Los premios Spotlight Awards se otorgan trimestralmente para reconocer a los miembros más destacados.

Conoce a los ganadores de Noviembre-Enero 2024

¡Ahora también puedes nominar a un candidato! Haga clic aquí

# Nuestros expertos

## Iván Villegas

Team Captain Security

Es Ingeniero en Telemática egresado del Instituto Politécnico Nacional (IPN). Actualmente cuenta con cinco años de experiencia formando parte del equipo del Centro de Asistencia Técnica (TAC) global de Cisco, principalmente en la tecnología de AAA/ISE.

Iván se desempeña como Team Captain enfocado en apoyar a su equipo en soporte técnico y manejo de clientes. Cuenta con las certificaciones de CCNP Enterprise y Security, CCNA y DevNet.

Descarga la presentación https://bit.ly/CL2doc-may24

# Nuestros expertos

## Ricardo Vera

Escalation Engineer

Se incorporó a Cisco en 2021 con el rol de Technical Consulting Engineer en el equipo de Next Generation Firewall.

A lo largo de su carrera profesional se especializó como experto certificado en su tecnología y actualmente se encuentra desempeñando el rol de Escalation Engineer en México, asistiendo a clientes en situaciones complejas alrededor del mundo en colaboración con los equipos de Technical Leaders e Ingeniería.

Descarga la presentación https://bit.ly/CL2doc-may24

# Nuestros expertos

## Michel Lepicard

Technical Consulting Engineer

Se unió a Cisco en 2020 certificándose como experto en el área de networking y desarrollador de aplicaciones. Posteriormente se incorporó al equipo de Next Generation Firewall volviéndose rápidamente en uno de los mejores miembros del equipo.

Actualmente apoya al equipo de BETA poniendo a prueba las nuevas características de los productos para encontrar defectos en el software o desarrollar nuevas áreas de oportunidad.

Descarga la presentación https://bit.ly/CL2doc-may24

slido

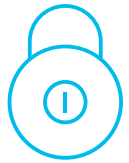
Join at

**slido.com**

**#4114 200**

Passcode: **u9jada**

# Agenda



1. Parte I
    a) Prerrequisitos para actualizar ISE
    b) Validaciones antes de actualizar ISE
    c) Métodos existentes para actualizar ISE
    d) Plan de contingencia
    e) Implicación de la actualización de ISE y FMC
2. Parte II
    a) Descripción general de FTD, FDM y FMC
    b) Tipos de implementaciones en FTD y FMC
    c) Prerrequisitos para una actualización
    d) Actualización de FMC
    e) Actualización de FTD
    f) Plan de Contingencia
    g) Guías y otras referencias

# Prerrequisitos para actualizar ISE

Max. 3 versiones arriba


Actualización intermedia para 4 versiones arriba

# Prerrequisitos para actualizar ISE

- La actualización solo está soportada para Máquinas Virtuales (VMs) y Servidores Físicos (UCS-SNS).
- Actualmente NO está soportado ningún tipo de actualización para instalaciones de ISE en la nube (Azure, Oracle o AWS).

Nota: La instalación de parches sí está soportado en ISE instalado en la nube.

- El único servidor con restricciones es el SNS-3515. Este servidor es compatible con ISE 3.0 máximo, y no puede actualizarse a 3.1 o superior.

# Prerrequisitos para actualizar ISE

- Para actualizaciones en máquinas virtuales, es importante considerar que ISE usa Red Hat (RHEL) para operar en el back-end. Entonces el virtualizador debe ser compatible con la versión de RHEL de ISE.

| Cisco ISE Release | RHEL Release |
|---|---|
| Cisco ISE 2.6 | RHEL 7.5 |
| Cisco ISE 2.7 | RHEL 7.6 |
| Cisco ISE 3.0 | RHEL 7.6 |
| Cisco ISE 3.1 | RHEL 8.2 |
| Cisco ISE 3.2 | RHEL 8.4 |
| Cisco ISE 3.3 | RHEL 8.4 |

Por ejemplo, para VMware la versión ESXi 6.7 o superior es compatible con cualquier nueva versión de ISE.

RHEL 8.2 and later supports the following VMware ESXi versions:

- VMware ESXi 6.7
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2
- VMware ESXi 7.0 U3

# Validaciones antes de actualizar ISE

Una vez elegida la versión a la que se quiere actualizar se deben realizar la verificación de ISE a través de dos métodos:

1. URT Bundle
2. Health Checks

**URT Bundle.**

Este se puede descargar desde https://software.cisco.com/, por ejemplo, para hacer una actualización hacia ISE 3.2 se debe descargar el URT respectivo de ISE 3.2.

# Validaciones antes de actualizar ISE

## Software Download

Downloads Home / Security / Network Visibility and Segmentation / Identity Services Engine / Identity Services Engine Software / Identity Services Engine System Software- 3.2.0

Search...

Expand All | Collapse All

Suggested Release

3.2.0

Latest Release

3.3 Patch 2

HP-CSCwi06794

HP-3.0P8-CSCwi06794

### Identity Services Engine Software

Release 3.2.0

My Notifications

Related Links and Documentation

Release Notes for 3.2.0

| File Information | Release Date | Size |
|---|---|---|
| Upgrade Readiness Tool (URT) to validate config DB upgrade from 2.7,3.0,3.1 to 3.2. This is a signed bundle for image integrity.<br>ise-urtbundle-3.2.0.542a-1.0.0.SPA.x86_64.tar.gz<br>Advisories | 27-Oct-2022 | 962.95 MB |

# Validaciones antes de actualizar ISE

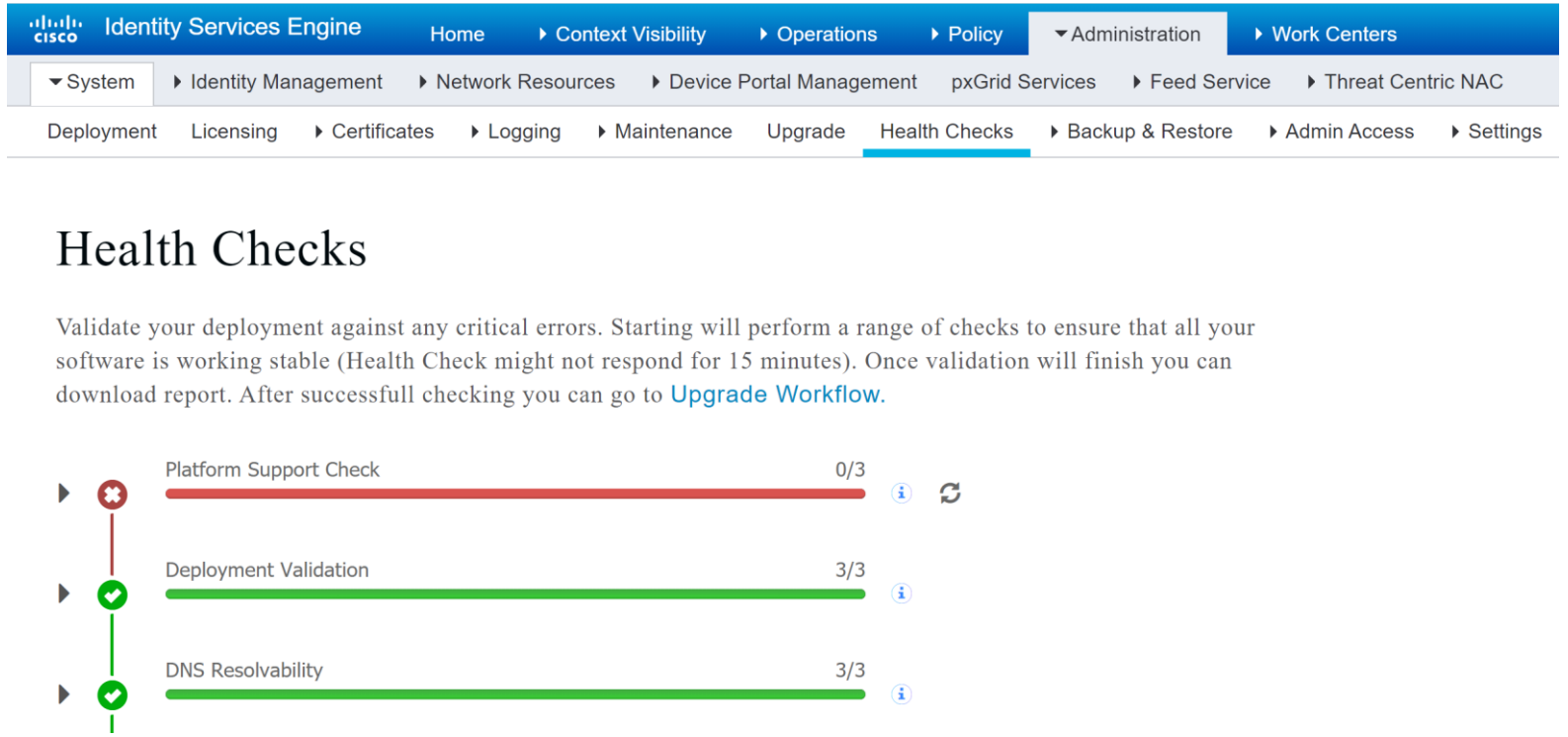
- Posteriormente este URT se debe guardar en un repositorio accesible desde ISE, y para ejecutar la verificación URT se usa el comando:

```
application install <nombre del archivo URT> <nombre del repositorio>
```

- El comando se debe realizar únicamente en el nodo Secundario de Administración, si es un cluster distribuido.
- Si es un solo nodo en el cluster, se hace en ese mismo nodo.

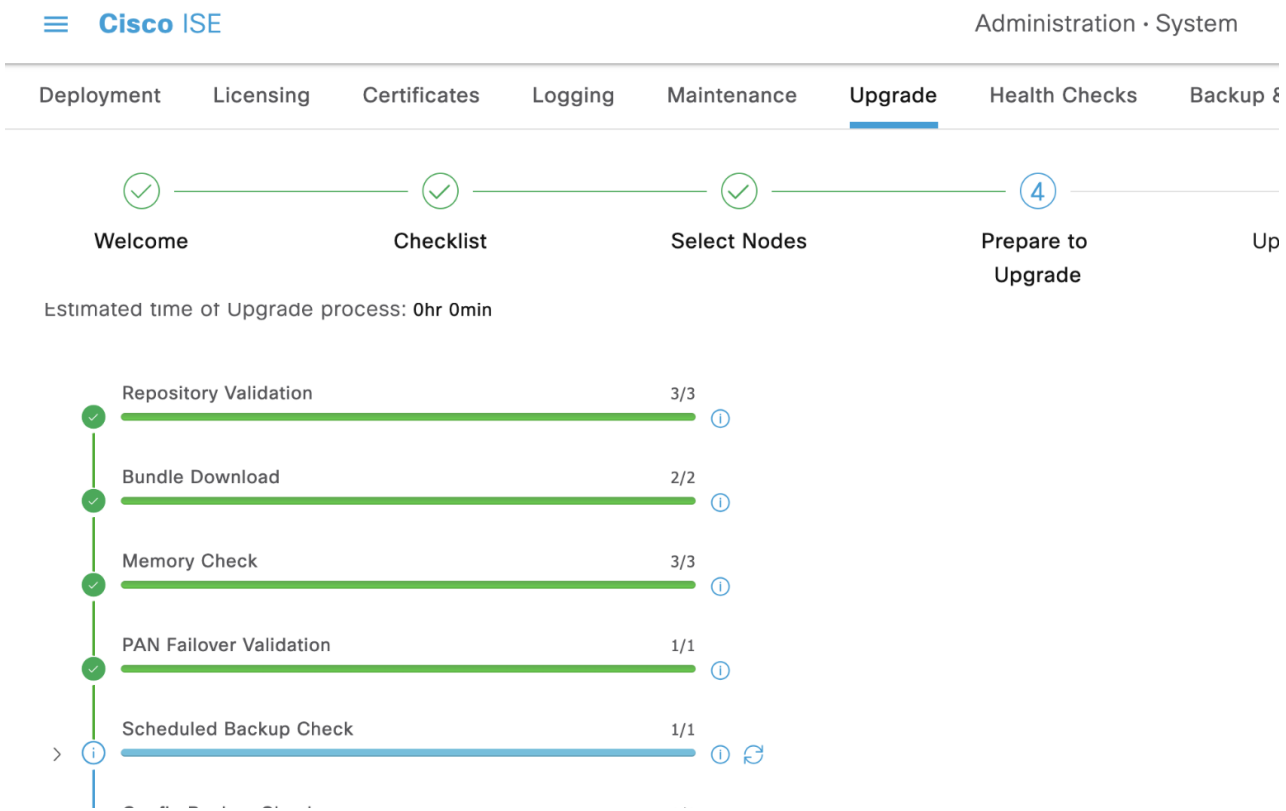
# Validaciones antes de actualizar ISE

- El segundo método que se debe utilizar para verificar ISE son los Health Checks. Está opción fue incluida en ISE 2.7 parche 3, y ISE 3.0 en adelante.
- Se encuentra en Administration > System > Health Checks.



# Validaciones antes de actualizar ISE

- A partir de ISE 3.2 parche 3 ya no es necesario usar el URT bundle, y se puede utilizar solamente los Health Checks, los cuales igual son verificados durante el proceso de actualización:



Active poll

0

Join at

**slido.com**

**#4114 200**

Passcode:

**u9jada**

**¿Qué herramienta se tiene que usar antes de actualizar ISE?**

a) Health check desde la Interfaz Grafica de ISE

0%

b) Solo el URT en el nodo Secundario de Administración

0%

c) URT y Health Checks en versiones anteriores a 3.2 parche 3

0%

# Métodos existentes para actualizar ISE

Existen 3 formas de actualizar ISE.

1. Back up and restore
2. Full Upgrade
3. Split upgrade (CLI)
   - Legacy Split Upgrade
   - New Split Upgrade

# Métodos existentes para actualizar ISE

## Backup and restore

- El primer método, backup and restore, como su nombre lo dice, implica tomar un backup de la configuración de ISE y crear un nuevo nodo desde 0 en la nueva versión deseada, y restaurar el backup de la configuración en este nuevo nodo.

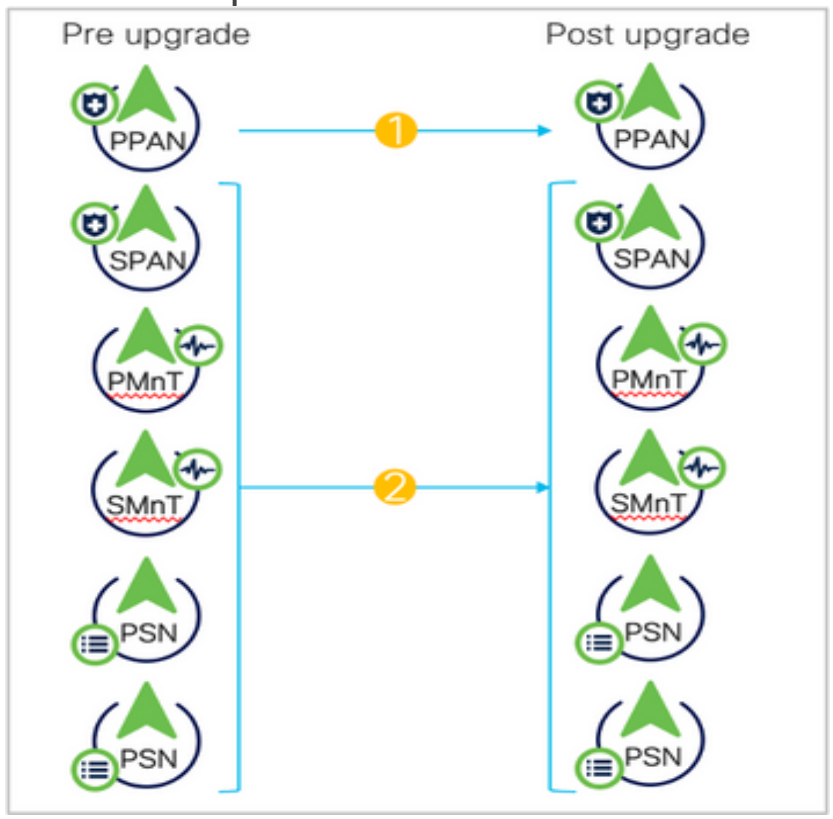
- Si es una actualizació a un cluster, posteriormente se debe apagar los nodos anteriores y reinstalar la nueva versión de ISE en estos, y se procede unir estos nodos al nodo en el cual se restauró la configuración para crear un cluster.

- Este método es ideal para clusters chicos y medianos (menos de 6 nodos) y es menos propenso a fallas, y proporciona disponibilidad (HA) durante el proceso.

# Métodos existentes para actualizar ISE

## Full Upgrade

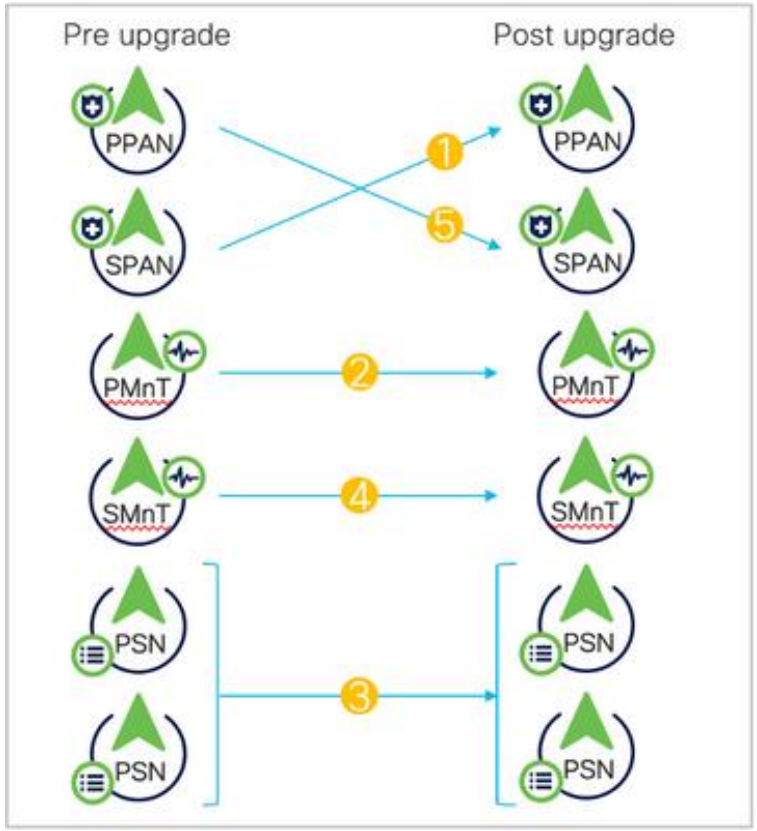
El método de Full Upgrade – es ideal cuando puede existir una ventana de mantenimiento en la cual no importe que los servicios estén fuera, el método full upgrade es el más rápido de todos ya que actualiza el nodo primario de administración y posterior a eso se actualizan todos los demás nodos al mismo tiempo.



# Métodos existentes para actualizar ISE

## Legacy Split Upgrade

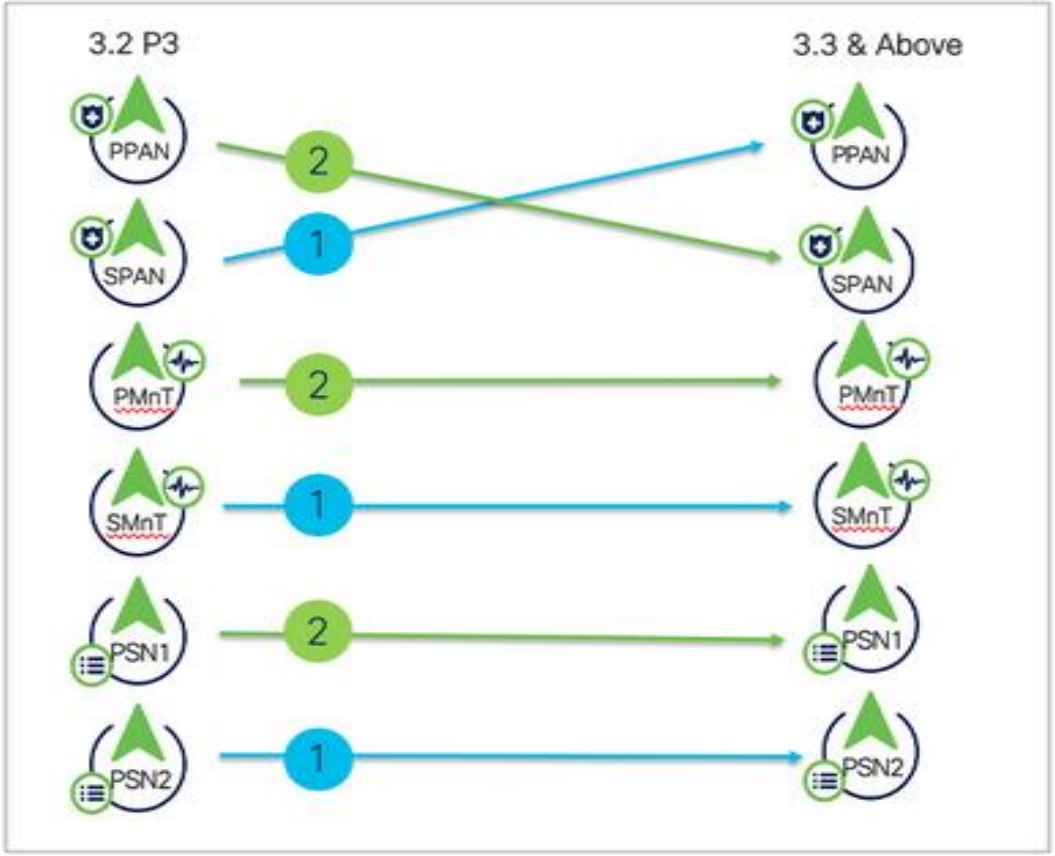
El método de Legacy Split Upgrade – llamado así porque es el usado en versiones anteriores a ISE 3.2 patch 3 – es ideal para clusters grandes, en los cuales se requiere que las autenticaciones sigan funcionando en todo momento. Sin embargo, es un proceso lento, aproximadamente 240 minutos por nodo.



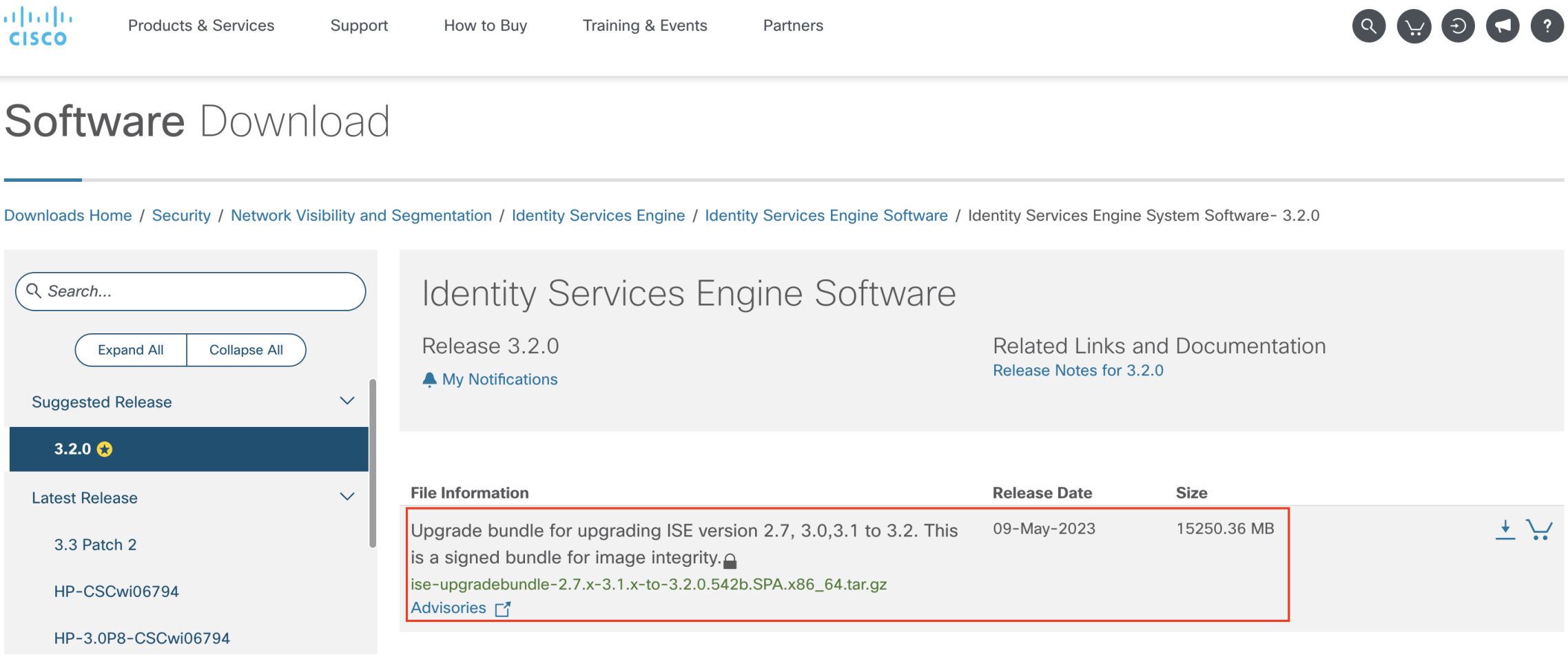
# Métodos existentes para actualizar ISE

## New Split Upgrade

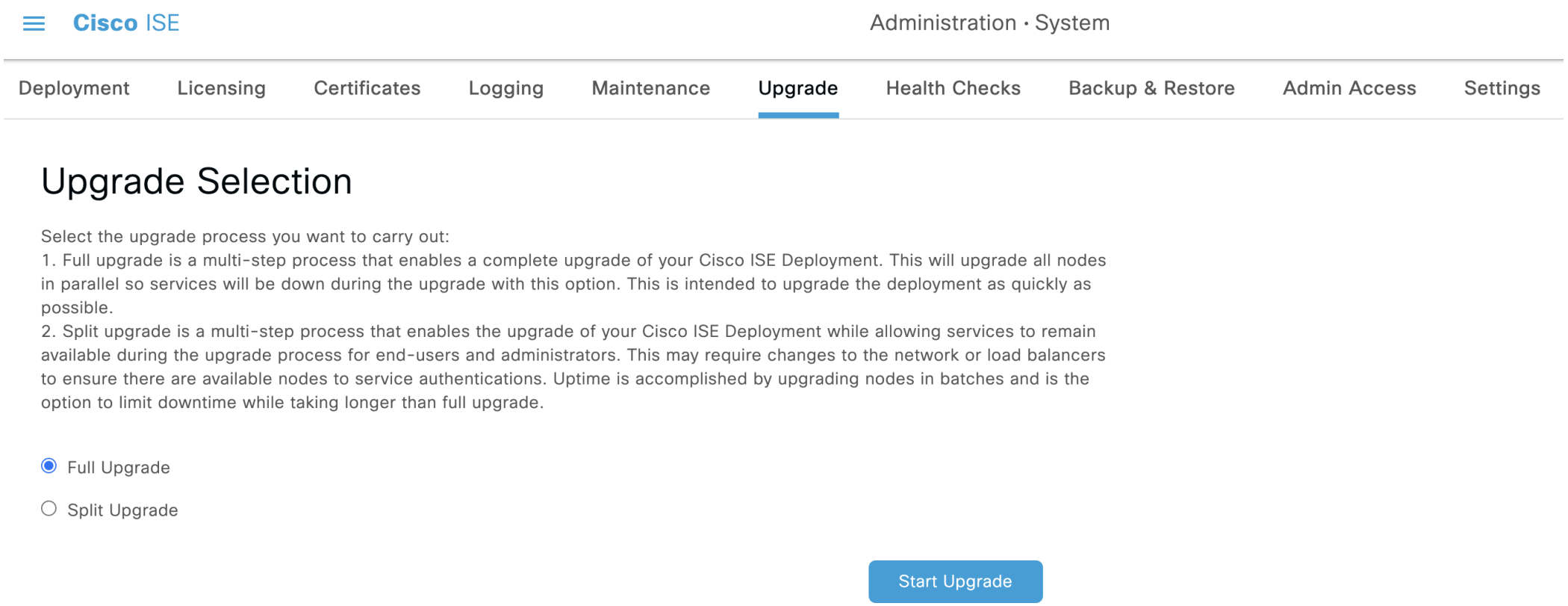
El método de New Split Upgrade - llamado así porque es el usado en ISE 3.2 patch 3 o superior – su objetivo es de igual manera es tener a ISE operando sin interrupción, sin embargo, es más rápido ya que el proceso se hace por iteraciones secuenciales y no por nodos.



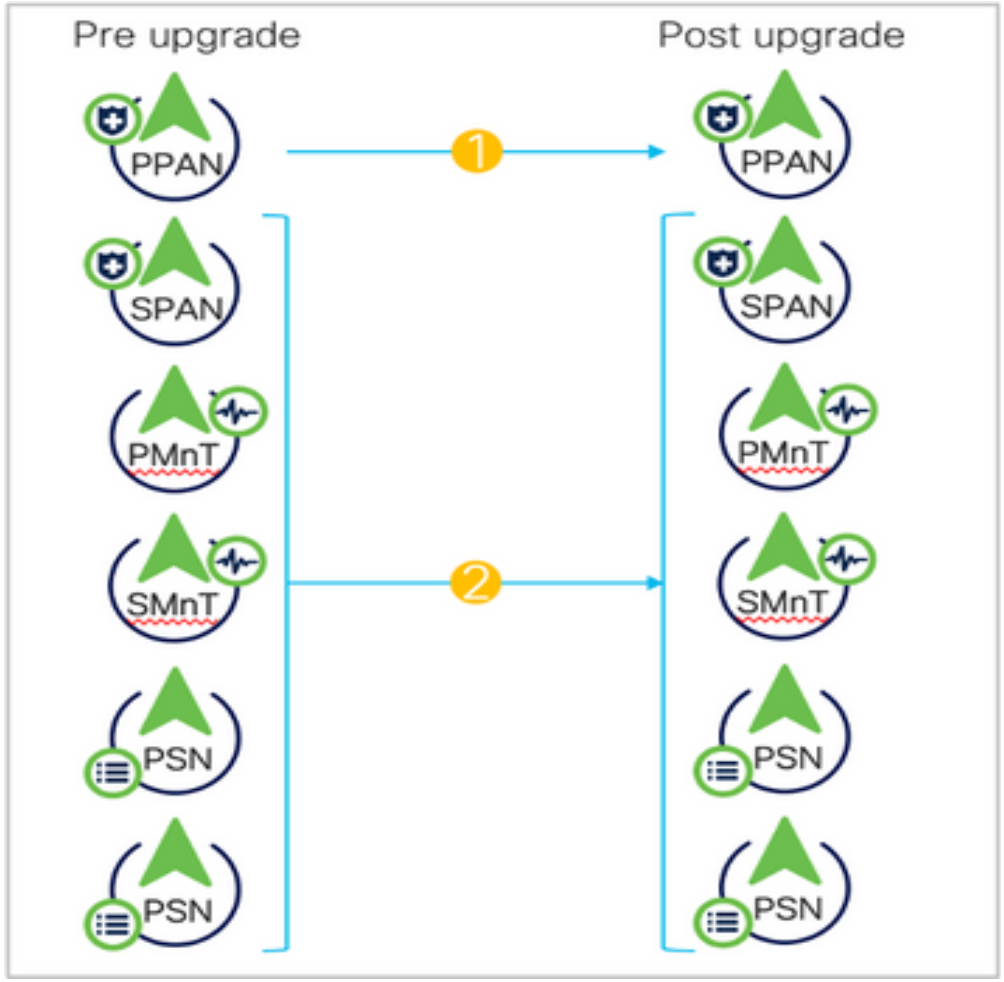
# ¿Dónde empiezo la actualización?



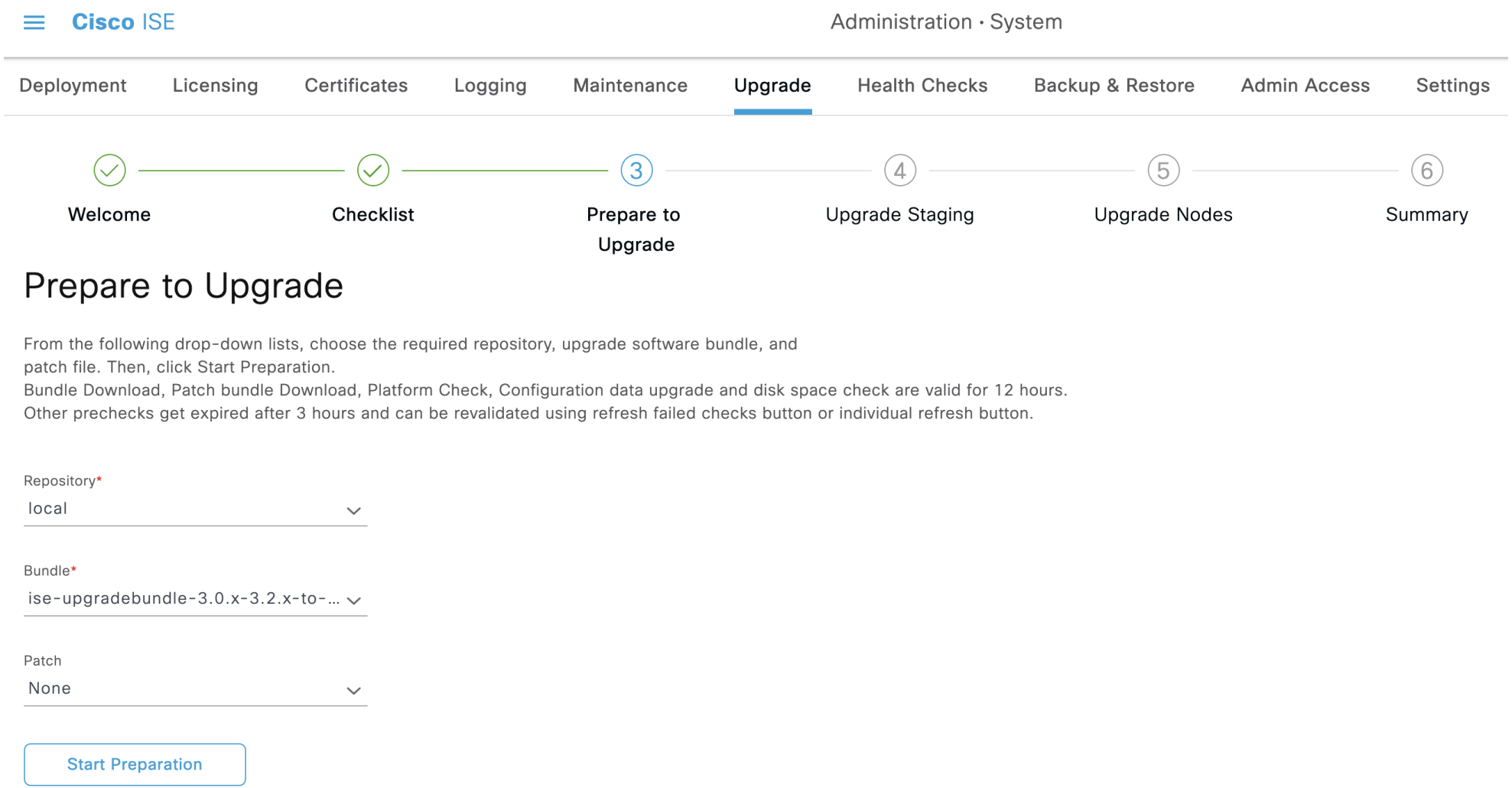
# ¿Dónde empiezo la actualización?



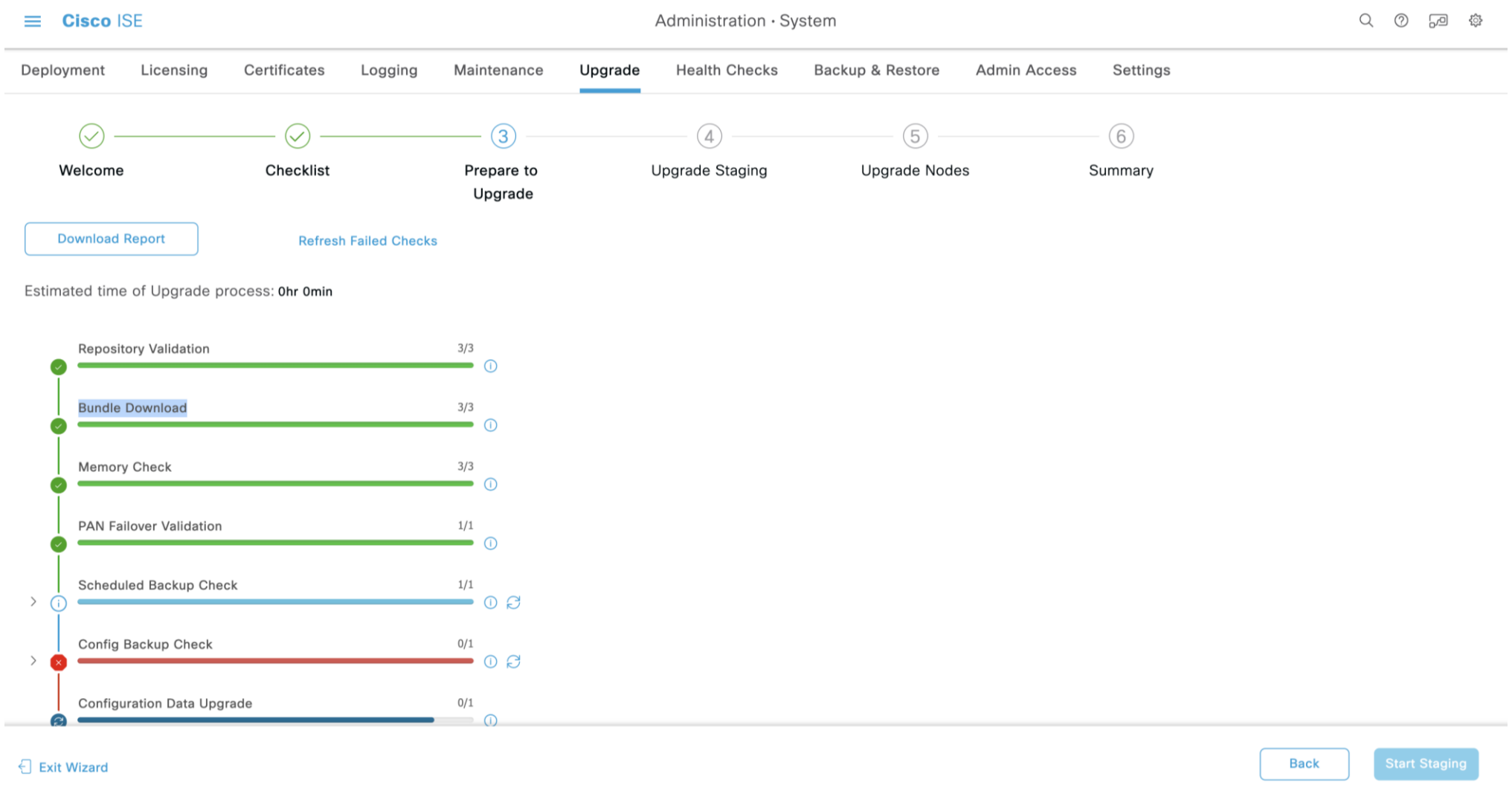
# Ejemplo de Full Upgrade



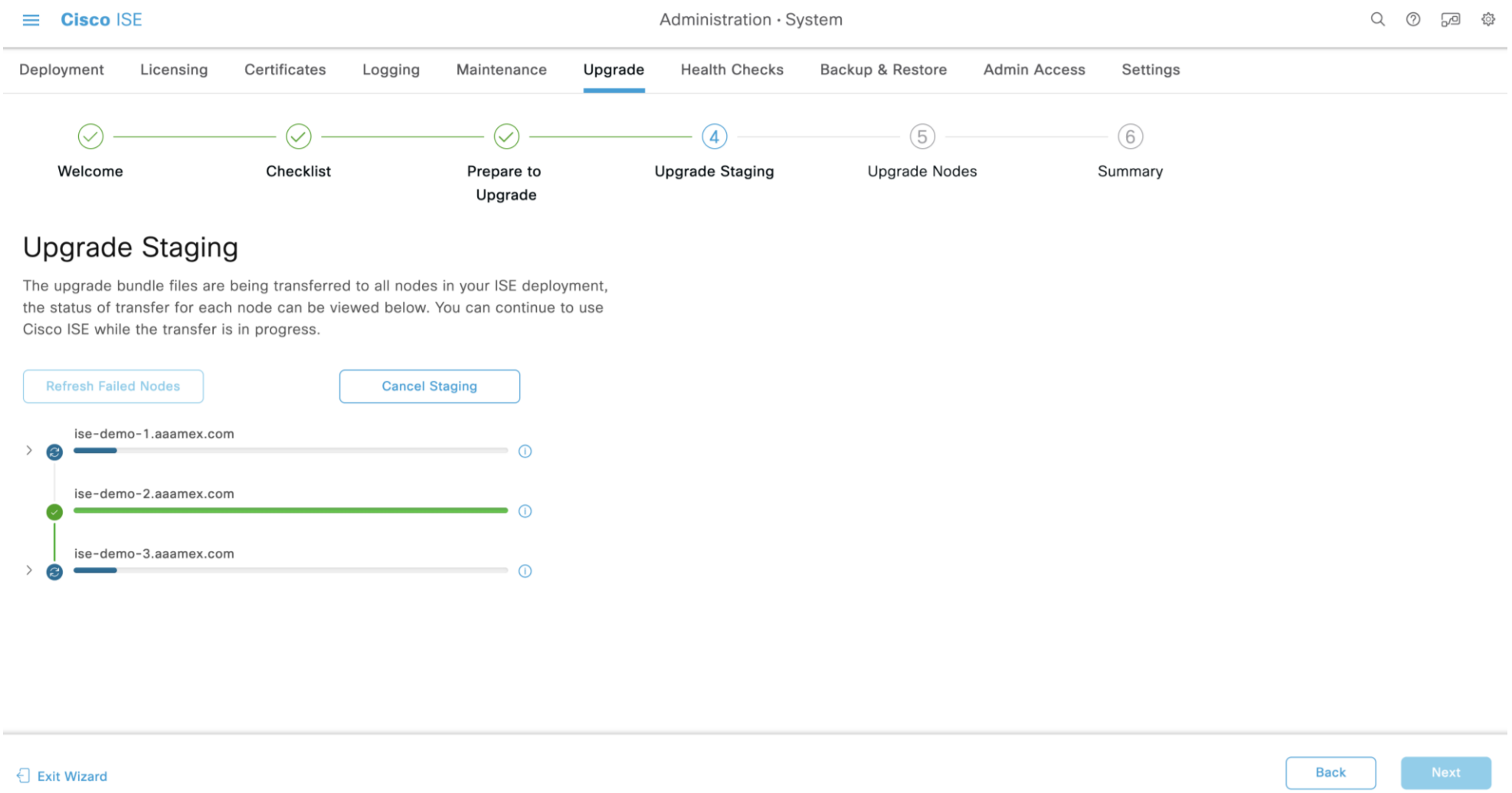
# Ejemplo – Full Upgrade 1/5



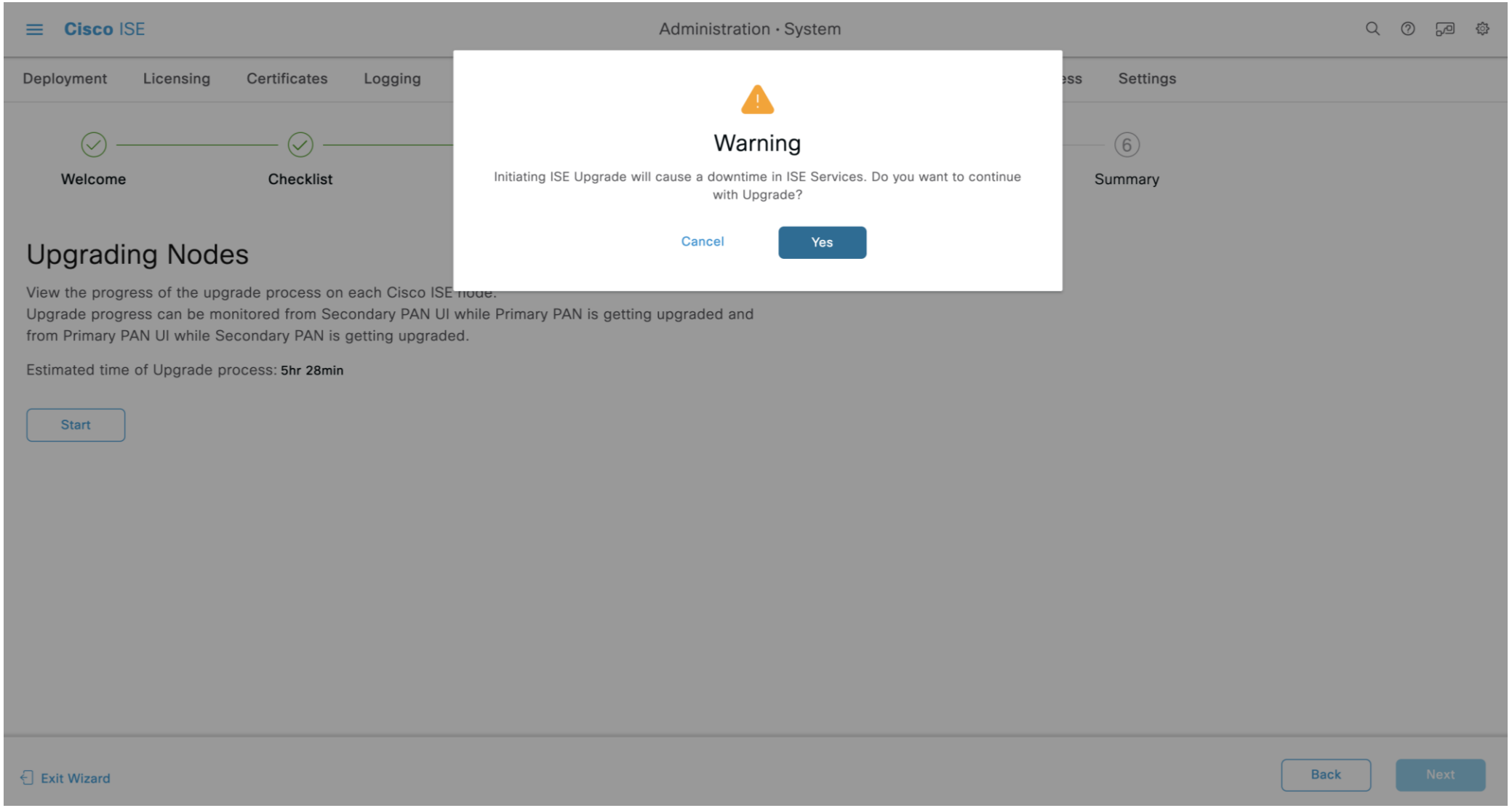
# Ejemplo – Full Upgrade 2/5



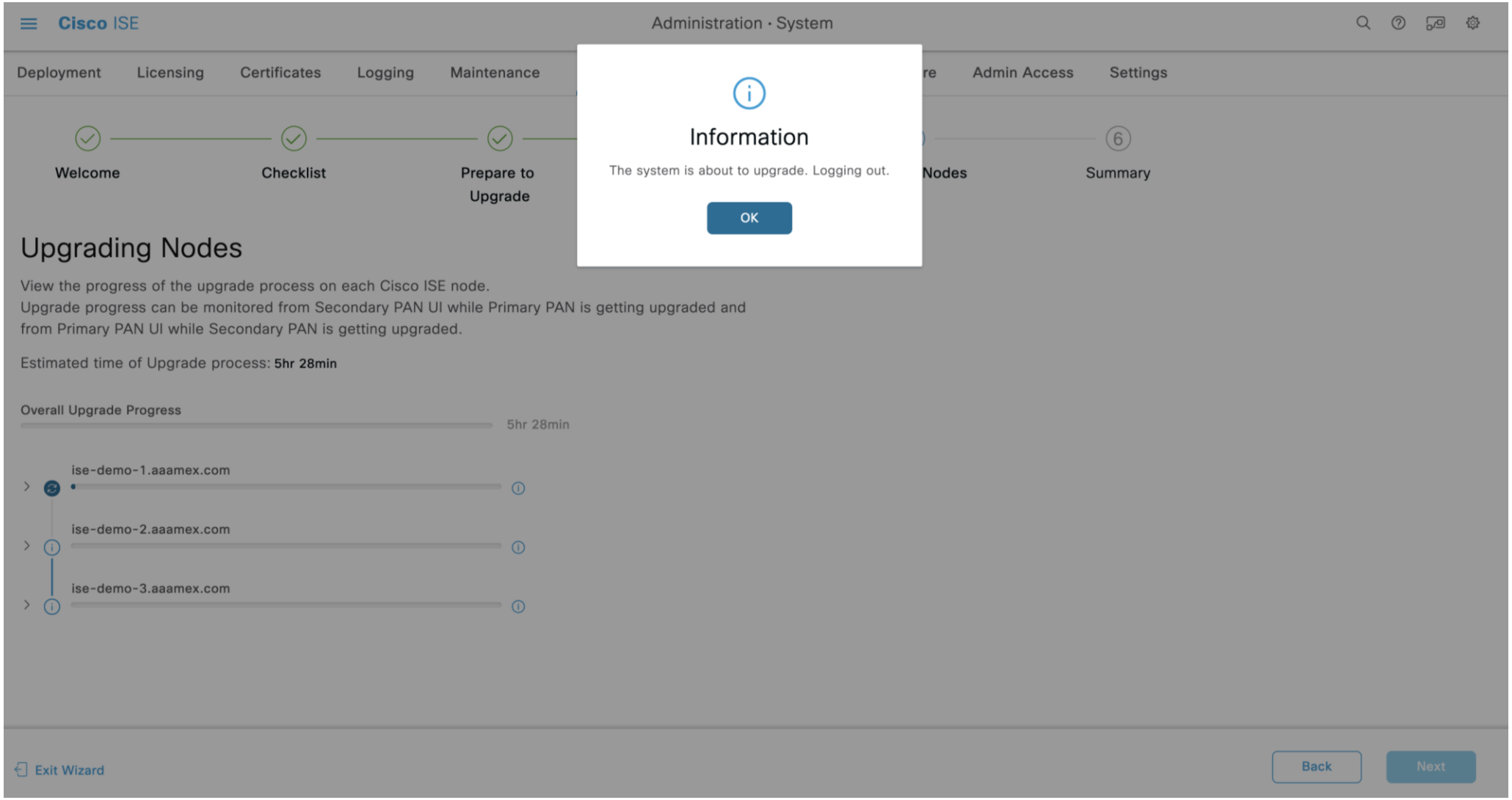
# Ejemplo – Full Upgrade 3/5



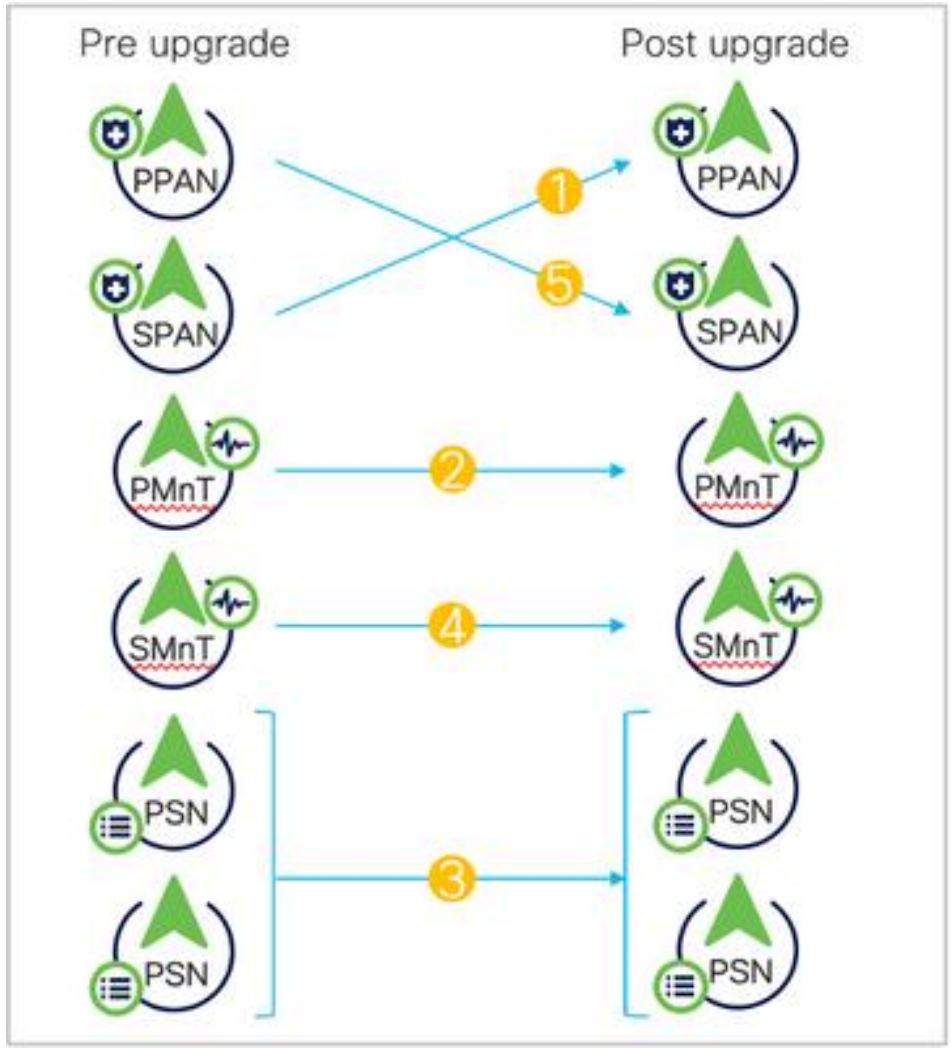
# Ejemplo – Full Upgrade 4/5



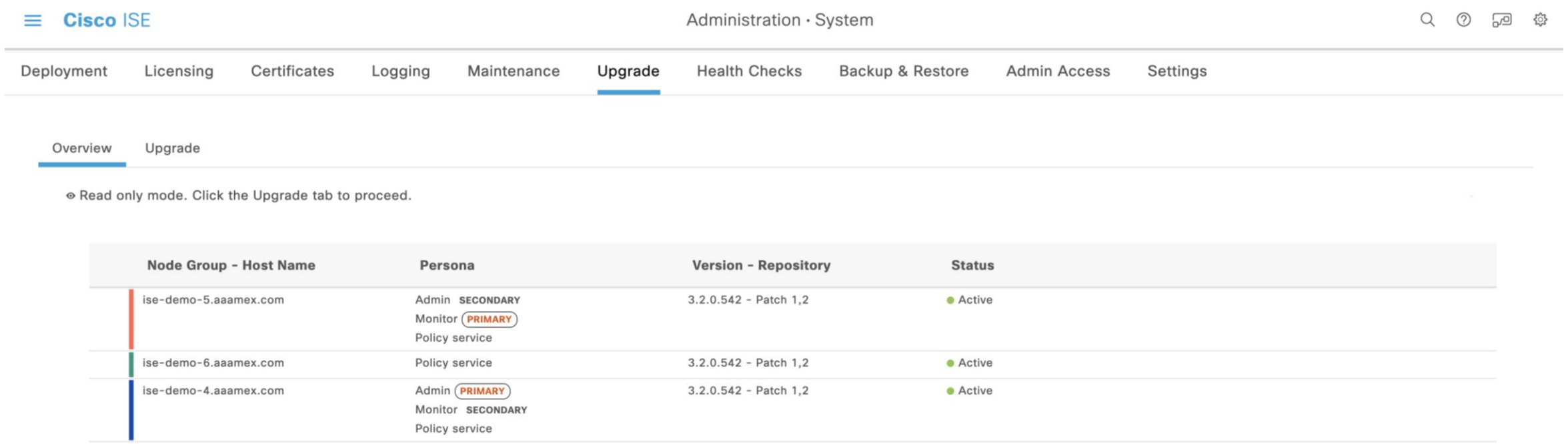
# Ejemplo – Full Upgrade 5/5



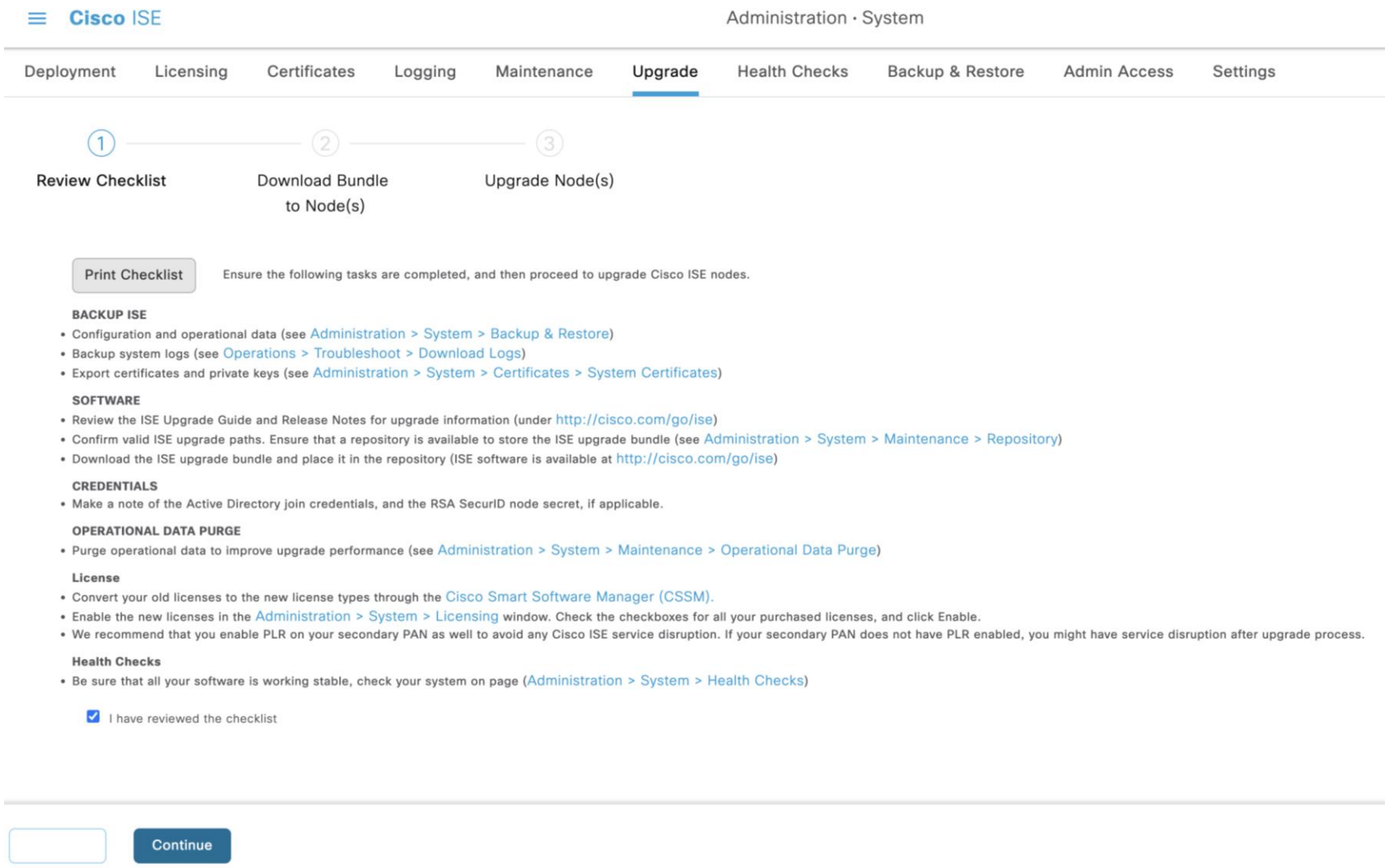
# Ejemplo de Legacy Split Upgrade



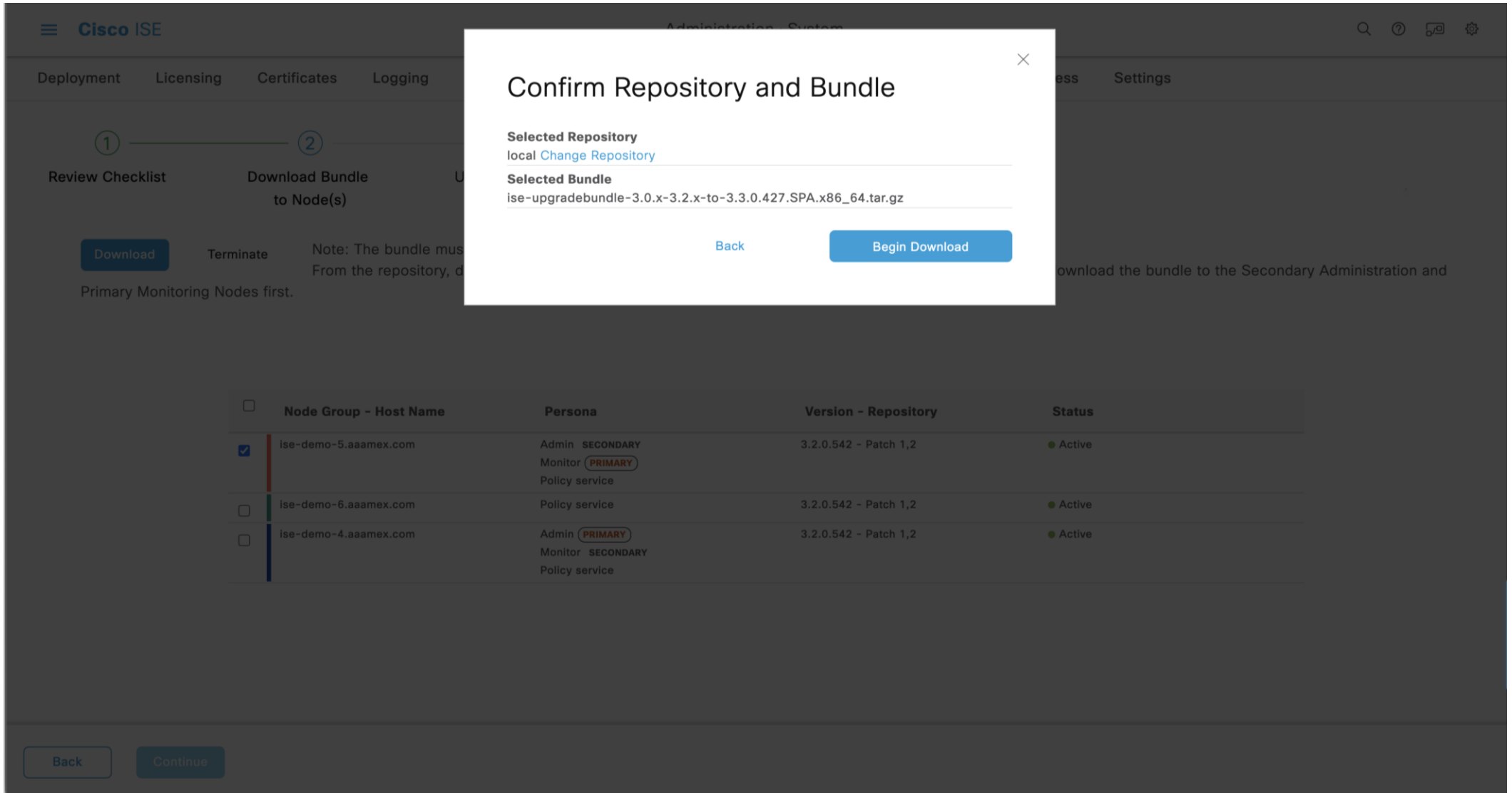
# Ejemplo – Legacy Split Upgrade 1/7



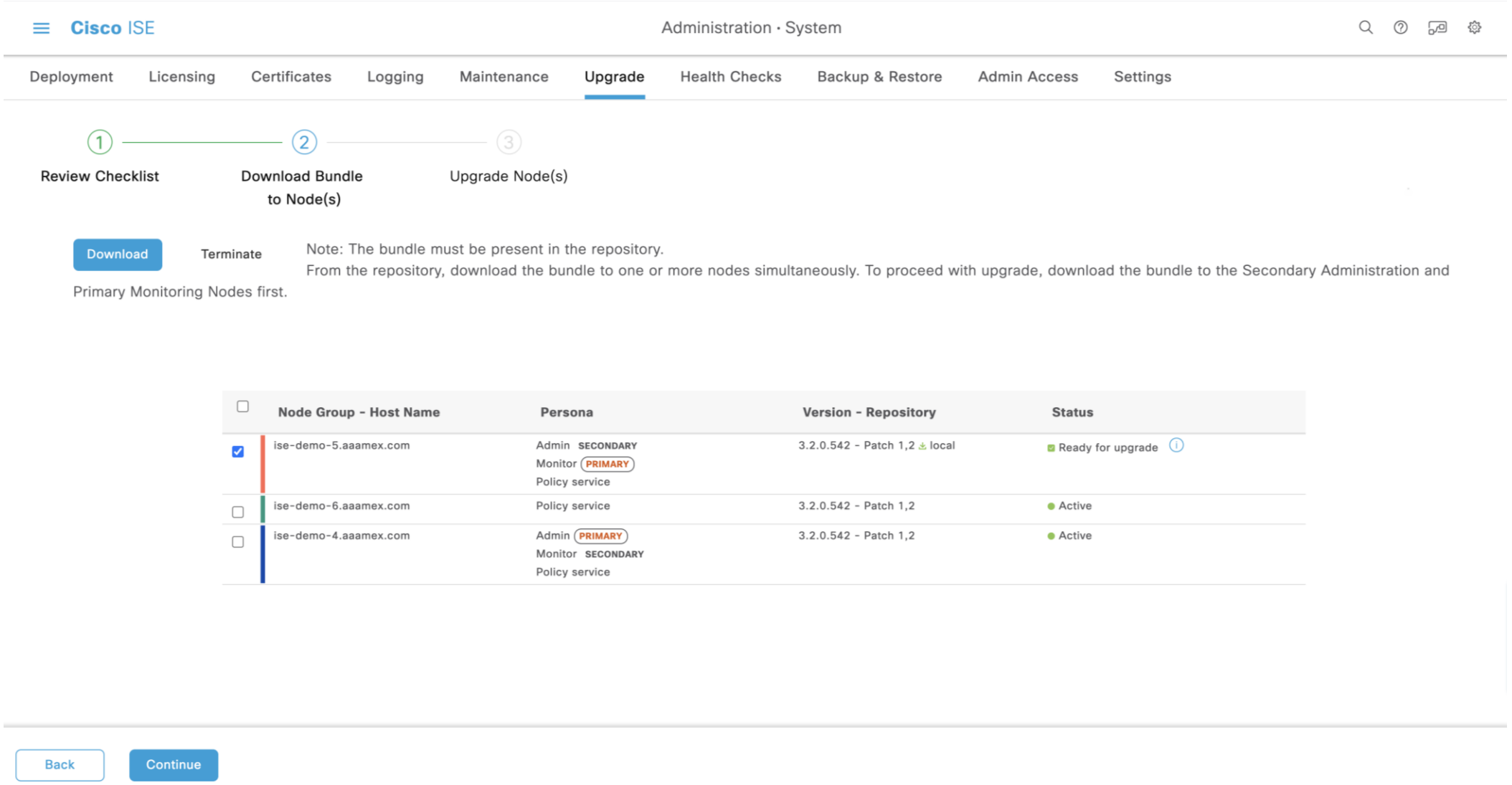
# Ejemplo – Legacy Split Upgrade 2/7



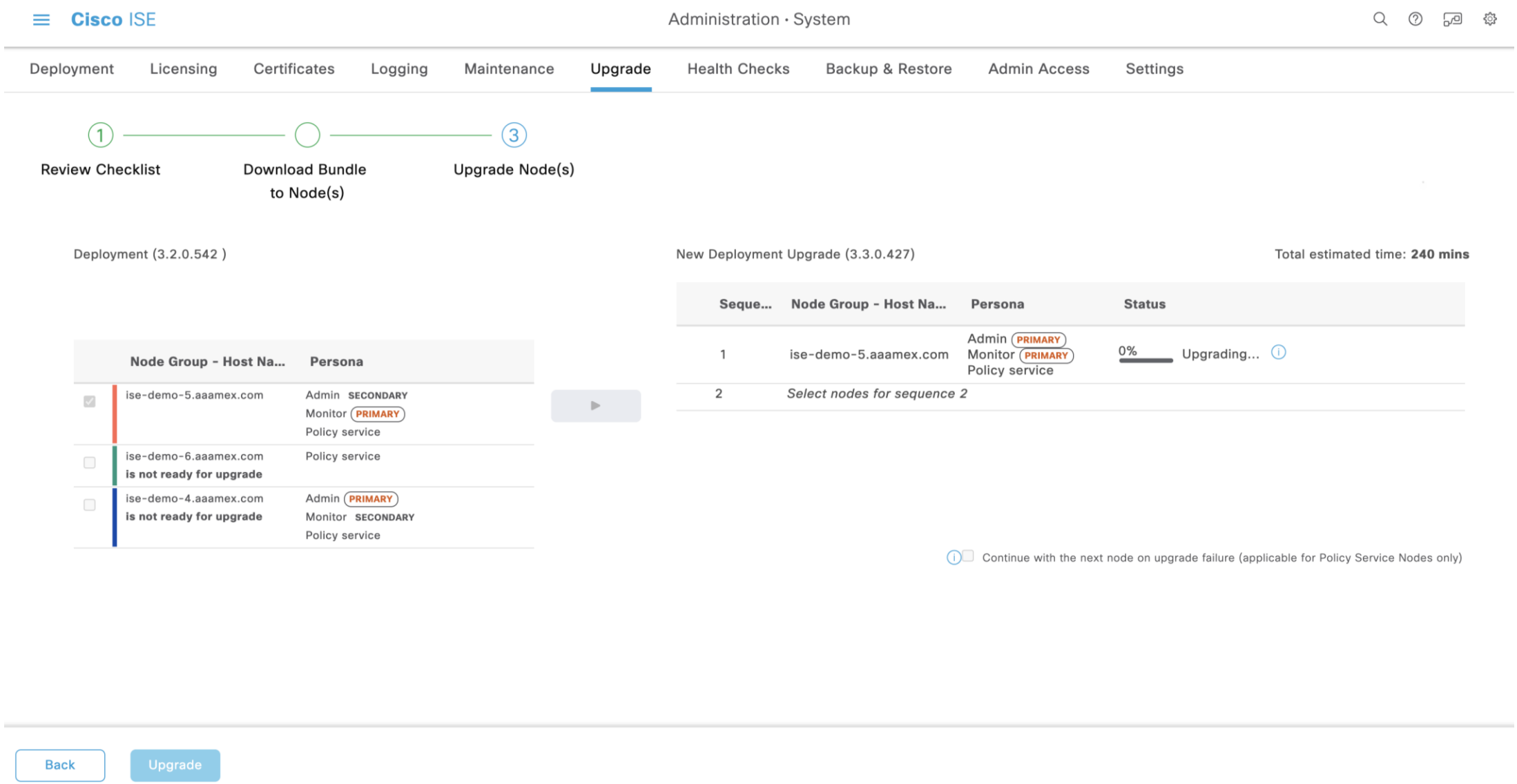
# Ejemplo – Legacy Split Upgrade 3/7



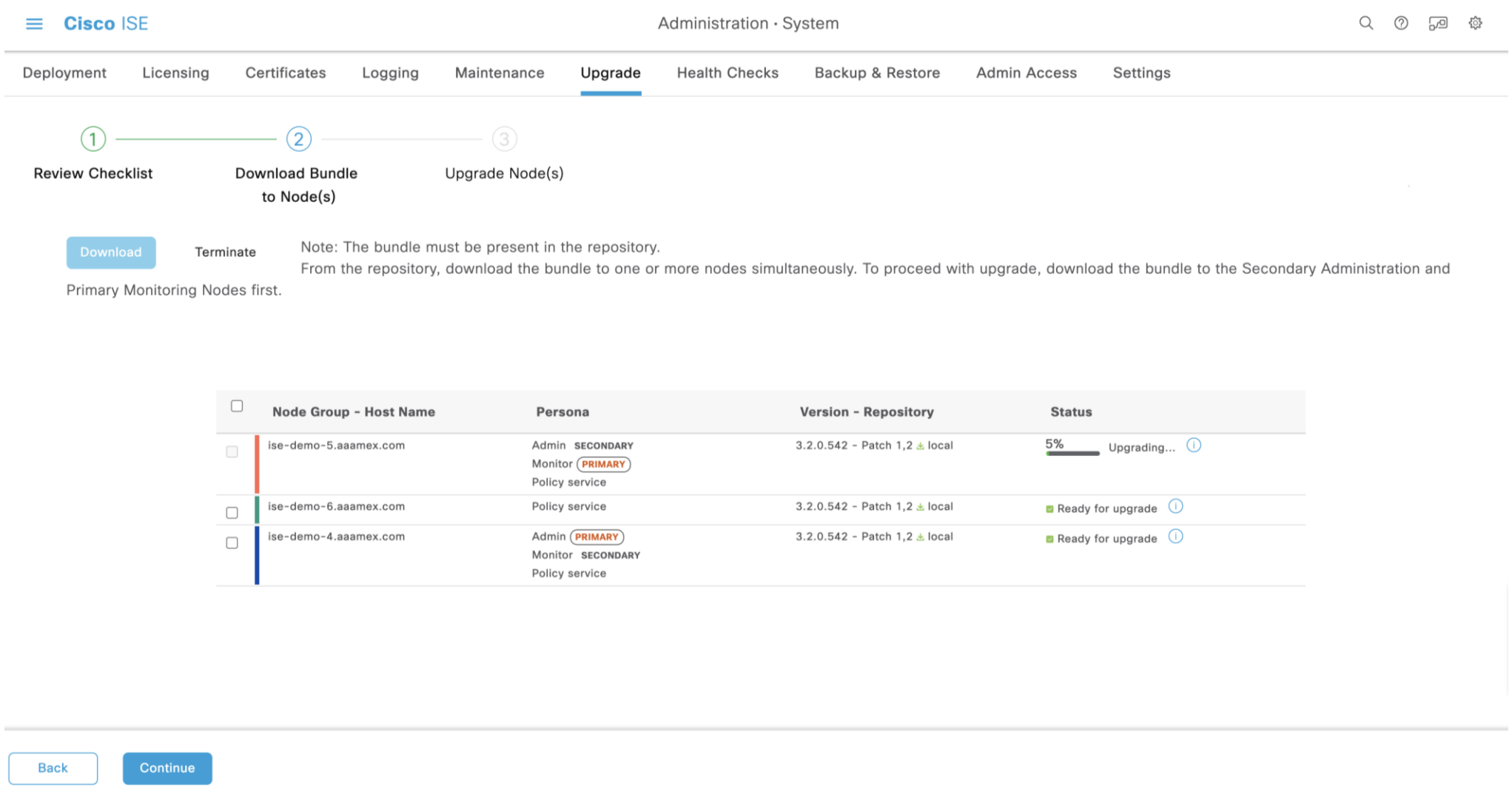
# Ejemplo – Legacy Split Upgrade 4/7



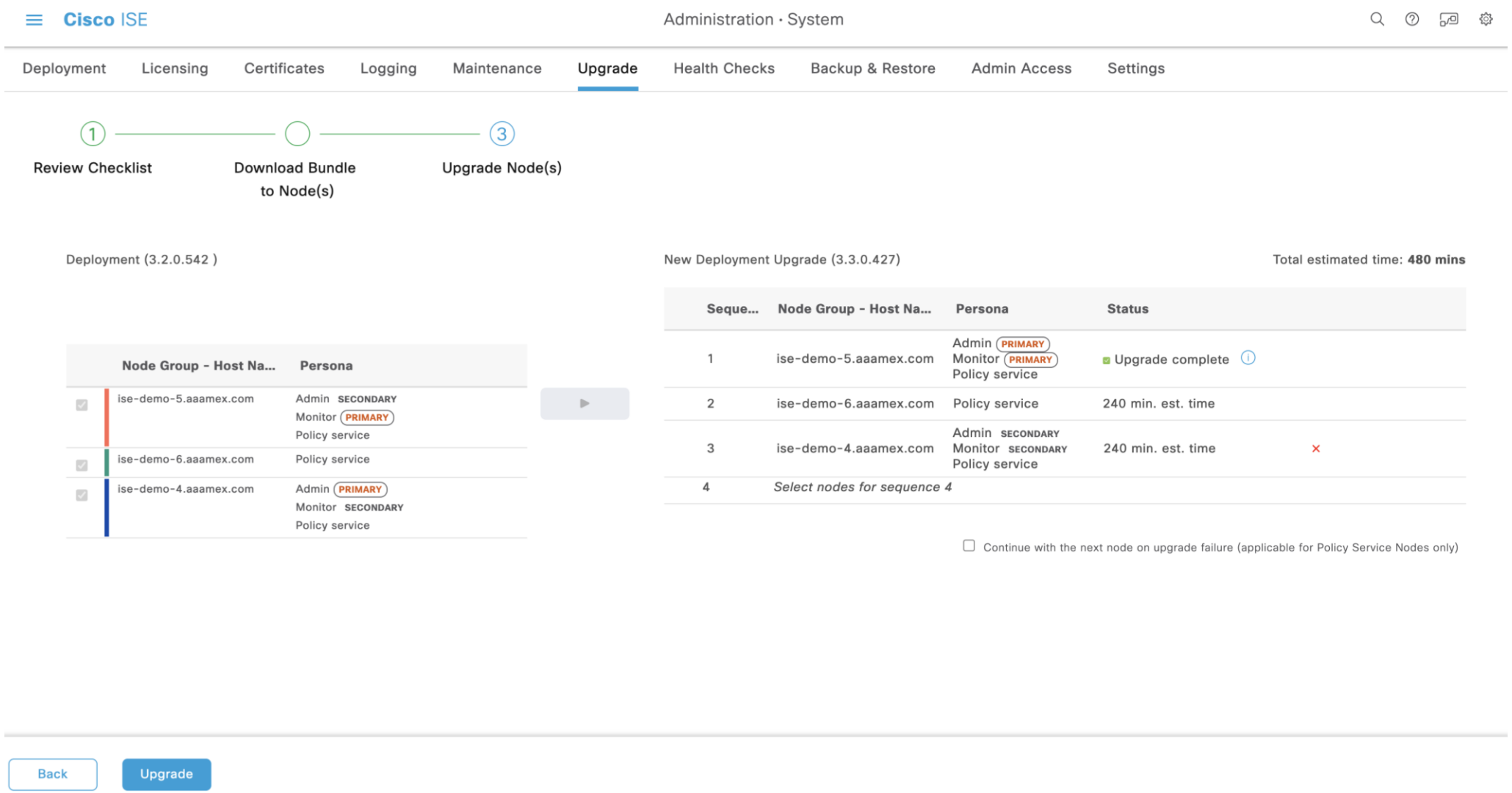
# Ejemplo – Legacy Split Upgrade 5/7



# Ejemplo – Legacy Split Upgrade 6/7

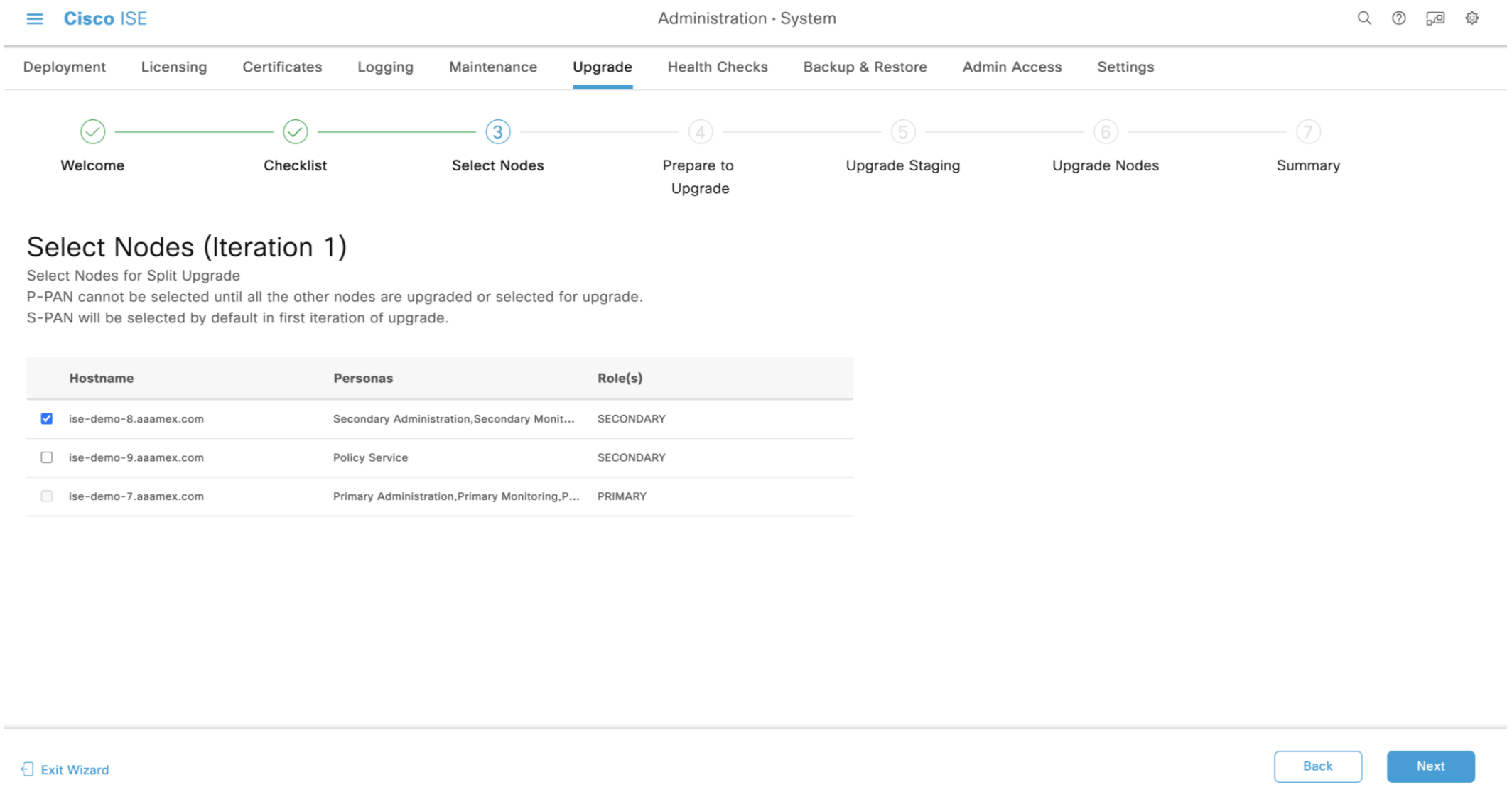


# Ejemplo – Legacy Split Upgrade 7/7

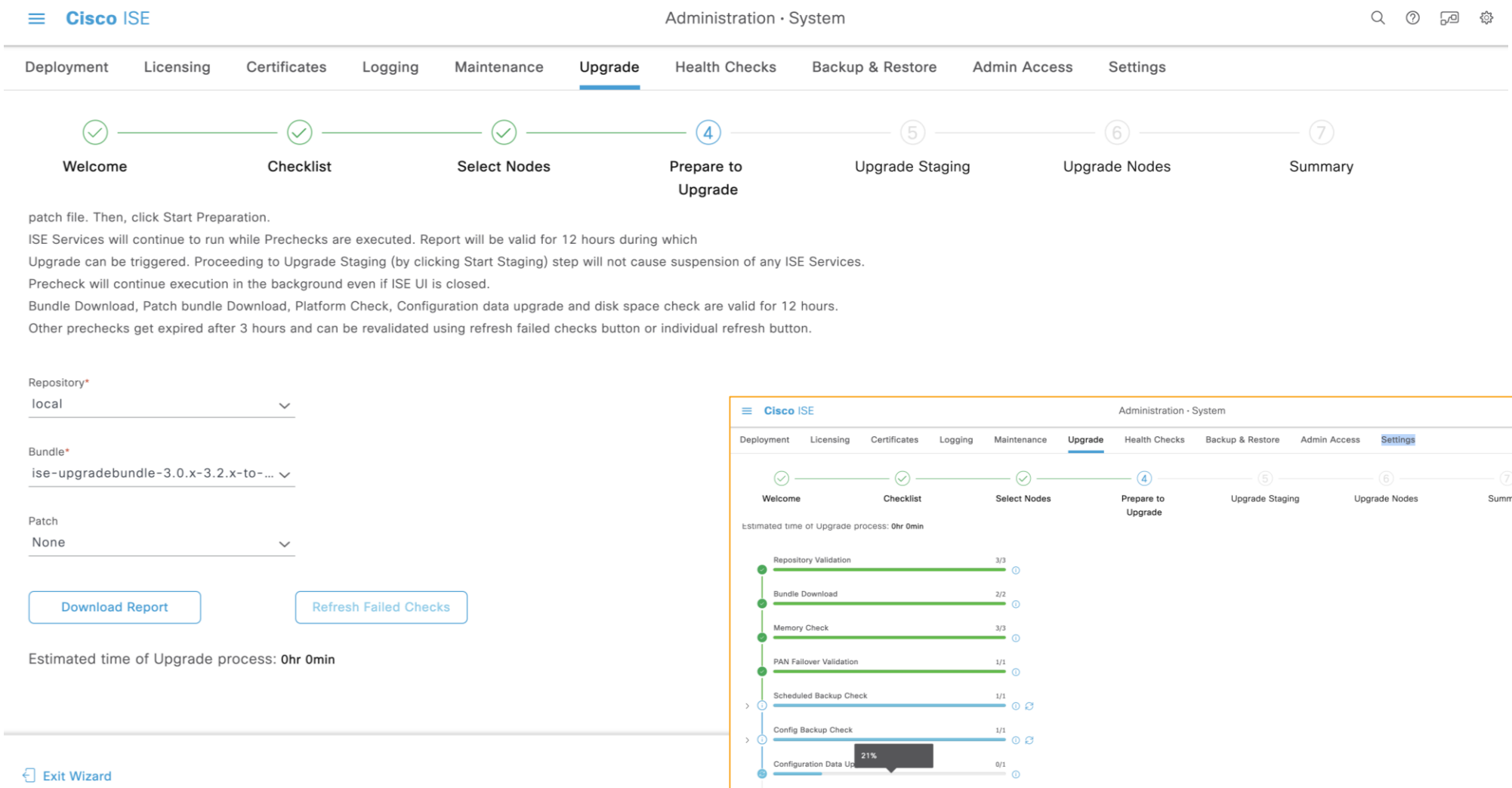


# Ejemplo de New Split Upgrade

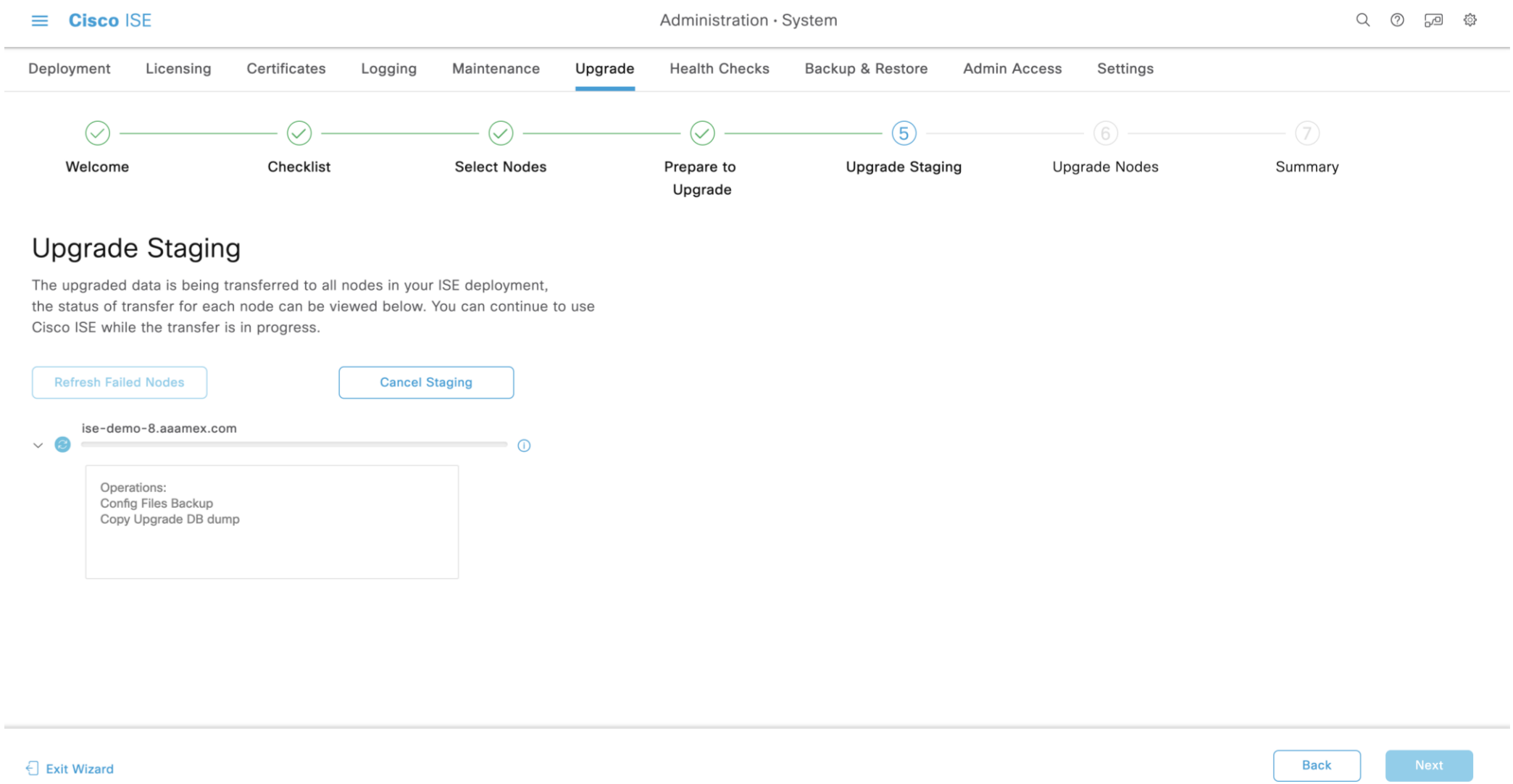
# Ejemplo – New Split Upgrade 1/9



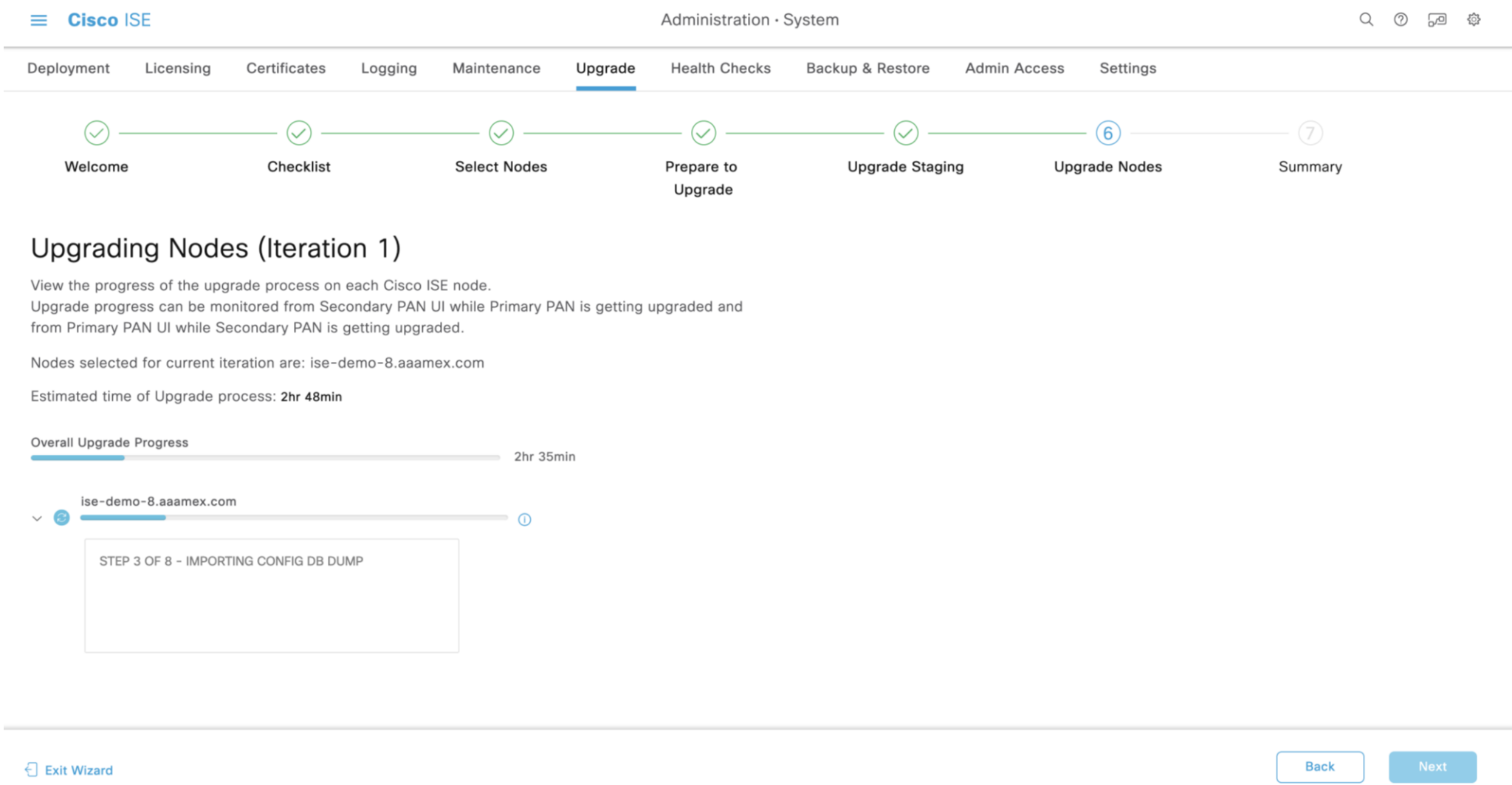
# Ejemplo – New Split Upgrade 2/9



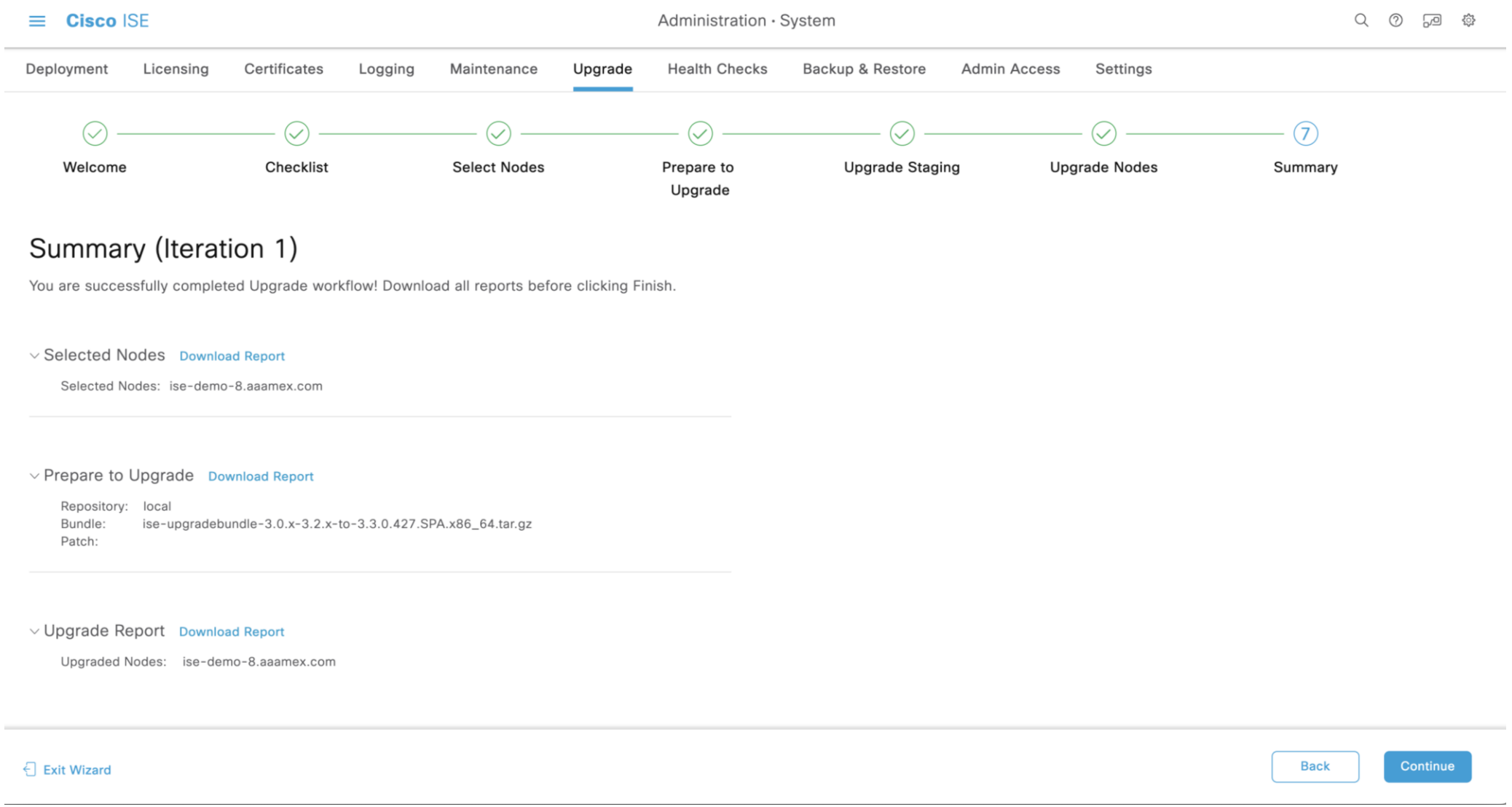
# Ejemplo – New Split Upgrade 3/9



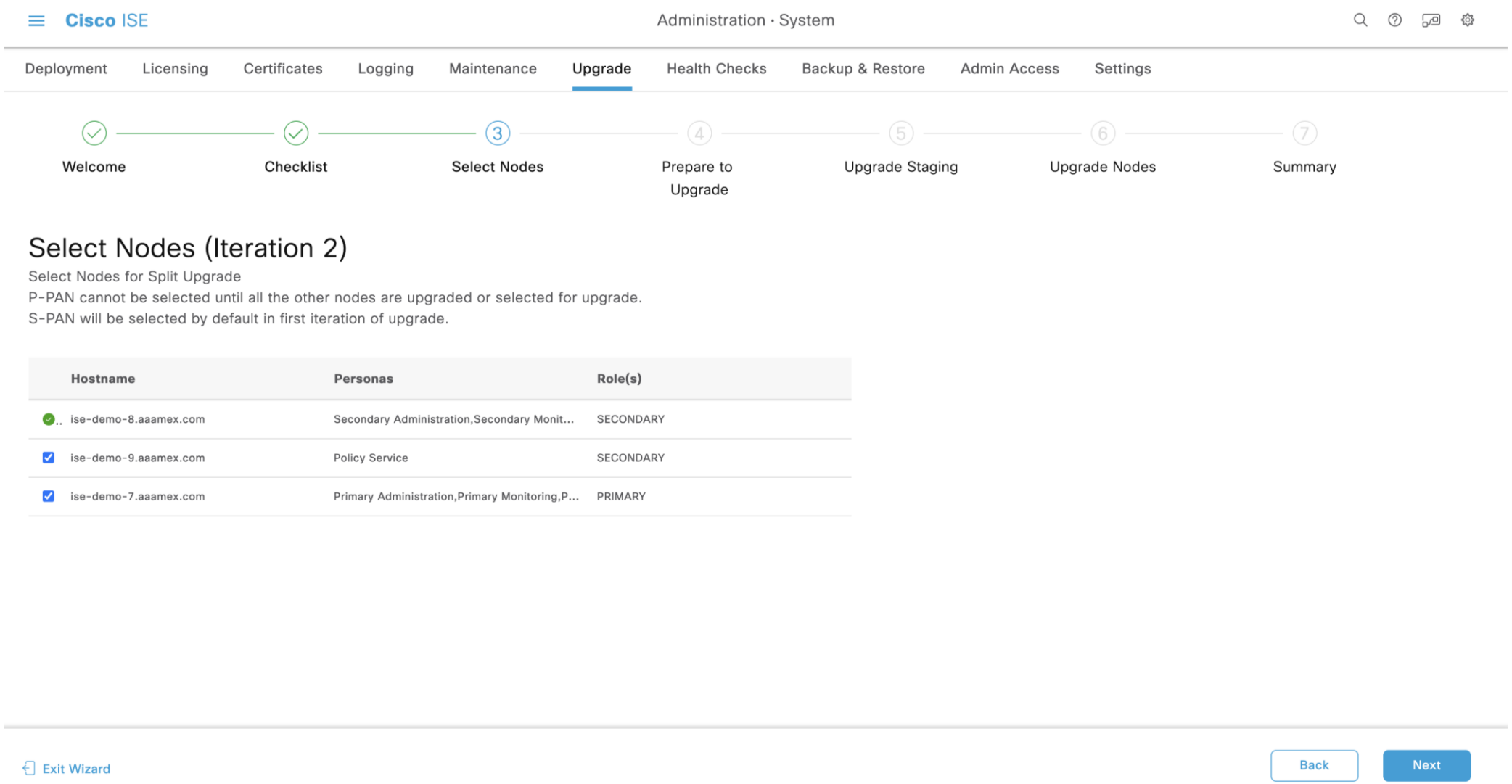
# Ejemplo – New Split Upgrade 4/9



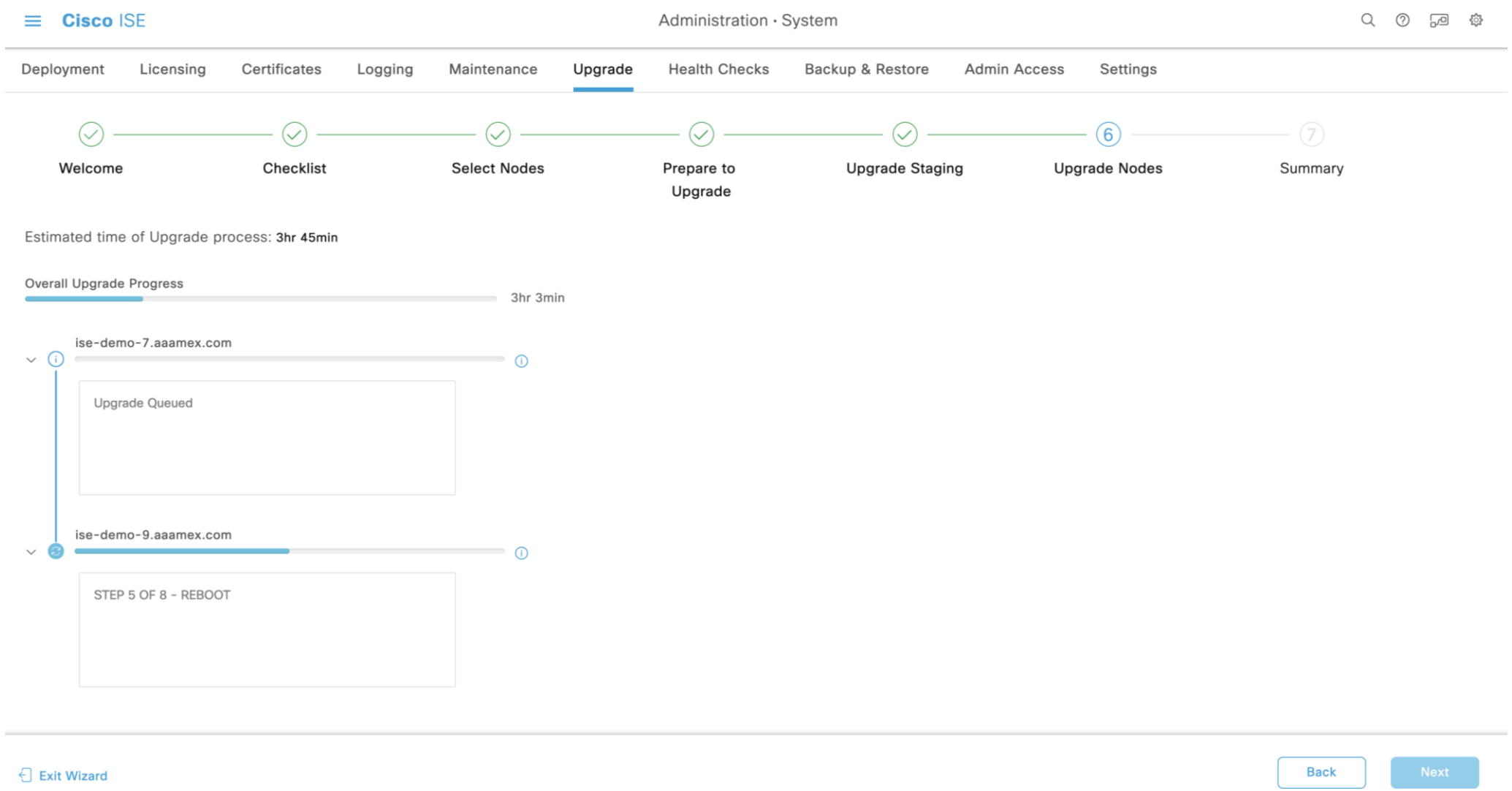
# Ejemplo – New Split Upgrade 5/9



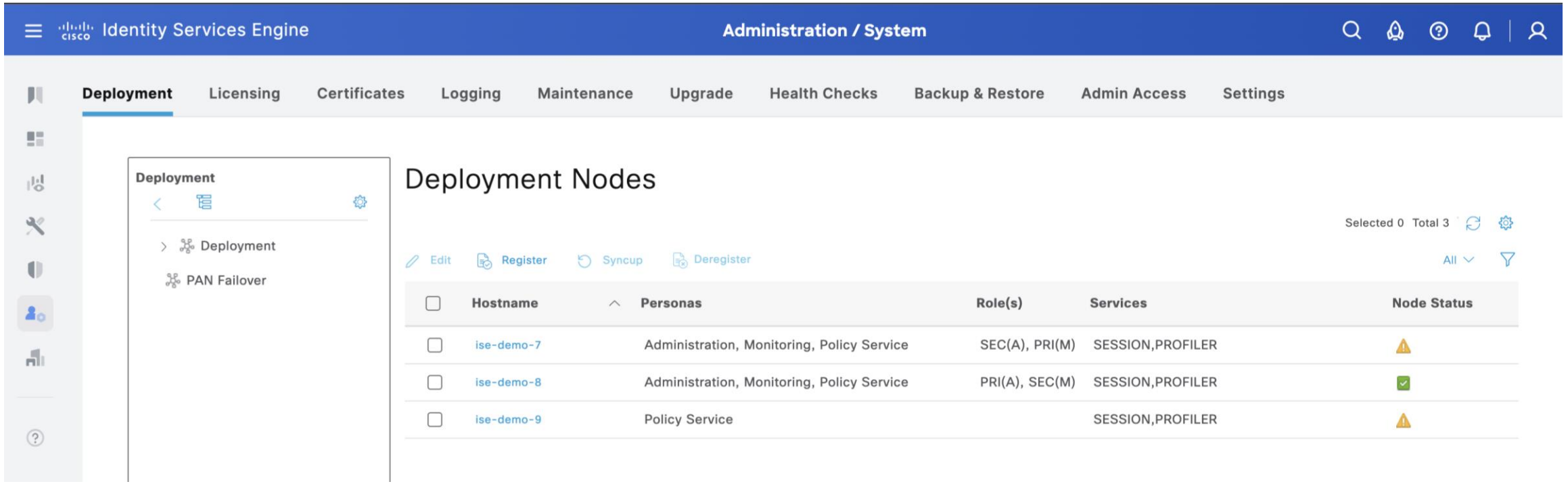
# Ejemplo – New Split Upgrade 6/9



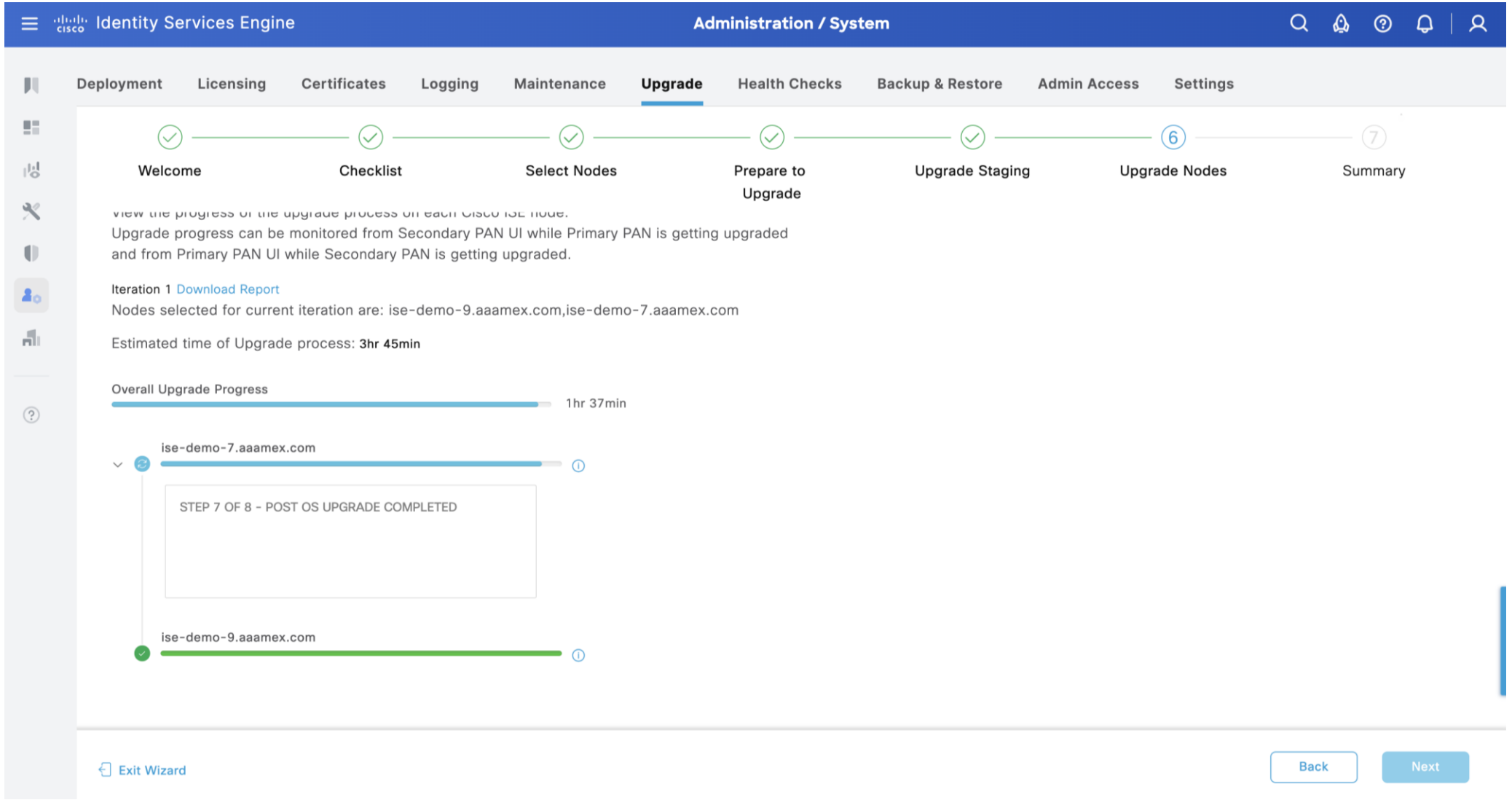
# Ejemplo – New Split Upgrade 7/9



# Ejemplo – New Split Upgrade 8/9



# Ejemplo – New Split Upgrade 9/9



Active poll

0

Join at

**slido.com**

**#4114 200**

Passcode:

**u9jada**

**¿Cuál de estos métodos se pueden usar para hacer upgrade de Cisco ISE?**

a) Split Upgrade, Full upgrade, backup and restore

0%

b) Split upgrade, schedule upgrade, reimage

0%

c) Split upgrade, isolated upgrade, full upgrade

0%

# Plan de contingencia

Si la actualización falla en algún nodo, se puede continuar con el proceso manualmente desde el CLI con los comandos:

```
application upgrade cleanup

application upgrade prepare <nombre del upgrade bundle> <nombre del repositorio>

application upgrade proceed
```

Si la actualización sigue fallando desde el CLI, se debe de registrar el nodo afectado y proceder con el siguiente nodo para no retrasar la actualización.

El nodo afectado debe ser reinstalado en la versión objetivo o aplicarle el comando:

```
application reset-config ise
```

Este comando reiniciará la configuración a valores de fábrica (sin quitar parches). Si el reset es exitoso, se puede intentar nuevamente la actualización en ese nodo usando los comandos de upgrade manualmente.

# Implicación de la actualización de ISE y FMC

La principal implicación es el funcionamiento de la integración pxGrid entre ISE y el FMC. Es importante verificar que las versiones de pxGrid sean compatibles entre FMC y ISE.

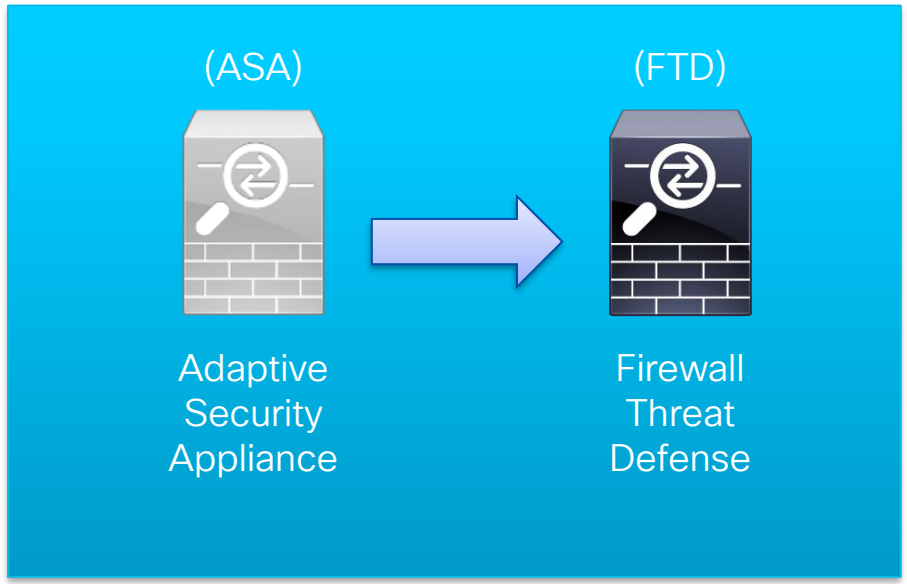
- ISE 3.0 ó anterior usa pxGrid versión 1 y 2.
- ISE 3.1 ó superior solo usa pxGrid versión 2.
- FMC 6.6 ó anterior solo usa pxGrid versión 1.
- FMC 6.7 ó superior solo usa pxGrid versión 2.

Tomando en cuenta lo anterior, por ejemplo, un FMC 6.6 puede operar con ISE 3.0, pero no puede operar con ISE 3.1.

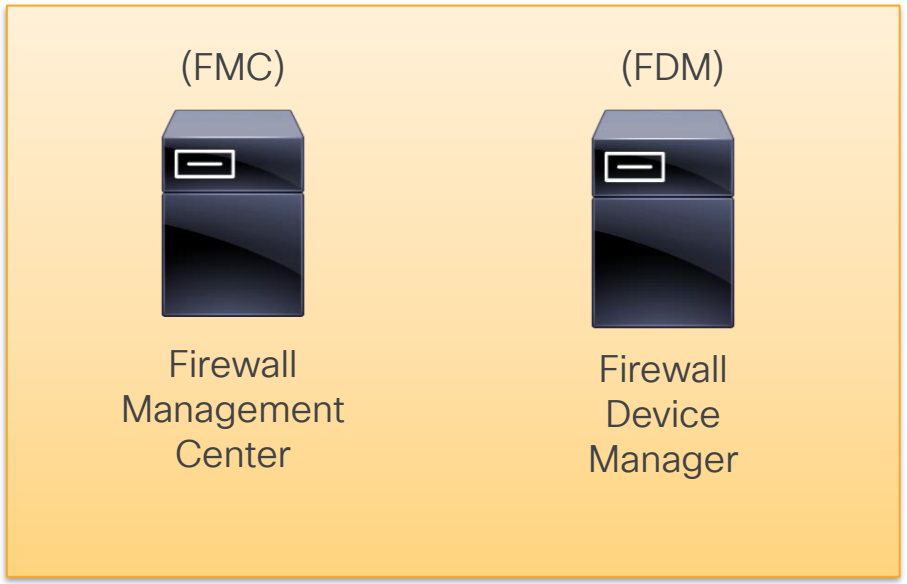
# Actualización de Secure Firewall

# Descripción general de FTD, FDM y FMC

## Cisco Firewalls



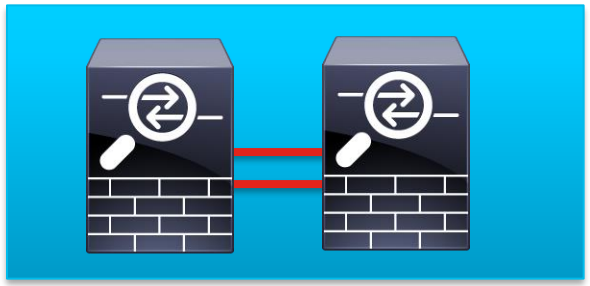

## Gestor del FTD



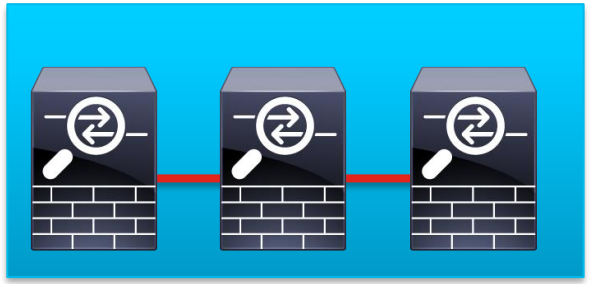
# Tipos de implementaciones en FTD y FMC

FTD

Standalone

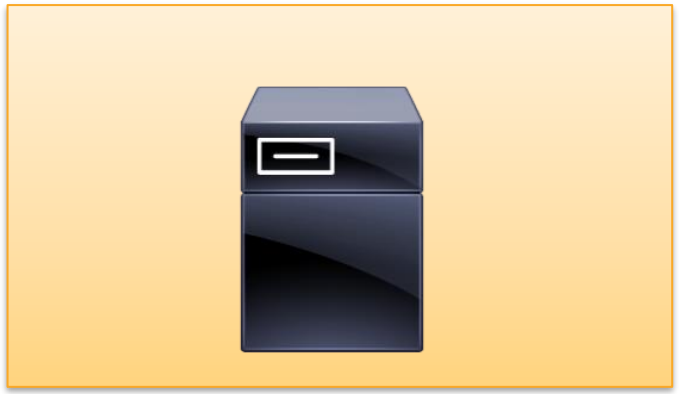


High Availability

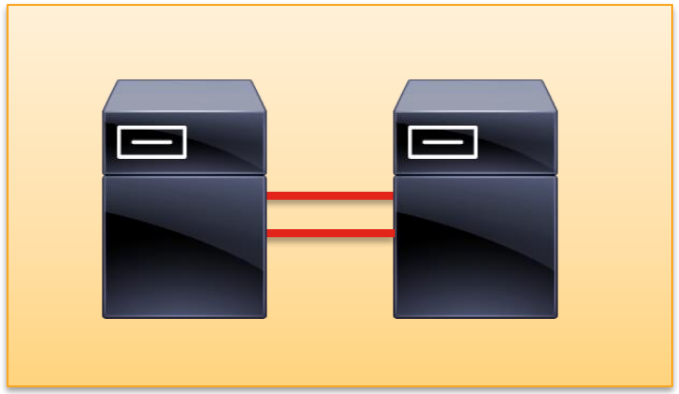


Cluster

FMC

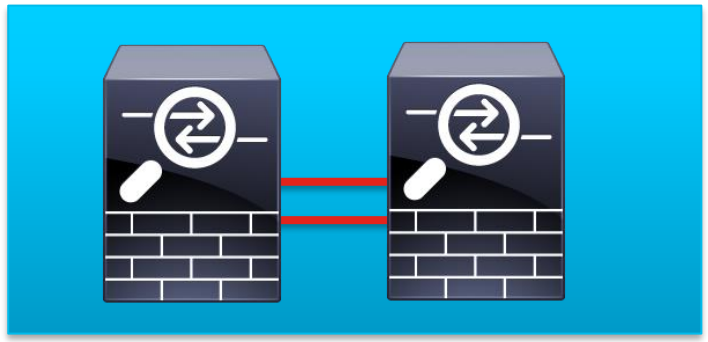


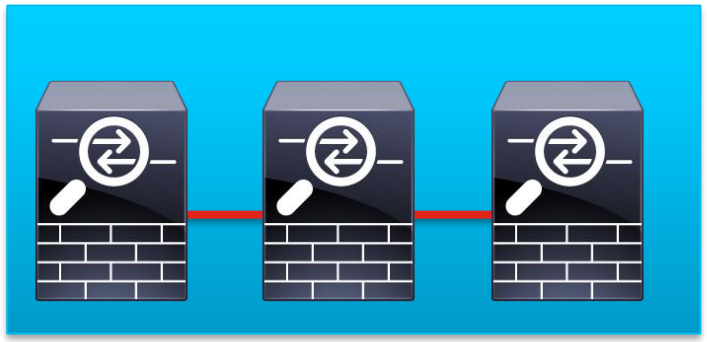
Standalone



High Availability

# Identificar tipo de implementación en FTD

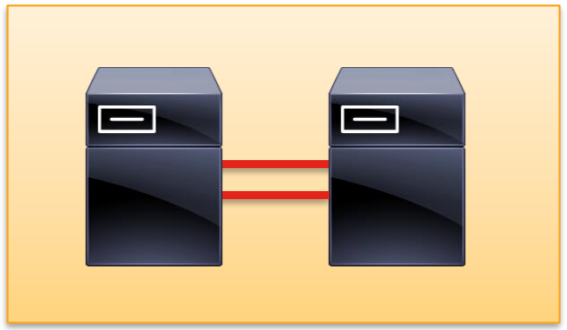


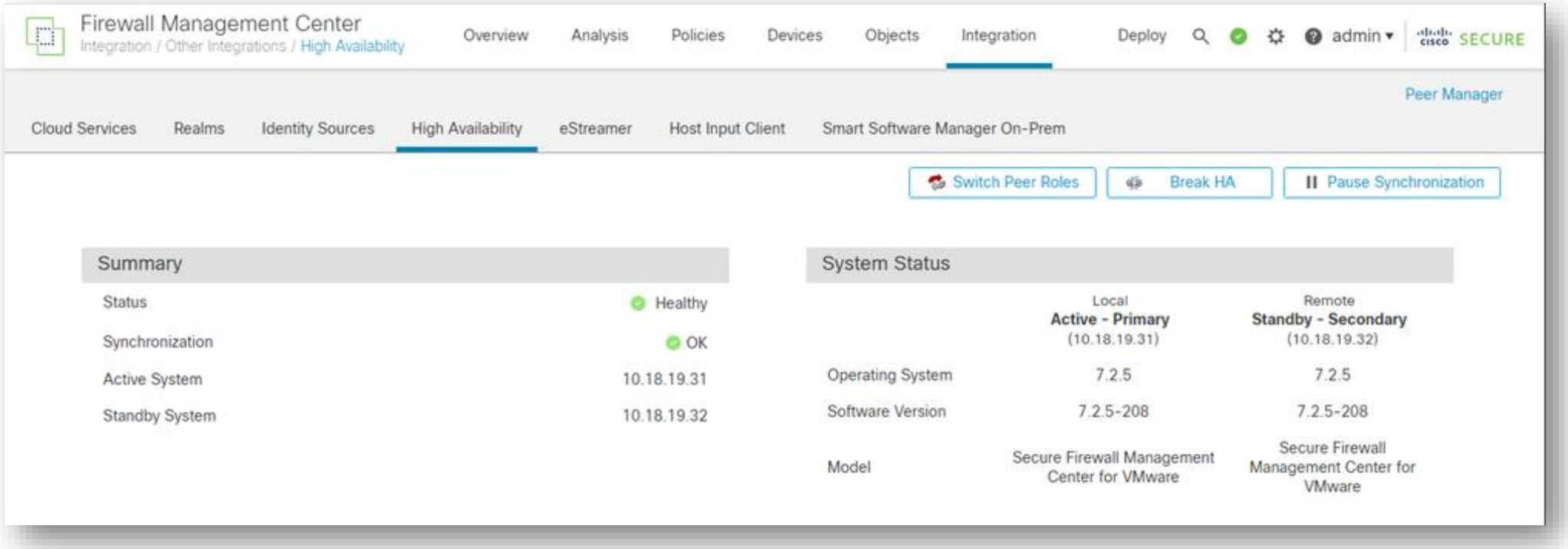


```
Cisco-ftd# show failover state

    State         Last Failure     Reason Date/Time
This host - Primary
    Active          None
Other host - Secondary
    Standby Ready  None

====Configuration State===
Sync Skipped
====Communication State===
Mac set
```

```
FTD-Cluster# show cluster info
Cluster FTD-Cluster-RB: On
Interface mode: spanned
Cluster Member Limit : 16
This is "unit-2-1" in state SLAVE
ID : 1
Site ID : 1
Version : 9.18(3)53
Serial No.: FCH22247MKJ
CCL IP : 10.99.2.1
CCL MAC : 0015.c500.028f
<--- More --->
```

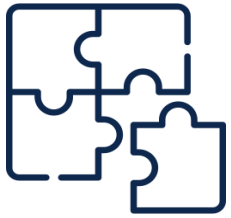
# Identificar tipo de implementación en FMC





# Prerrequisitos para una actualización

TAC Tip



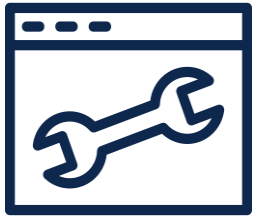
Validar compatibilidad de actualización

Generar un respaldo de las configuraciones

Descargar y subir el paquete de instalación al gestor del firewall

Ejecutar la verificación de preparacion para hacer validaciones técnicas

Limpiar deployments y tareas pendientes

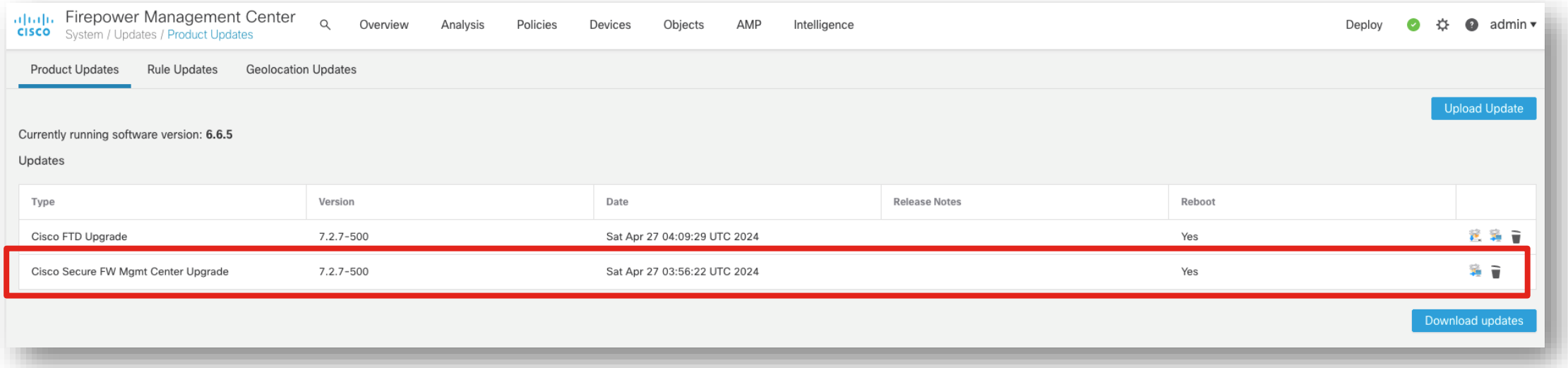


Agendar ventana de mantenimiento

# Actualización de FMC

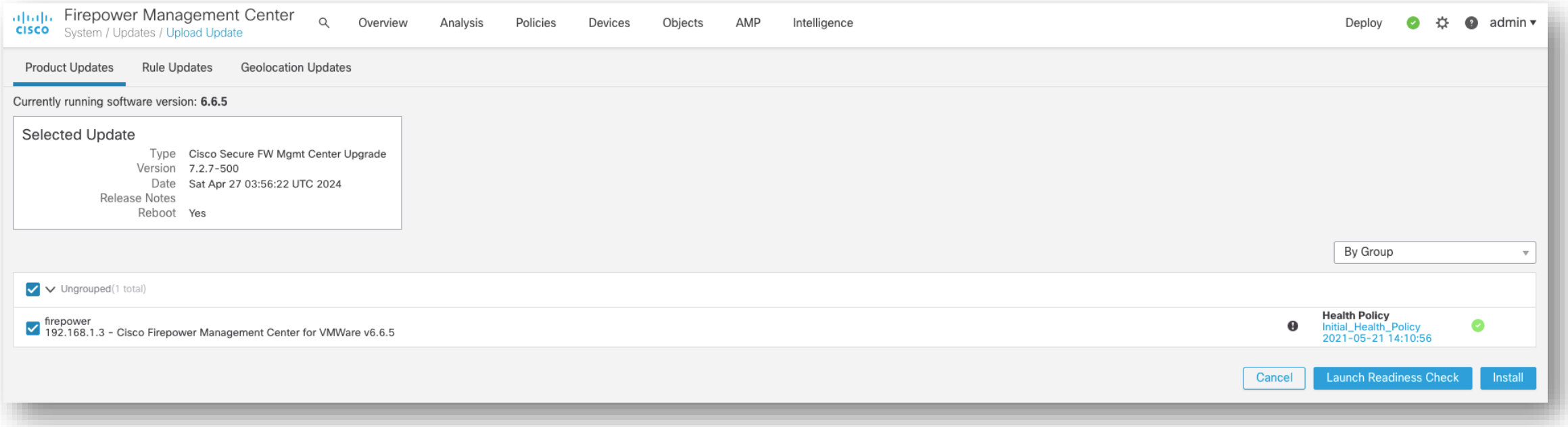
# Actualización de FMC

1. Loguearse a la interfaz gráfica del FMC
2. Dirigirse a System (⚙) > Updates
3. Haz click en el icono de “instalar” sobre el paquete de actualización deseado para comenzar la actualización ( )



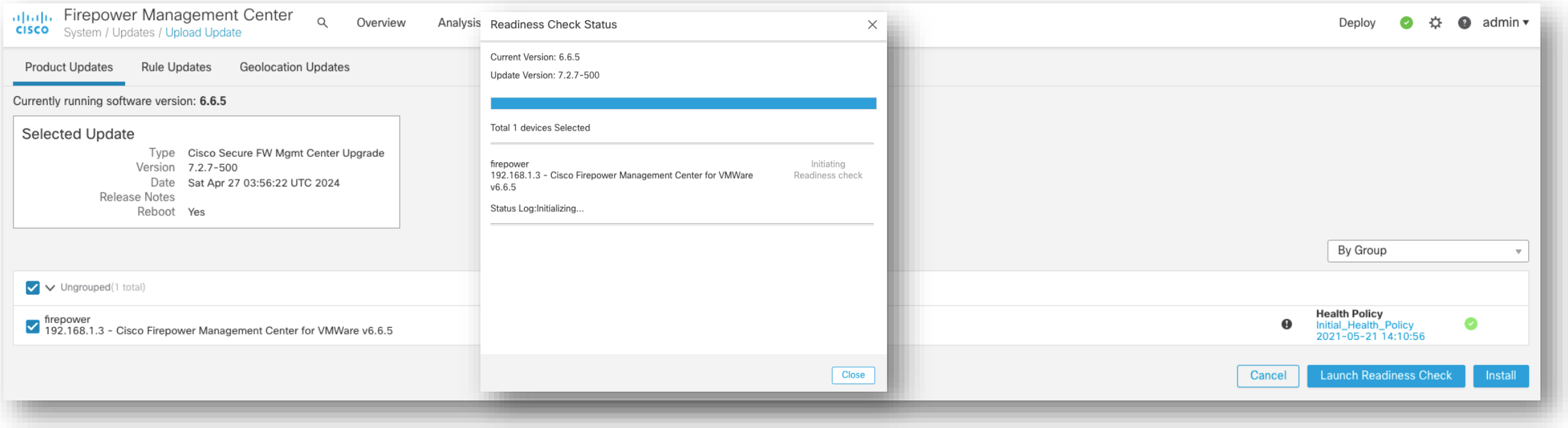
# Actualización de FMC

1. Selecciona el equipo a instalar
2. Haz click en el botón “Launch Readiness Check” para ejecutar las validaciones técnicas



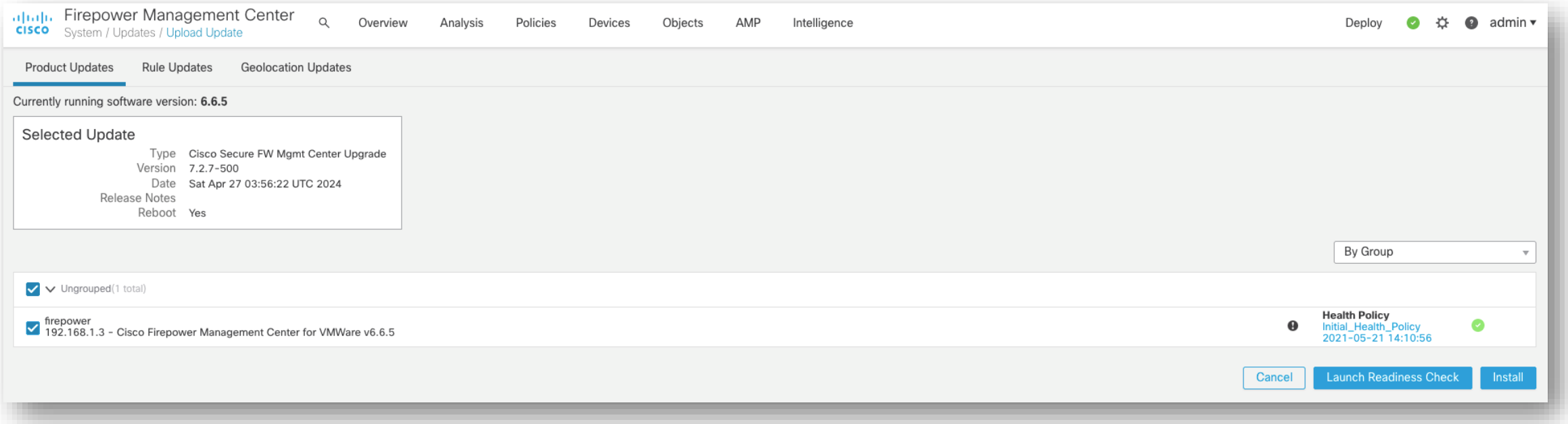
# Actualización de FMC

1. Selecciona el equipo a instalar
2. Haz click en el botón “Launch Readiness Check” para ejecutar las validaciones técnicas



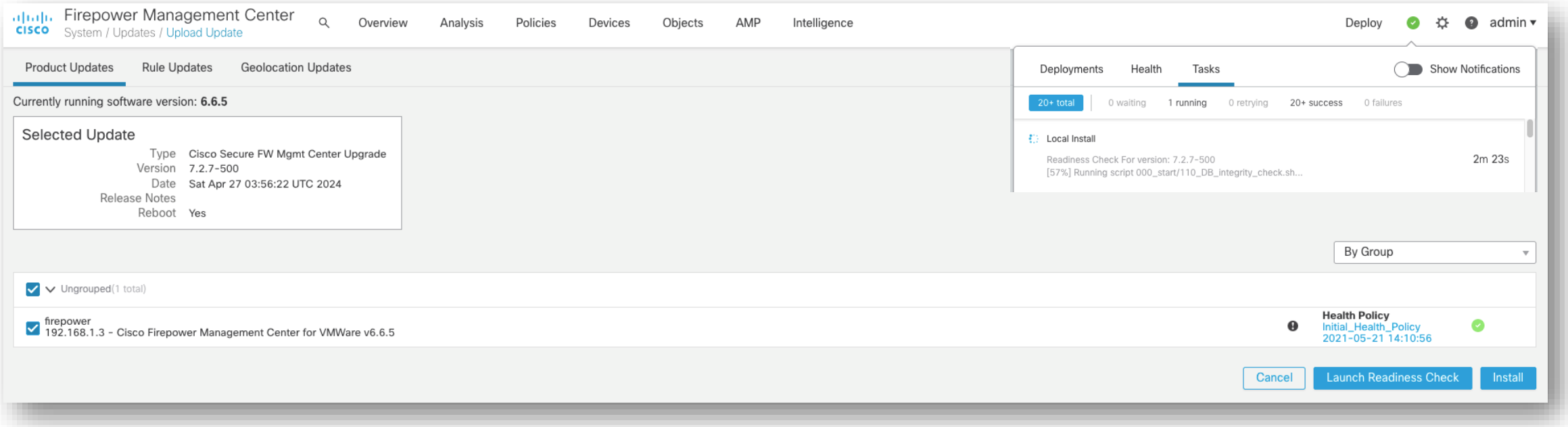
# Actualización de FMC

1. Selecciona el equipo a instalar
2. Haz click en el botón “Launch Readiness Check” para ejecutar las validaciones técnicas



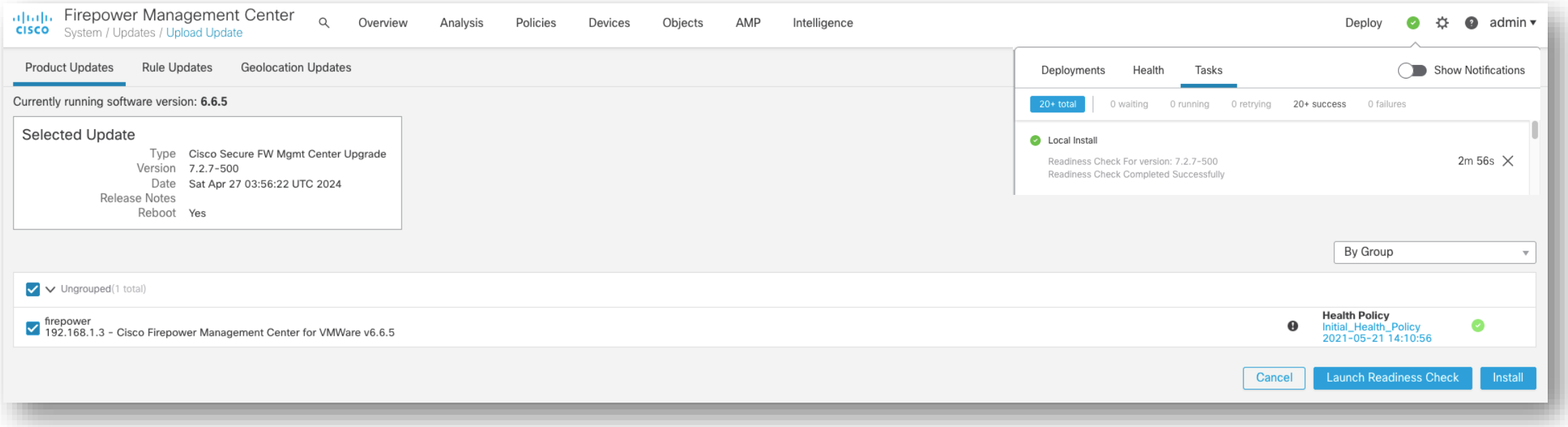
# Actualización de FMC

1. Selecciona el equipo a instalar
2. Haz click en el botón “Launch Readiness Check” para ejecutar las validaciones técnicas



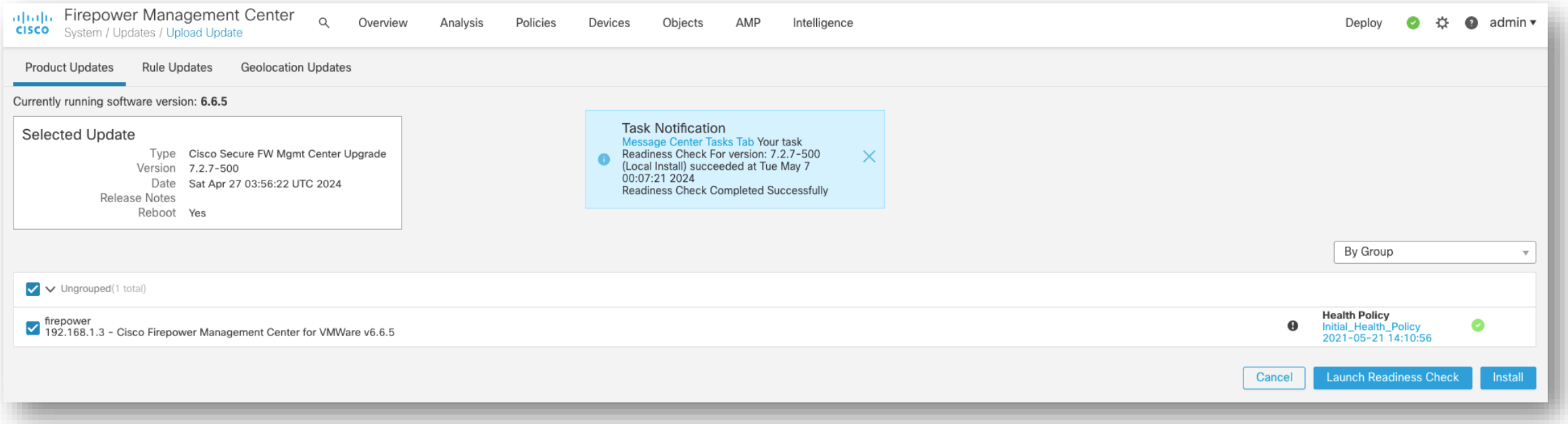
# Actualización de FMC

1. Selecciona el equipo a instalar
2. Haz click en el botón “Launch Readiness Check” para ejecutar las validaciones técnicas



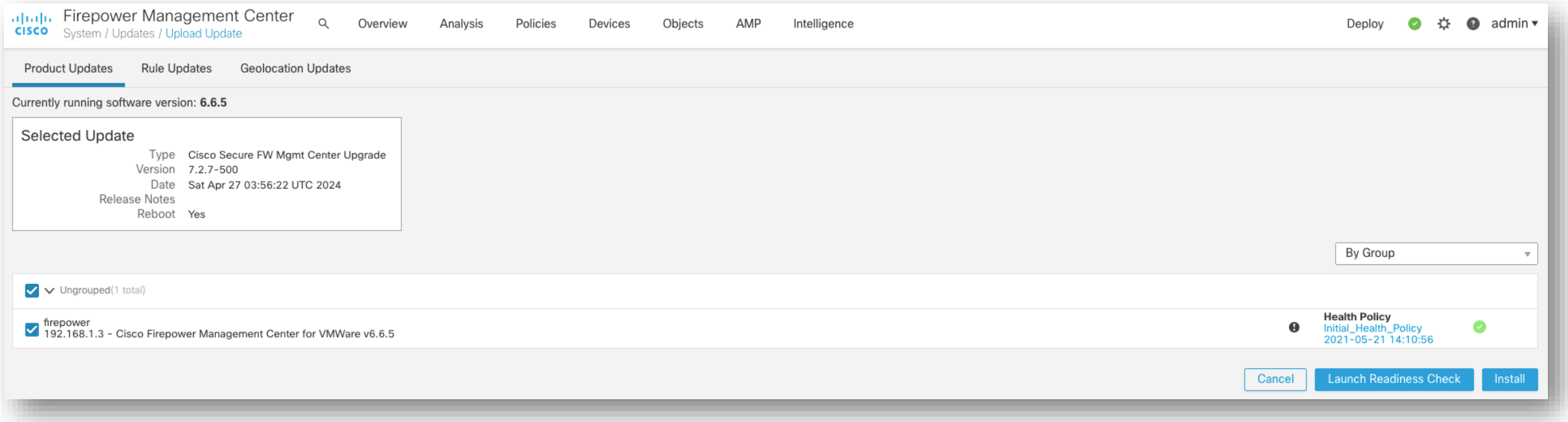
# Actualización de FMC

1. Selecciona el equipo a instalar
2. Haz click en el botón “Launch Readiness Check” para ejecutar las validaciones técnicas



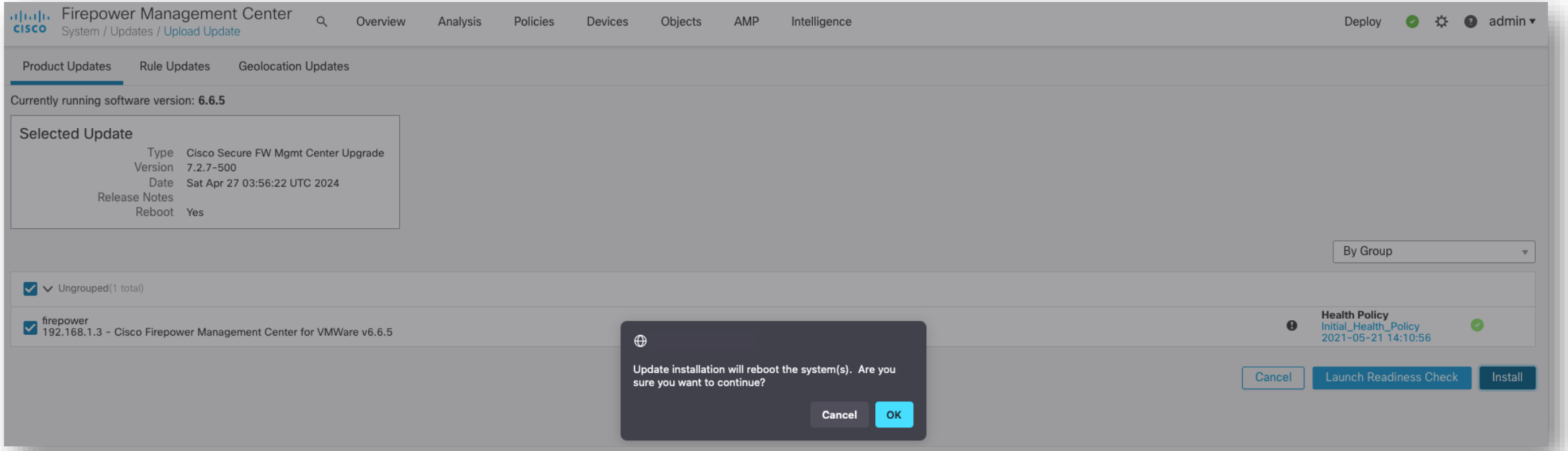
# Actualización de FMC

- Haz click en el botón de “Install” para comenzar la actualización



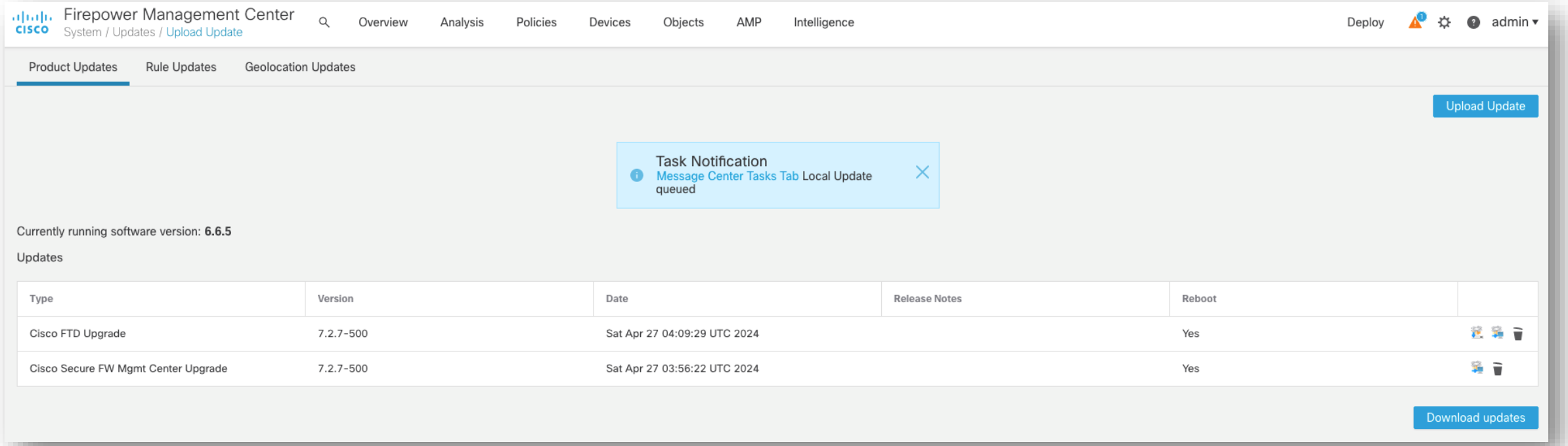
# Actualización de FMC

- Haz click en el botón de “Install” para comenzar la actualización



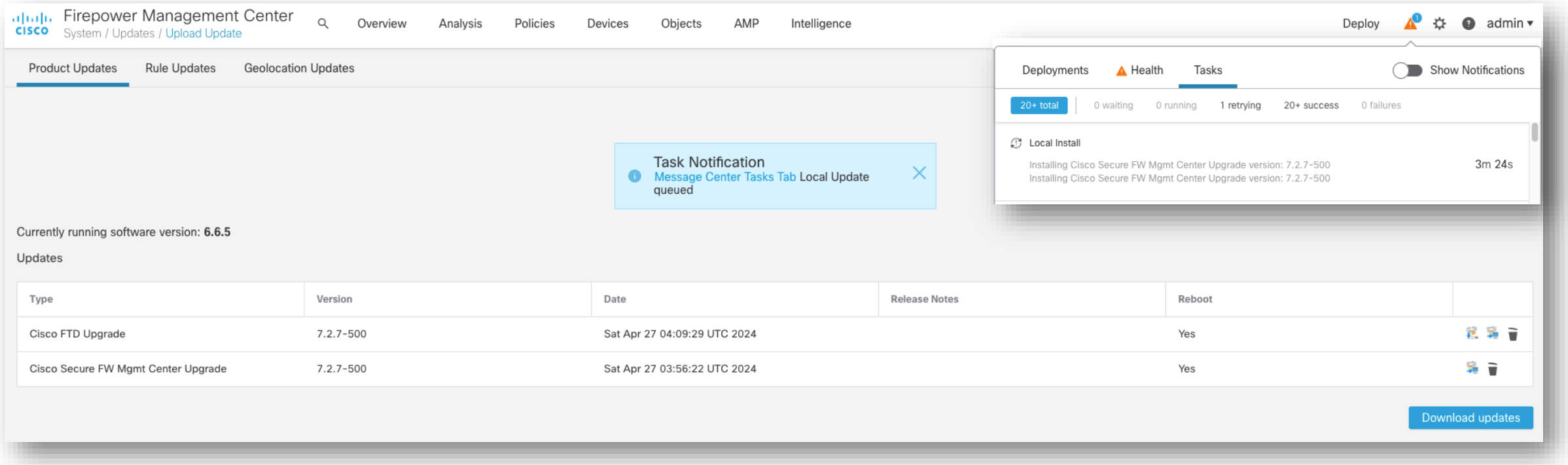
# Actualización de FMC

- Haz click en el botón de “Install” para comenzar la actualización



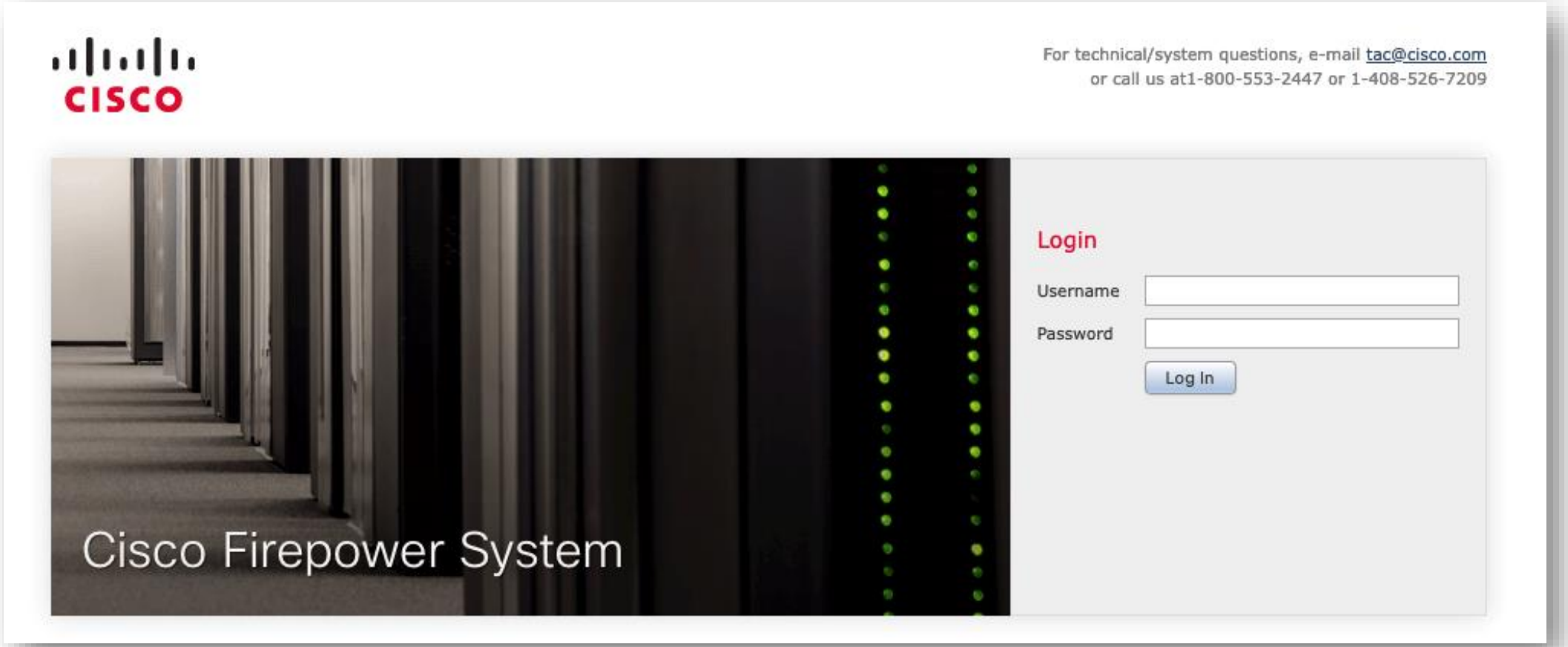
# Actualización de FMC

- Haz click en el botón de “Install” para comenzar la actualización



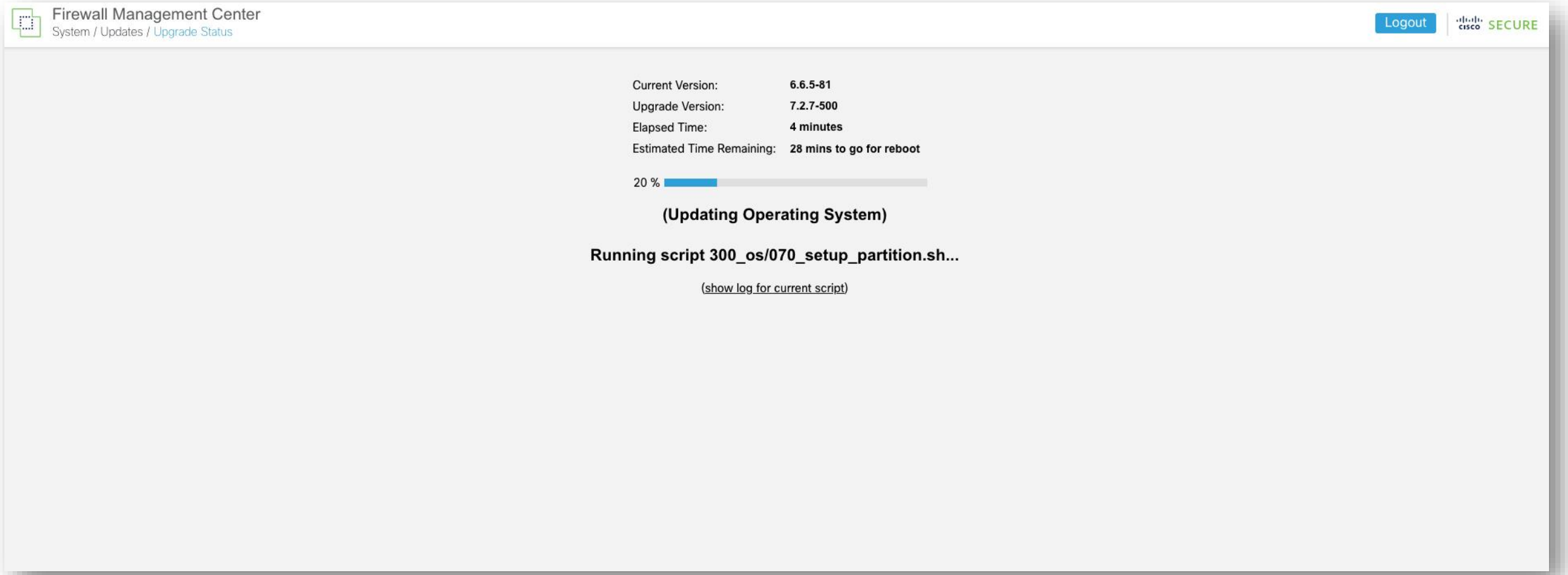
# Actualización de FMC

- Iniciar sesión de nuevo en la interfaz gráfica temporal para monitorear la actualización



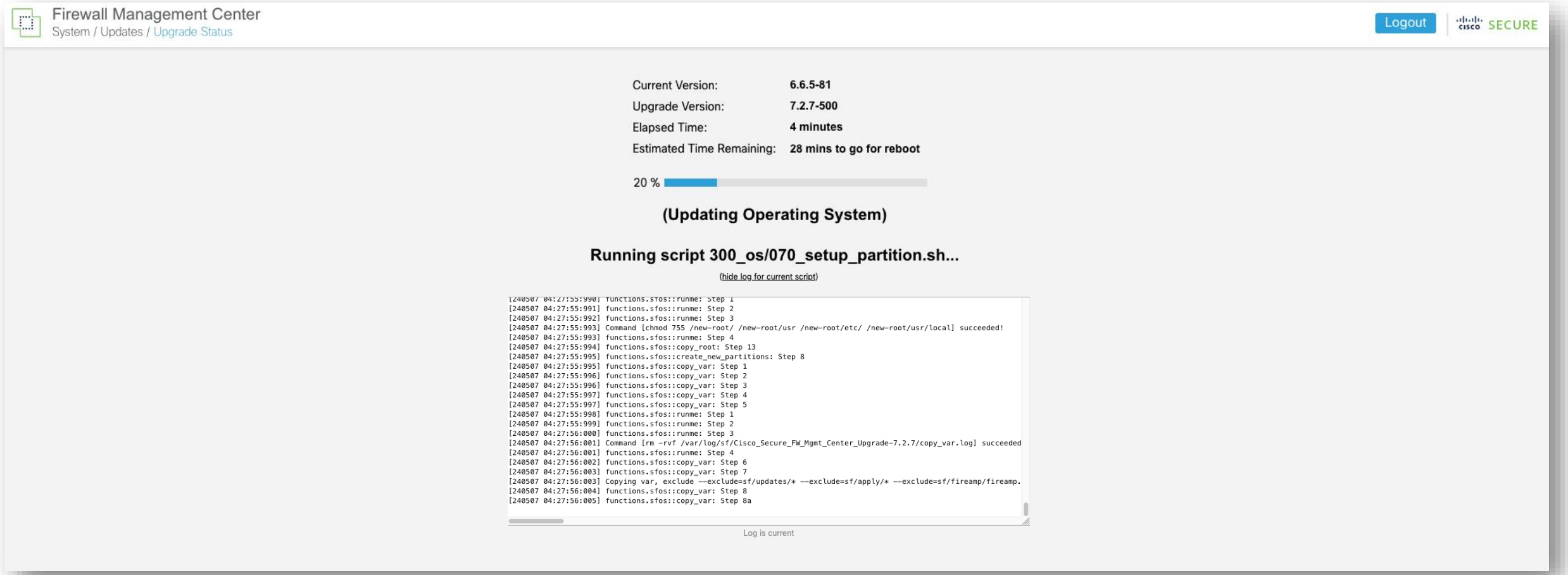
# Actualización de FMC

- Iniciar sesión de nuevo en la interfaz gráfica temporal para monitorear la actualización



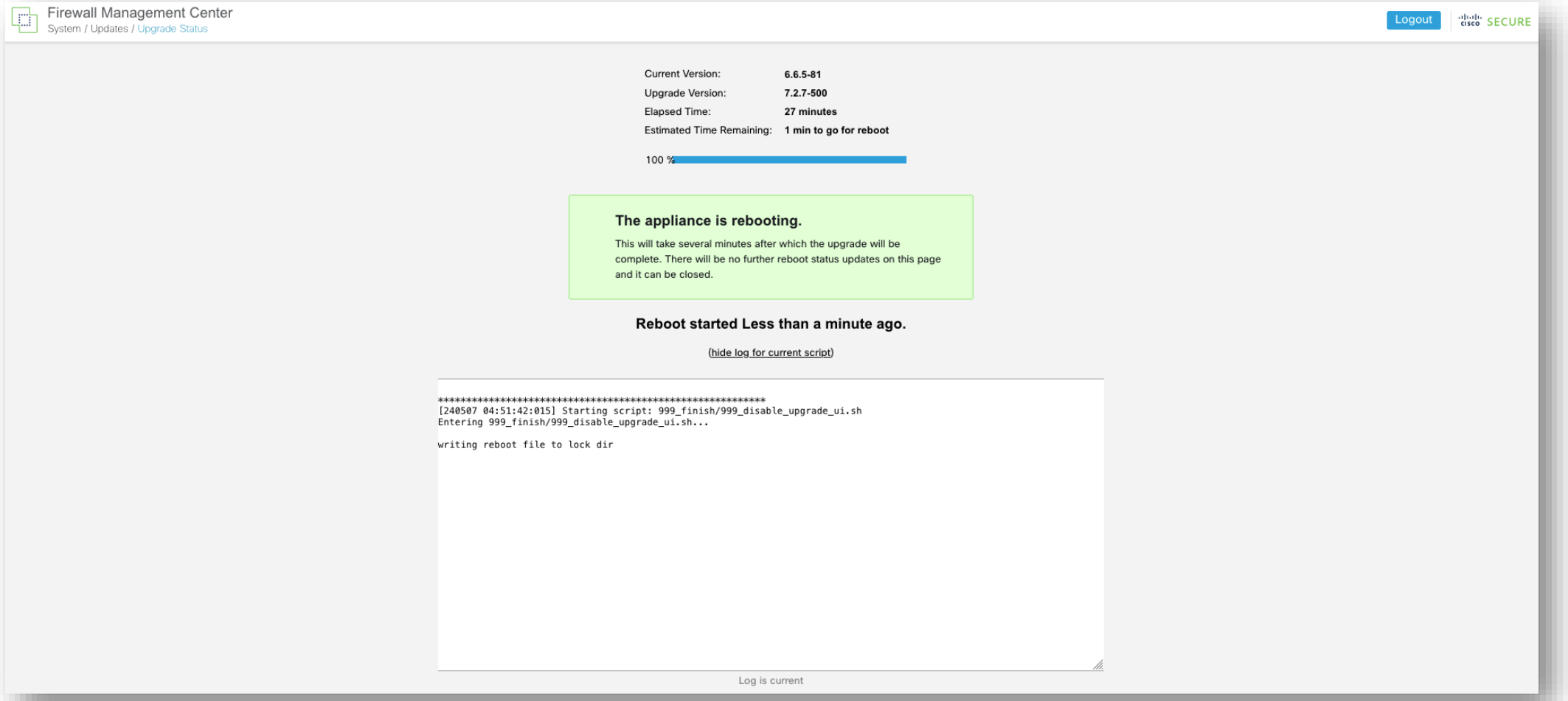
# Actualización de FMC

- Iniciar sesión de nuevo en la interfaz gráfica temporal para monitorear la actualización



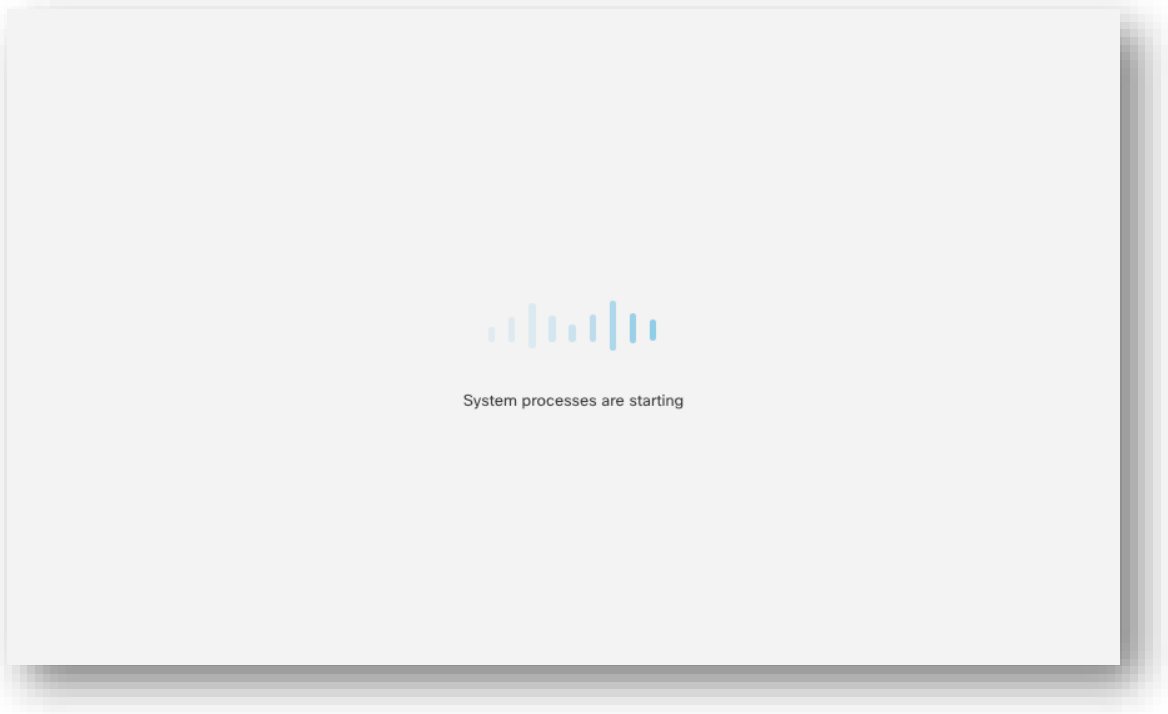
# Actualización de FMC

- Iniciar sesión de nuevo en la interfaz gráfica temporal para monitorear la actualización



# Actualización de FMC

- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración

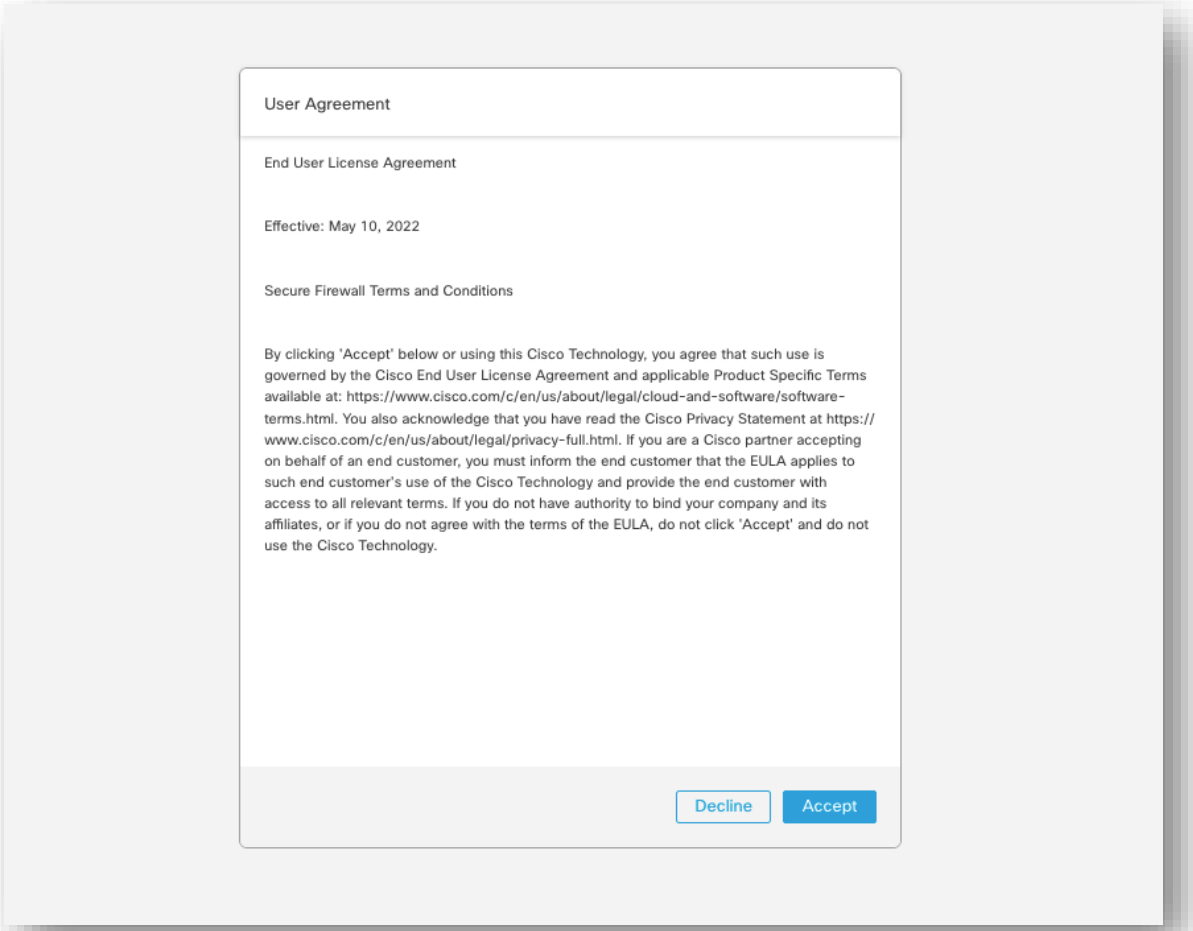


# Actualización de FMC

- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración

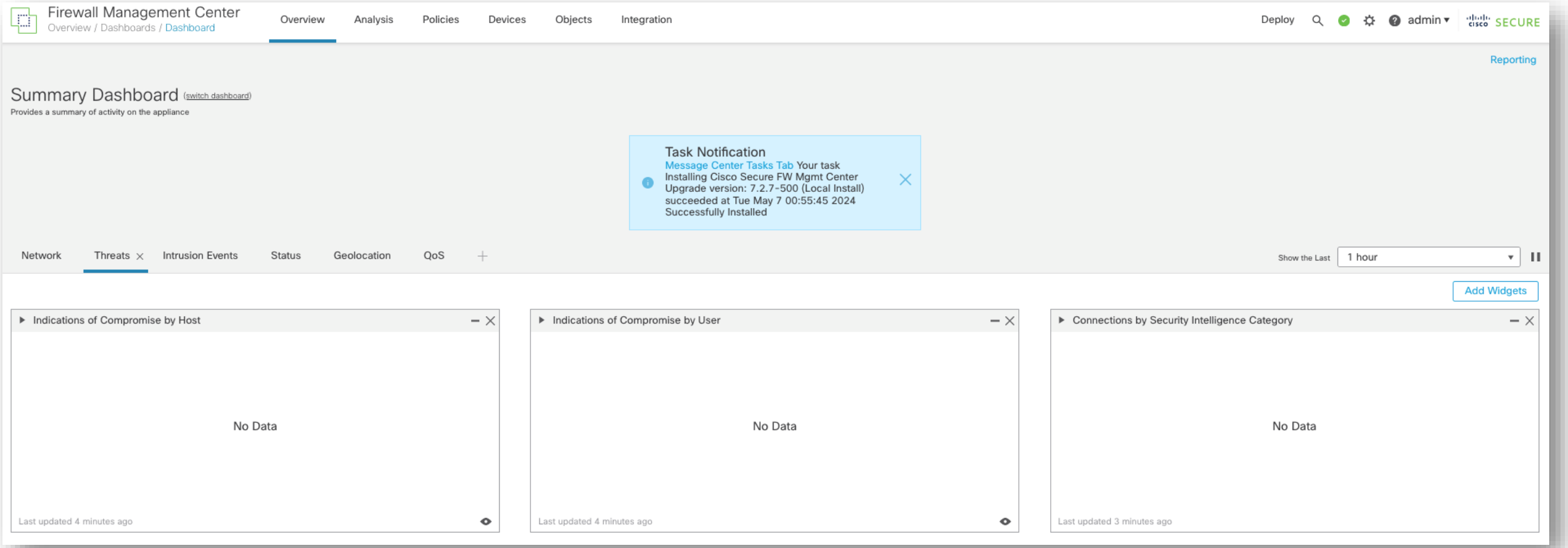
# Actualización de FMC

- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración



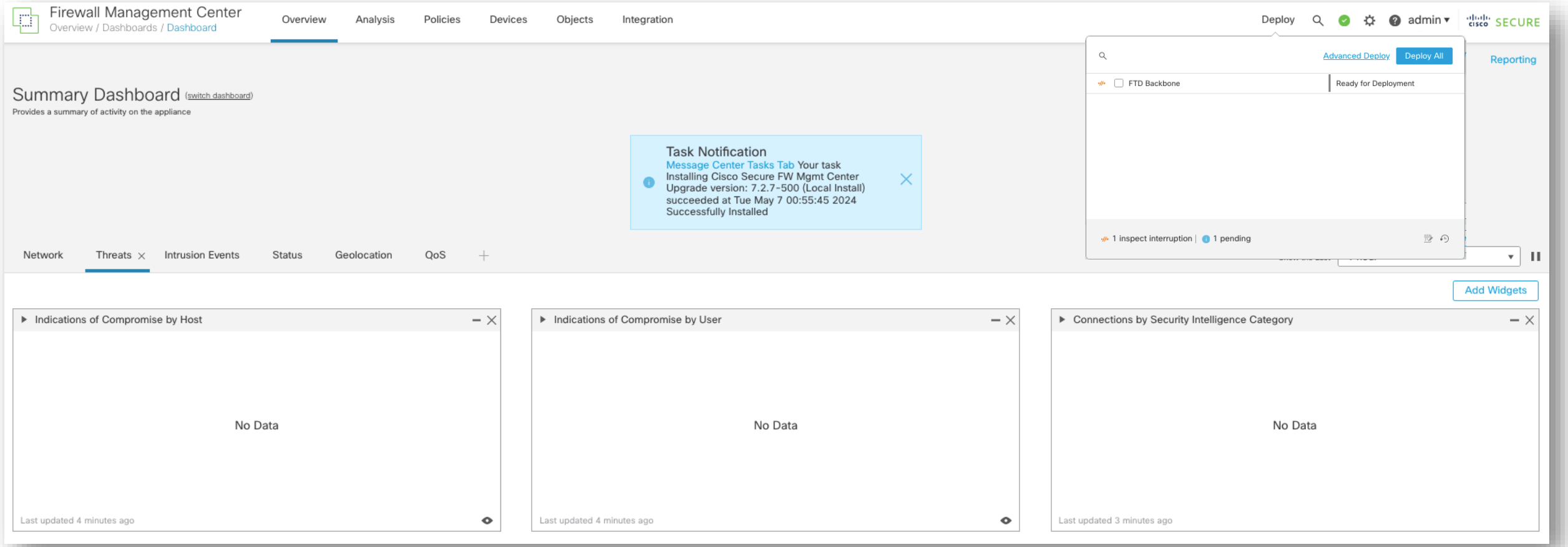
# Actualización de FMC

- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración



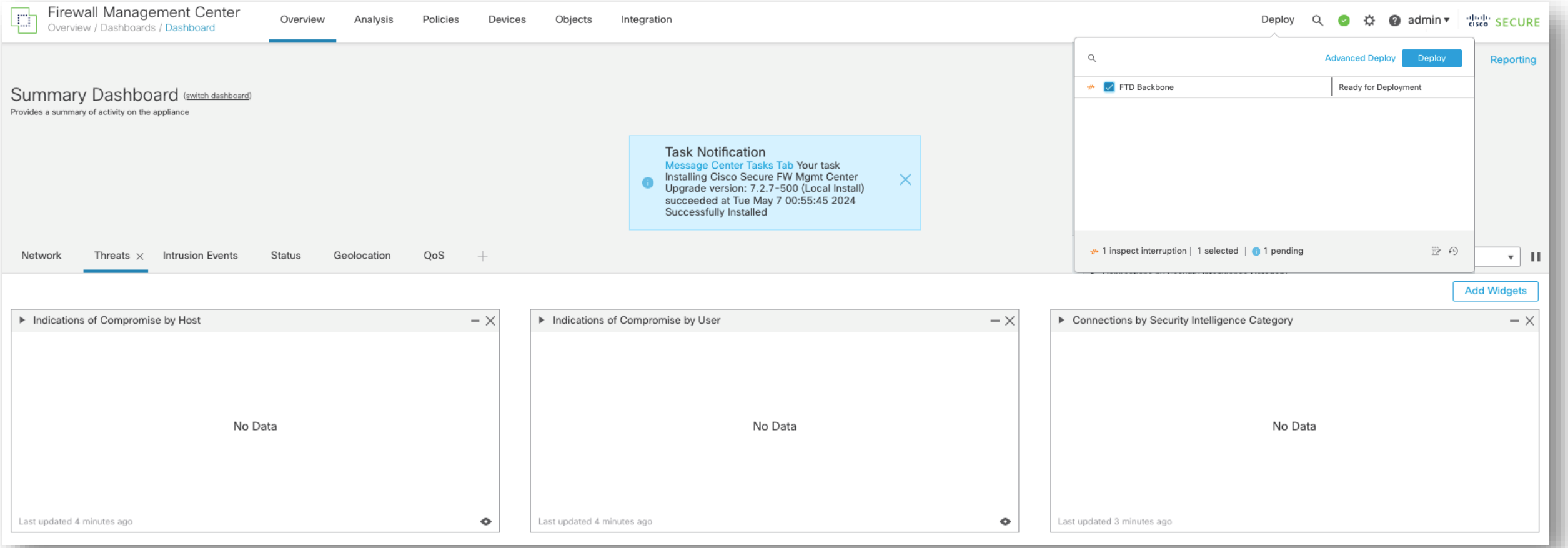
# Actualización de FMC

- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración



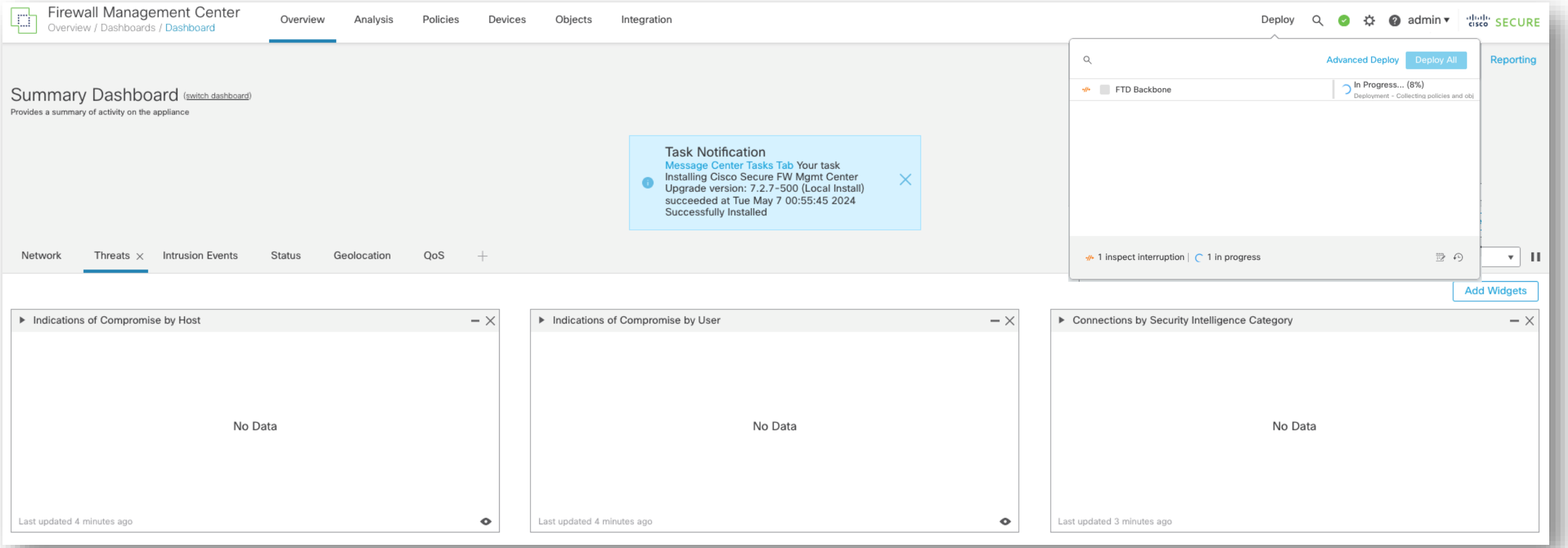
# Actualización de FMC

- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración



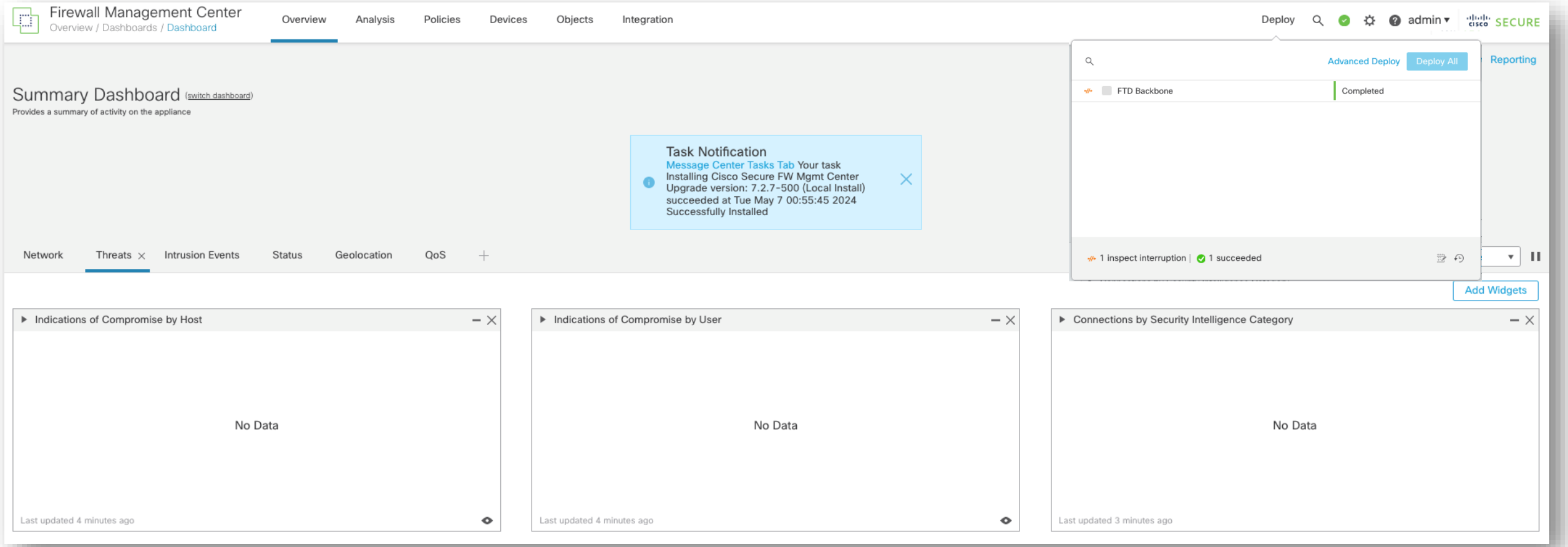
# Actualización de FMC

- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración



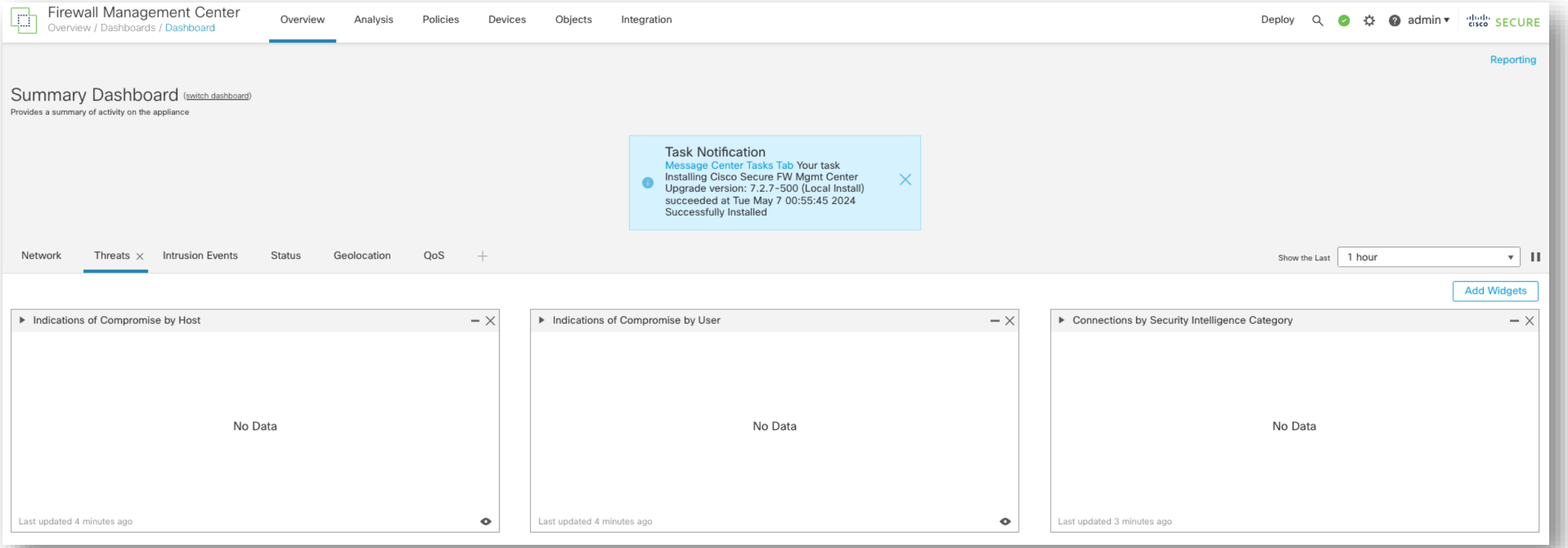
# Actualización de FMC

- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración



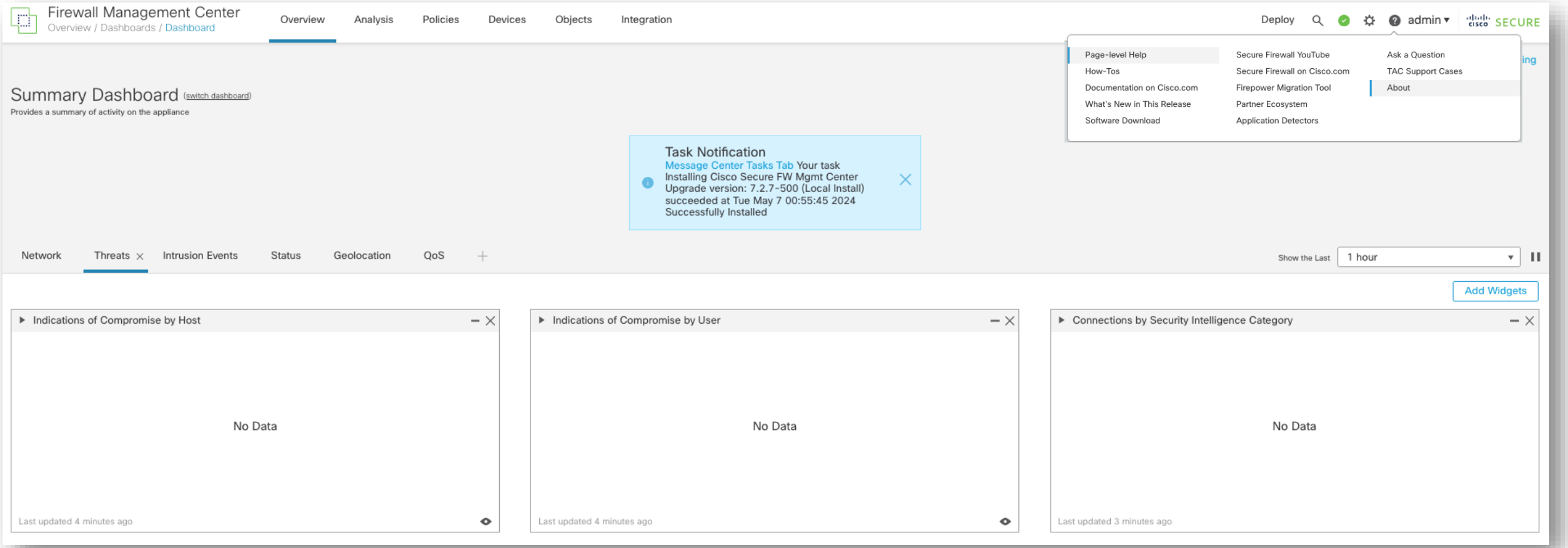
# Actualización de FMC

- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración



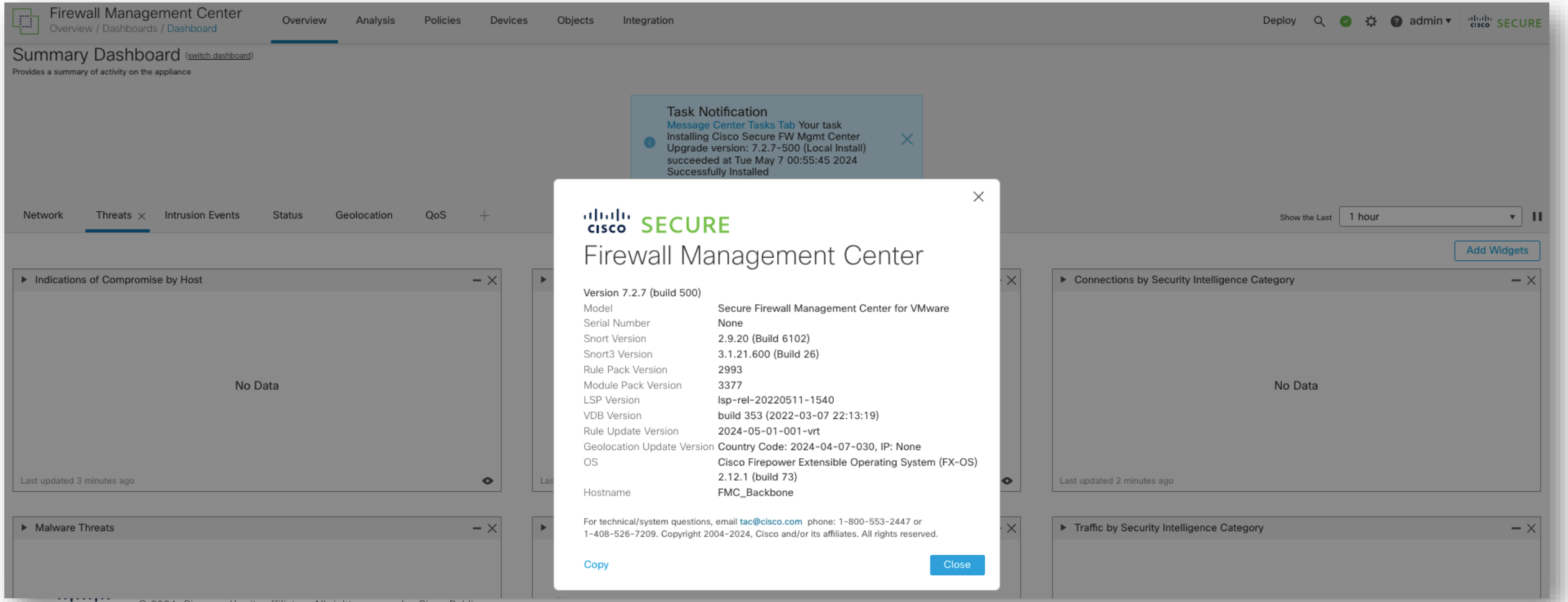
# Actualización de FMC

- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración



# Actualización de FMC

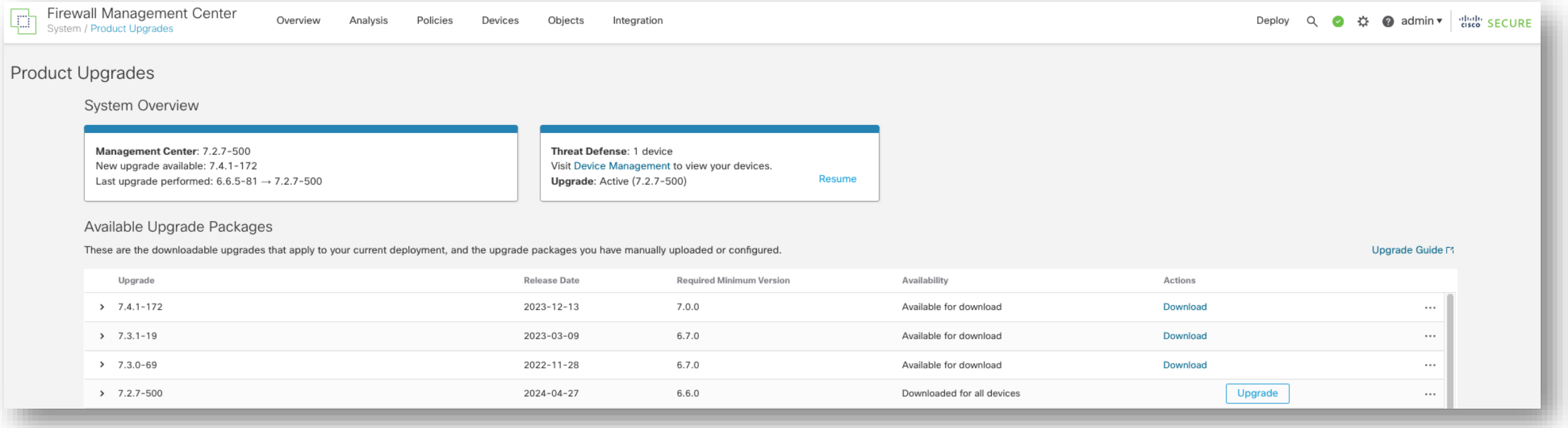
- Iniciar sesión en la interfaz gráfica del FMC y realizar las implementaciones de configuración



# Actualización de FTD

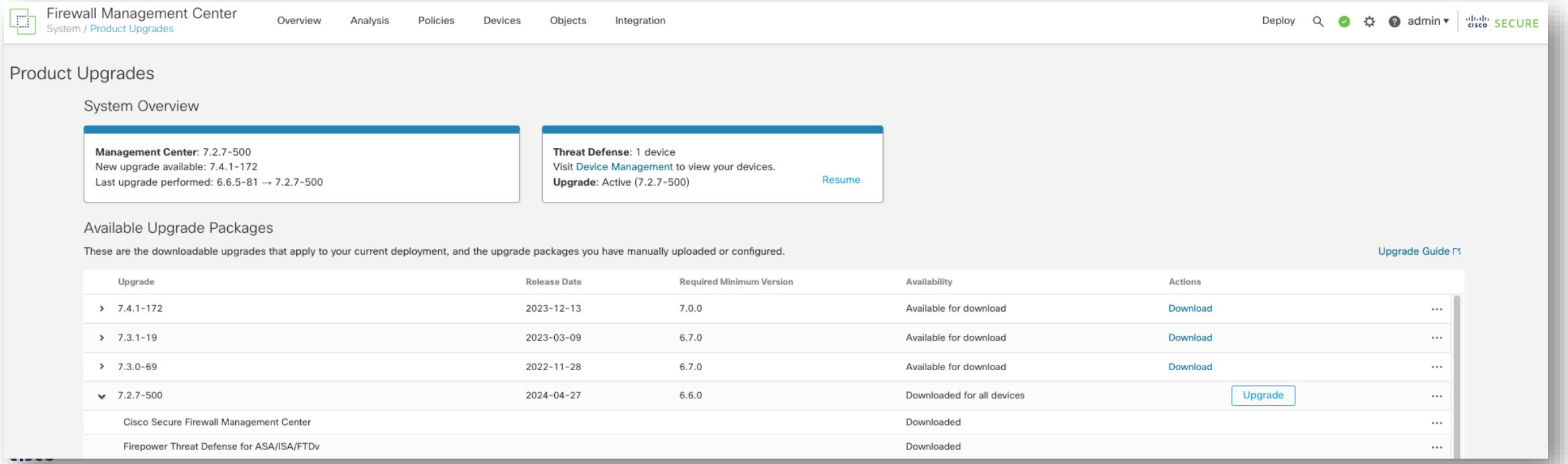
# Actualización de FTD

1. Iniciar sesión en la interfaz gráfica del FMC
2. Dirigirse a System (⚙) > Product Upgrades
3. Haz click en el botón de “Upgrade” sobre el paquete de actualización deseado para iniciar el asistente de actualización.



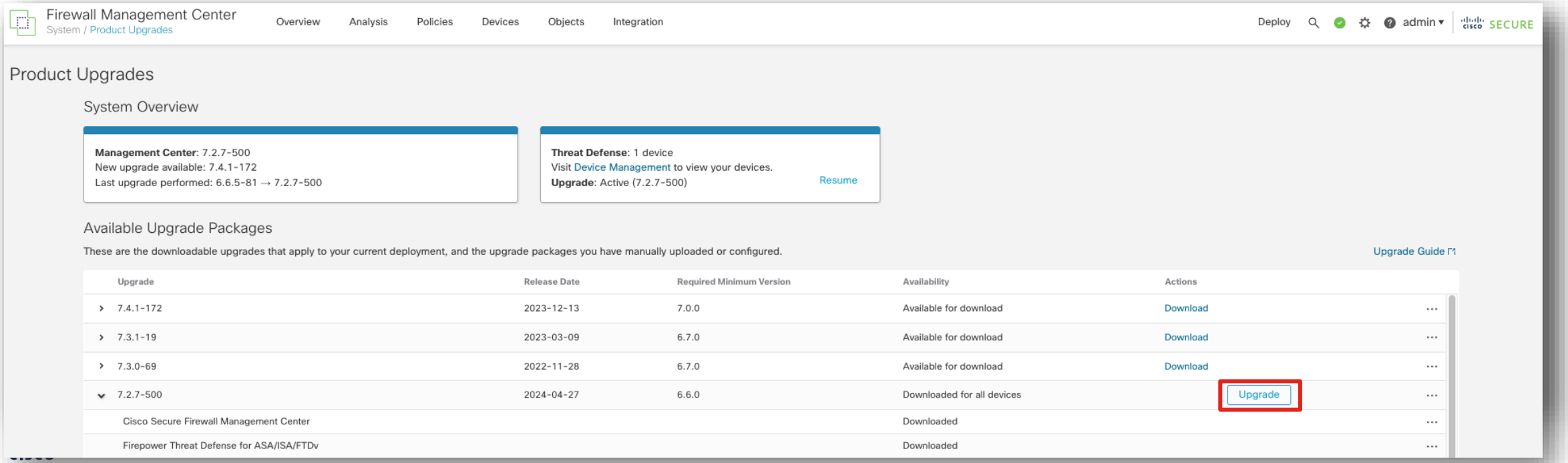
# Actualización de FTD

1. Iniciar sesión en la interfaz gráfica del FMC
2. Dirigirse a System (⚙) > Product Upgrades
3. Haz click en el botón de “Upgrade” sobre el paquete de actualización deseado para iniciar el asistente de actualización.



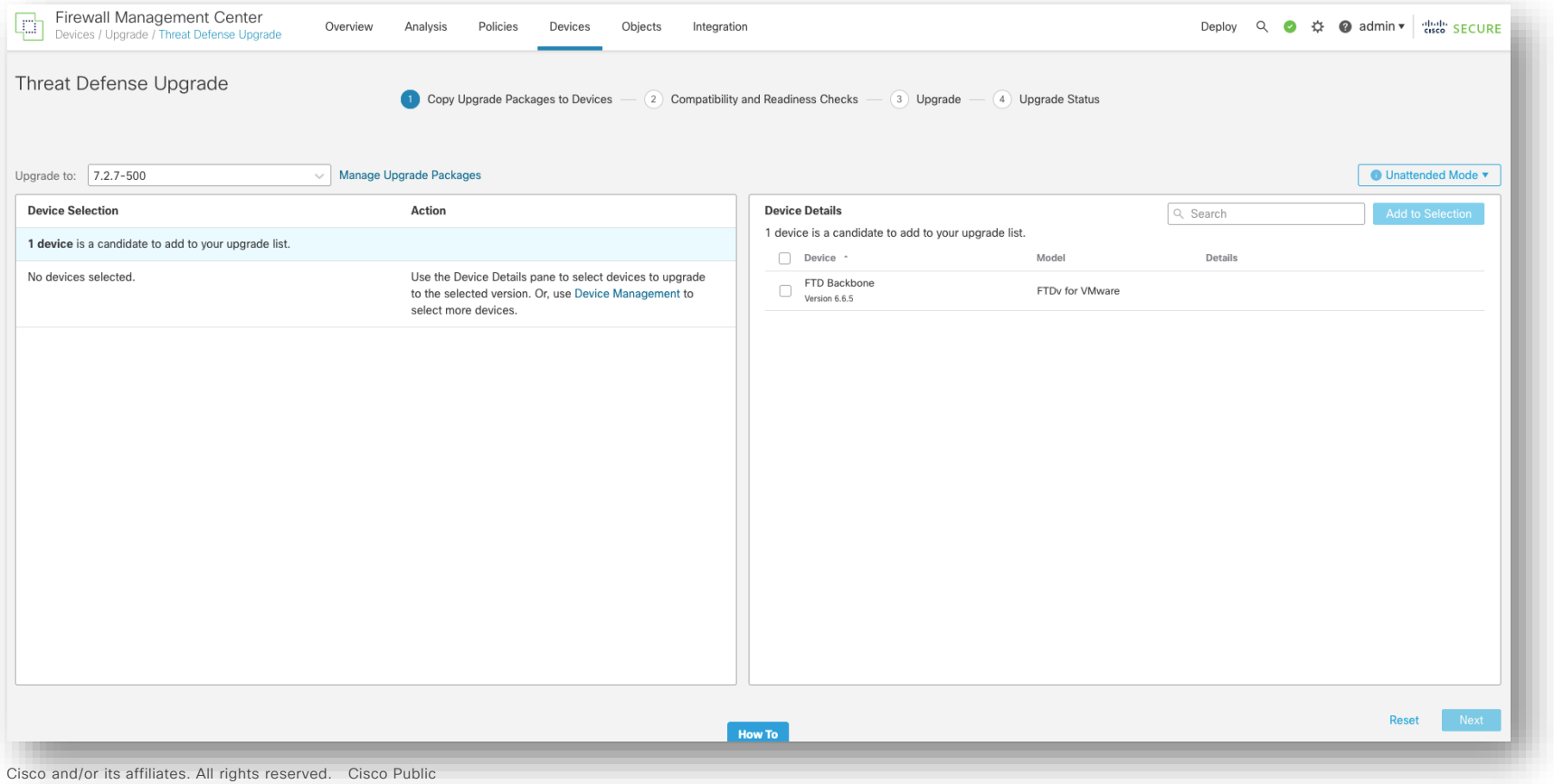
# Actualización de FTD

1. Iniciar sesión en la interfaz gráfica del FMC
2. Dirigirse a System (⚙) > Product Upgrades
3. Haz click en el botón de “Upgrade” sobre el paquete de actualización deseado para iniciar el asistente de actualización.



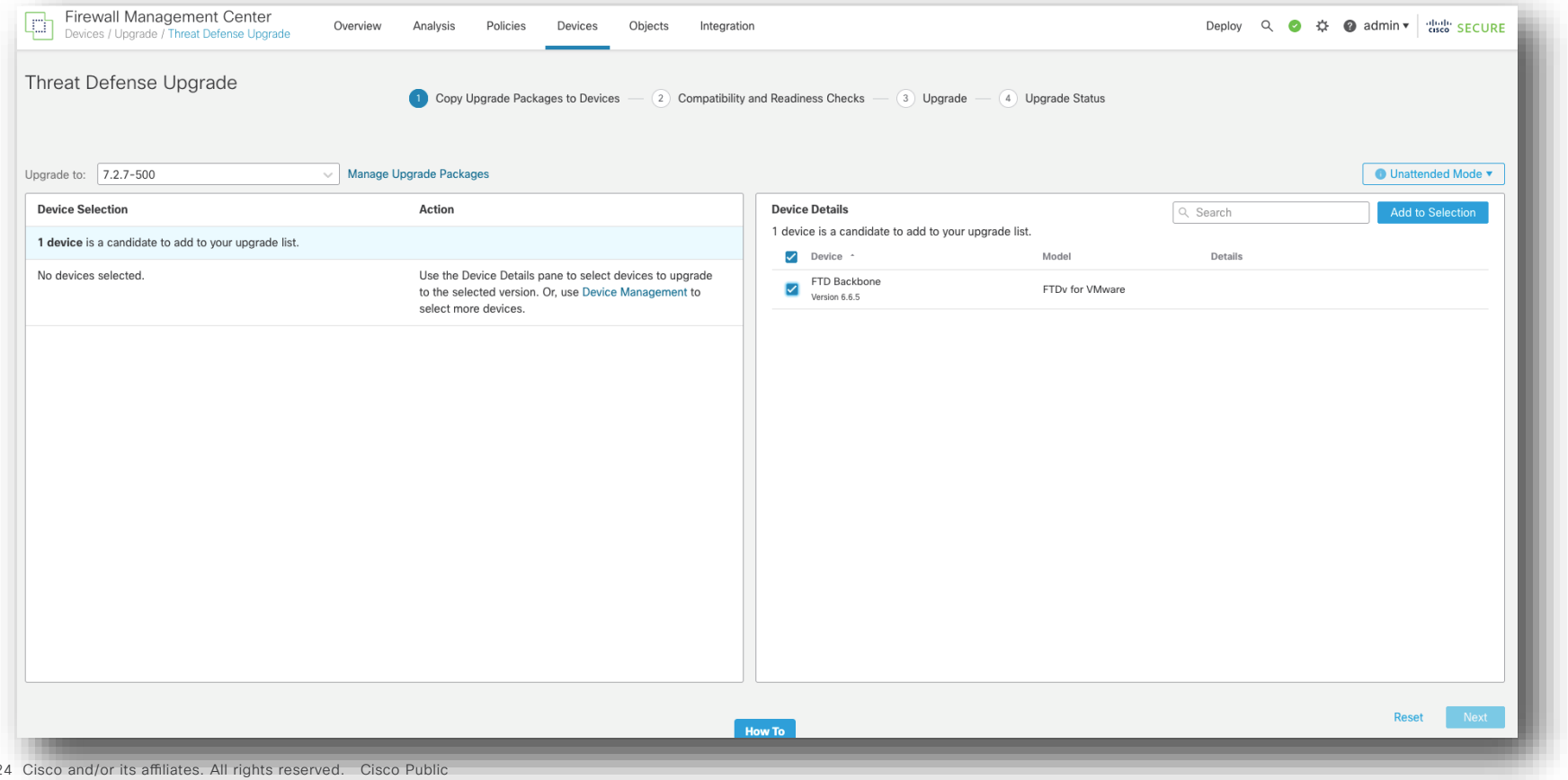
# Actualización de FTD

1. Selecciona los equipos a actualizar
2. Haz click en “Add to Selection” para agregarlos a la lista de actualización



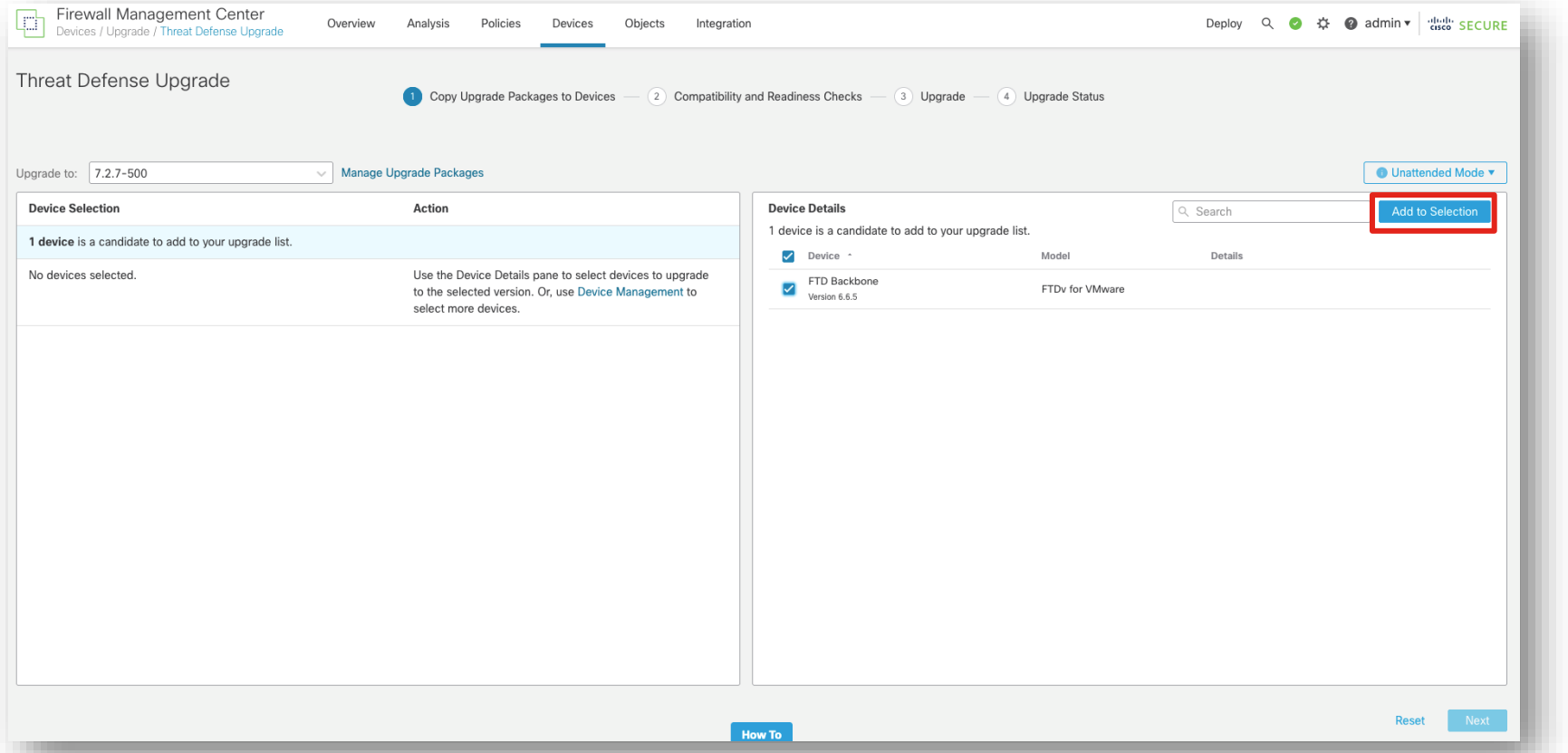
# Actualización de FTD

1. Selecciona los equipos a actualizar
2. Haz click en “Add to Selection” para agregarlos a la lista de actualización



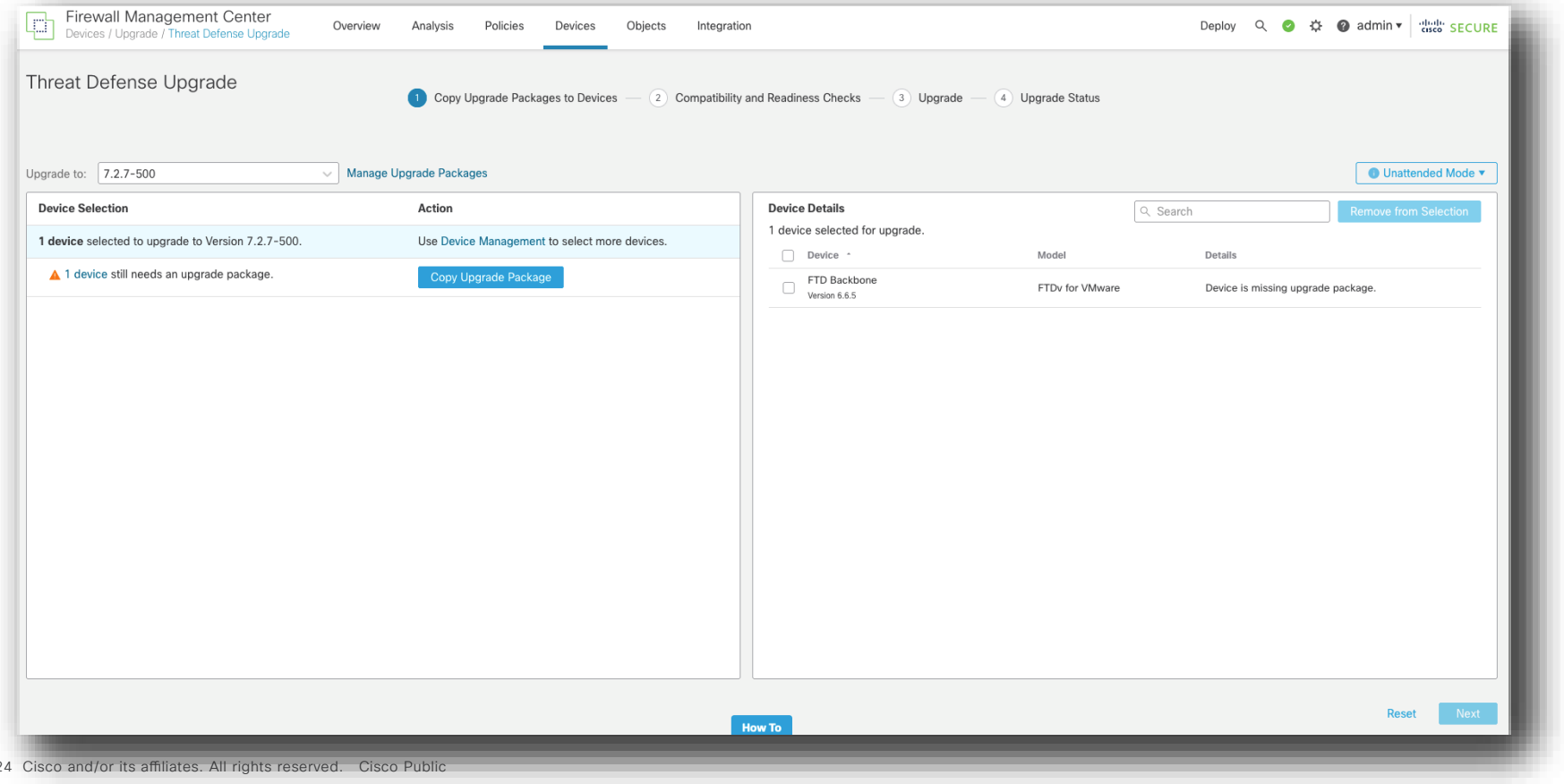
# Actualización de FTD

1. Selecciona los equipos a actualizar
2. Haz click en “Add to Selection” para agregarlos a la lista de actualización



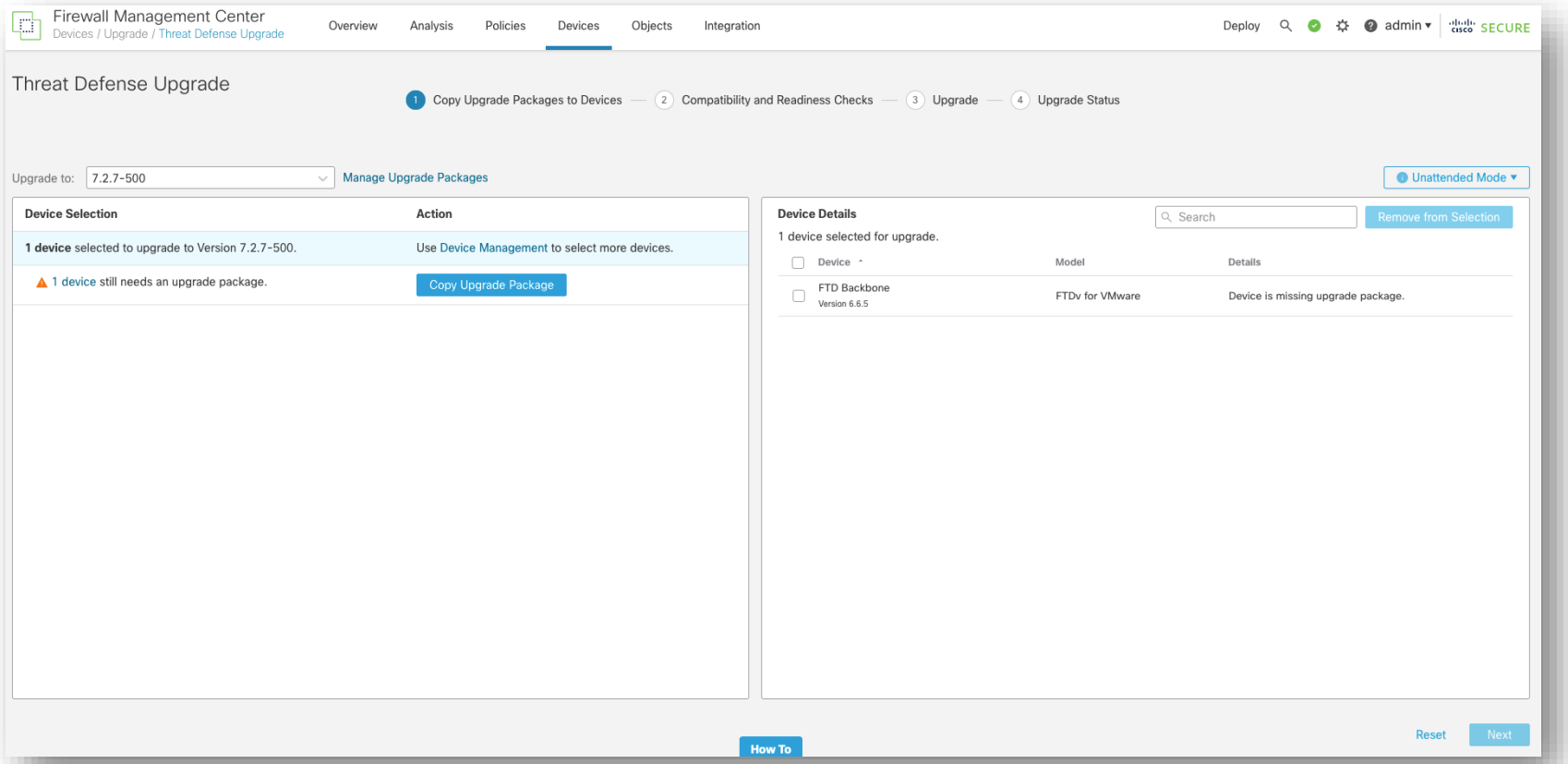
# Actualización de FTD

1. Selecciona los equipos a actualizar
2. Haz click en “Add to Selection” para agregarlos a la lista de actualización



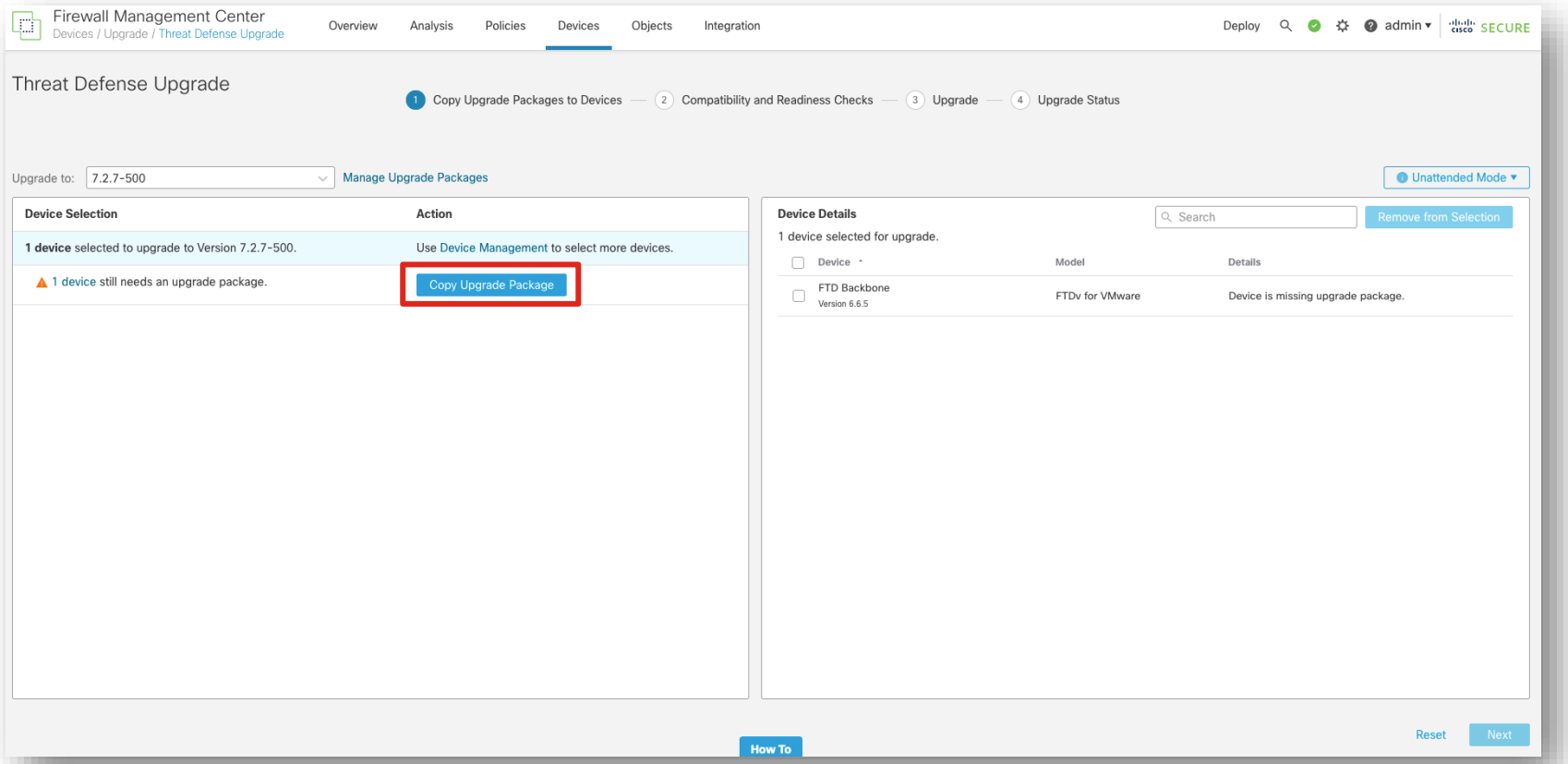
# Actualización de FTD

1. Haz click en “Copy Upgrade Package” para enviar el paquete de instalación al FTD



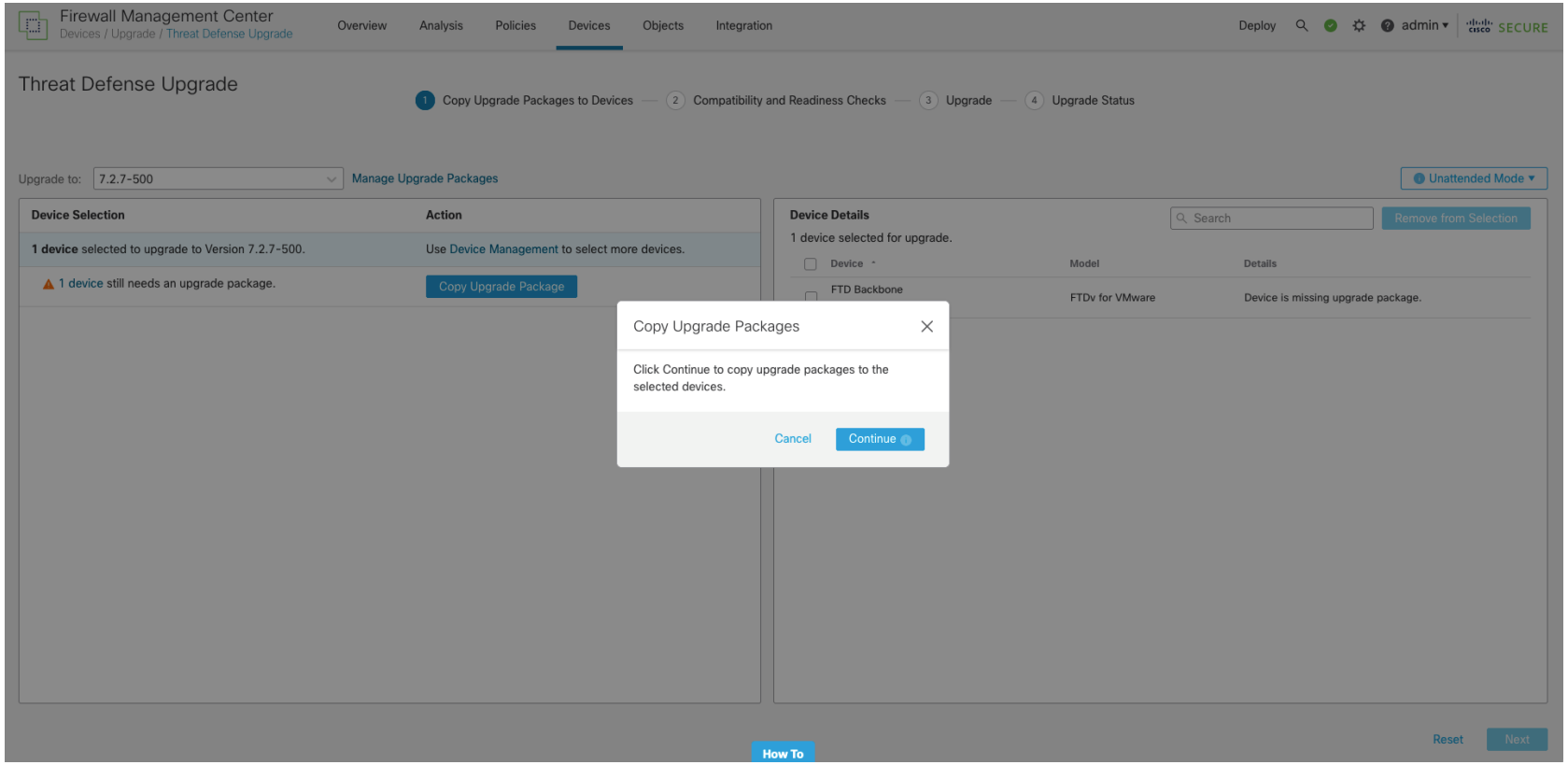
# Actualización de FTD

1. Haz click en “Copy Upgrade Package” para enviar el paquete de instalación al FTD



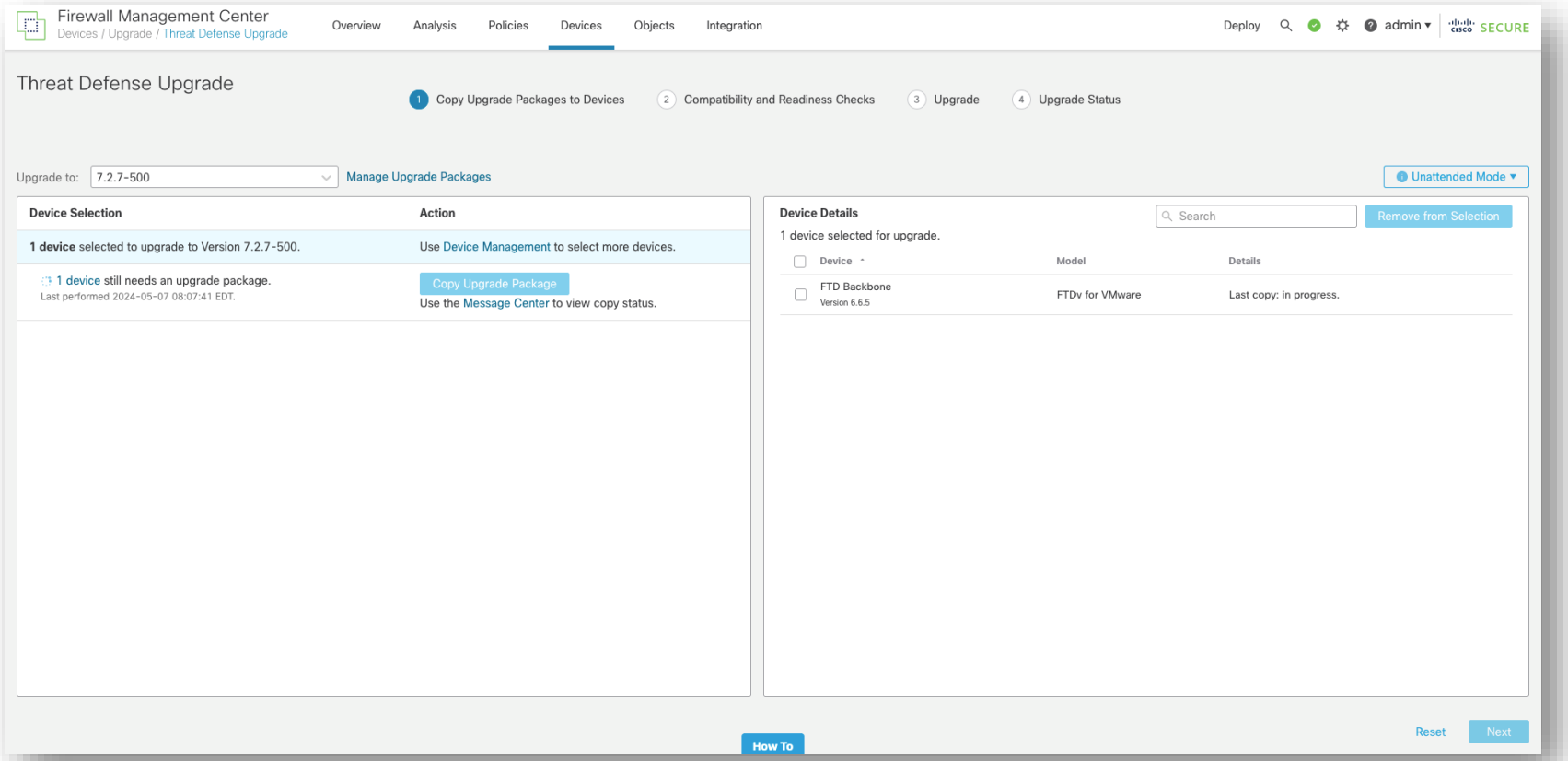
# Actualización de FTD

1. Haz click en “Copy Upgrade Package” para enviar el paquete de instalación al FTD



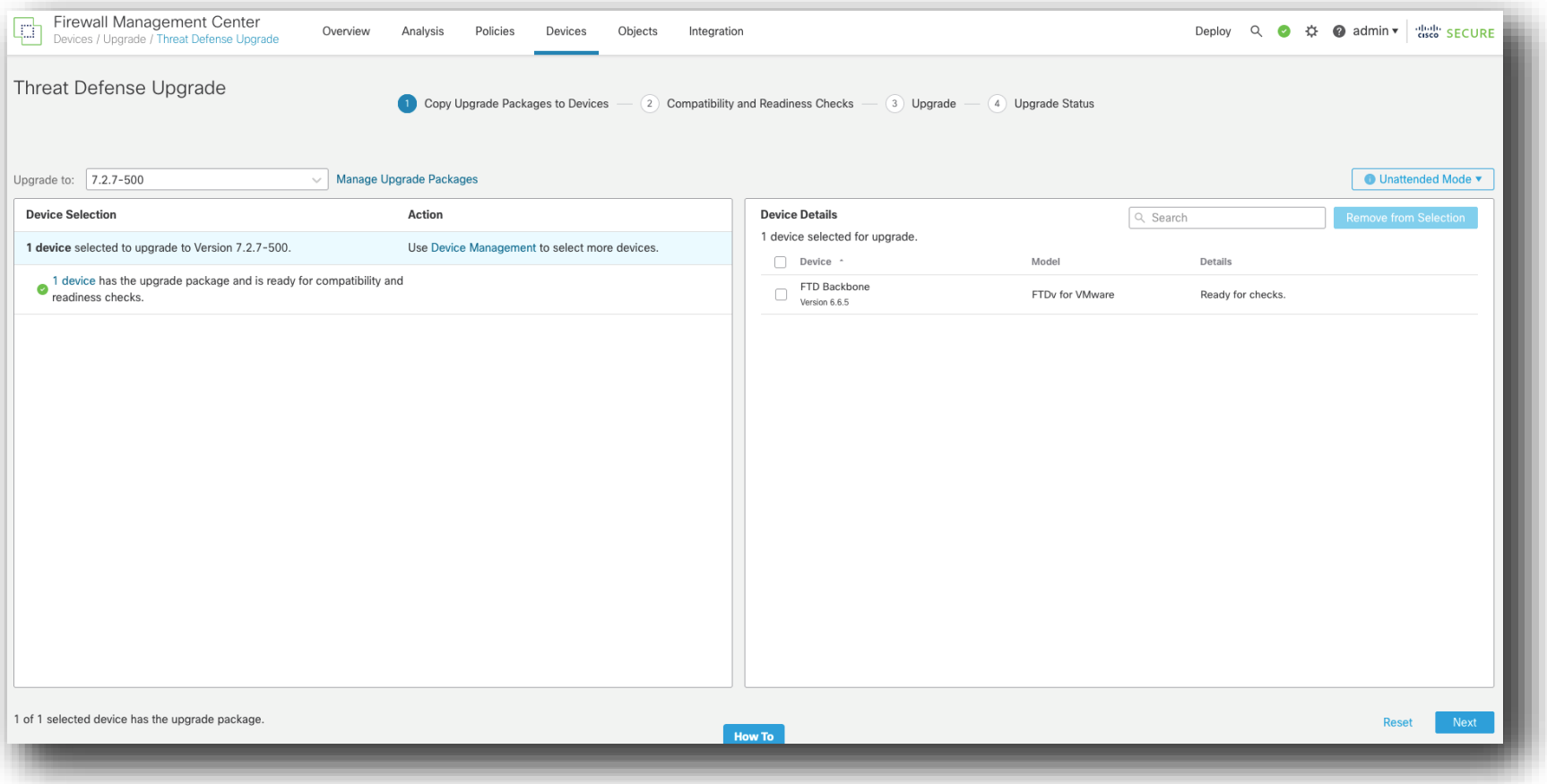
# Actualización de FTD

1. Haz click en “Copy Upgrade Package” para enviar el paquete de instalación al FTD



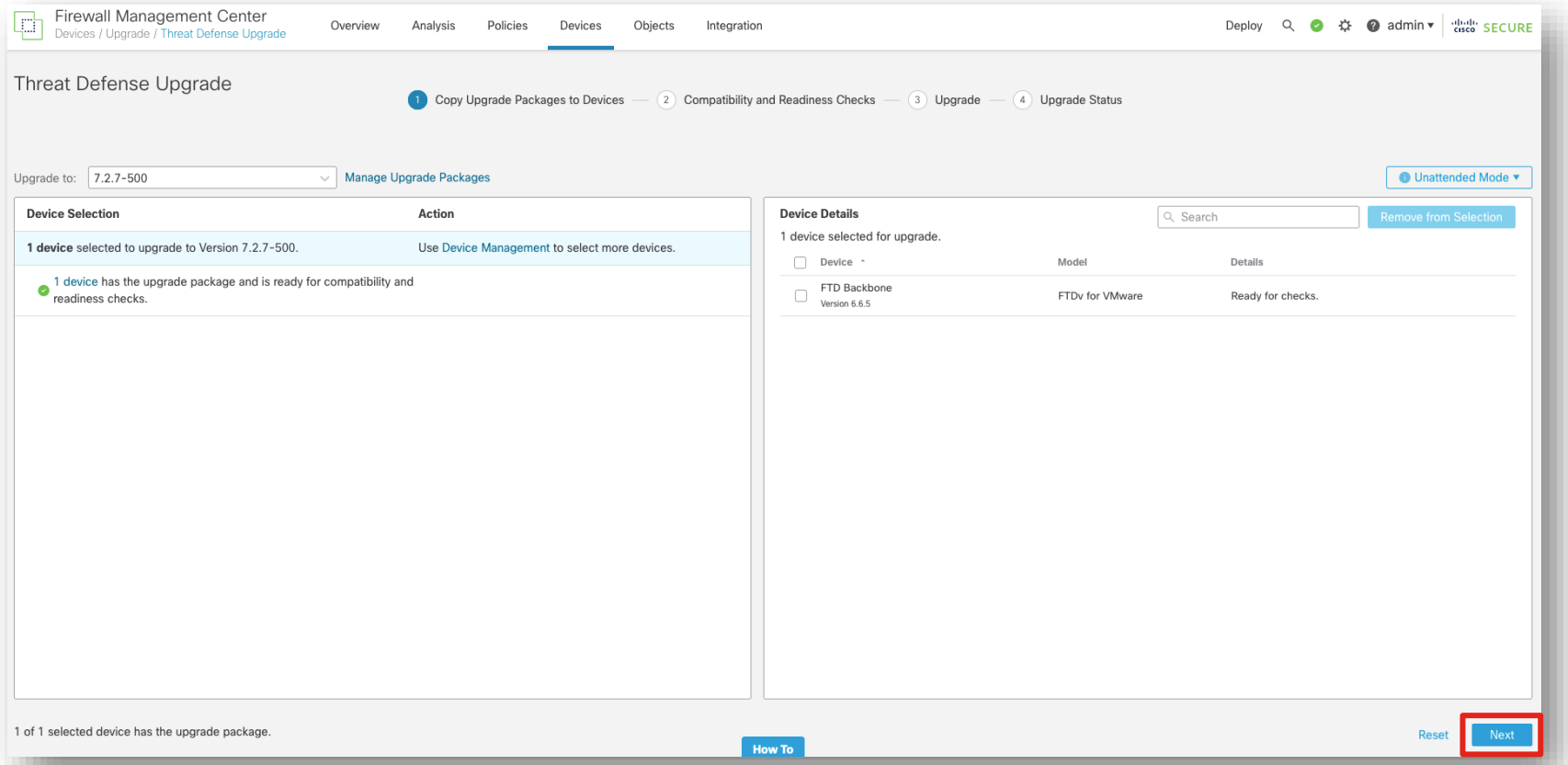
# Actualización de FTD

1. Haz click en “Copy Upgrade Package” para enviar el paquete de instalación al FTD



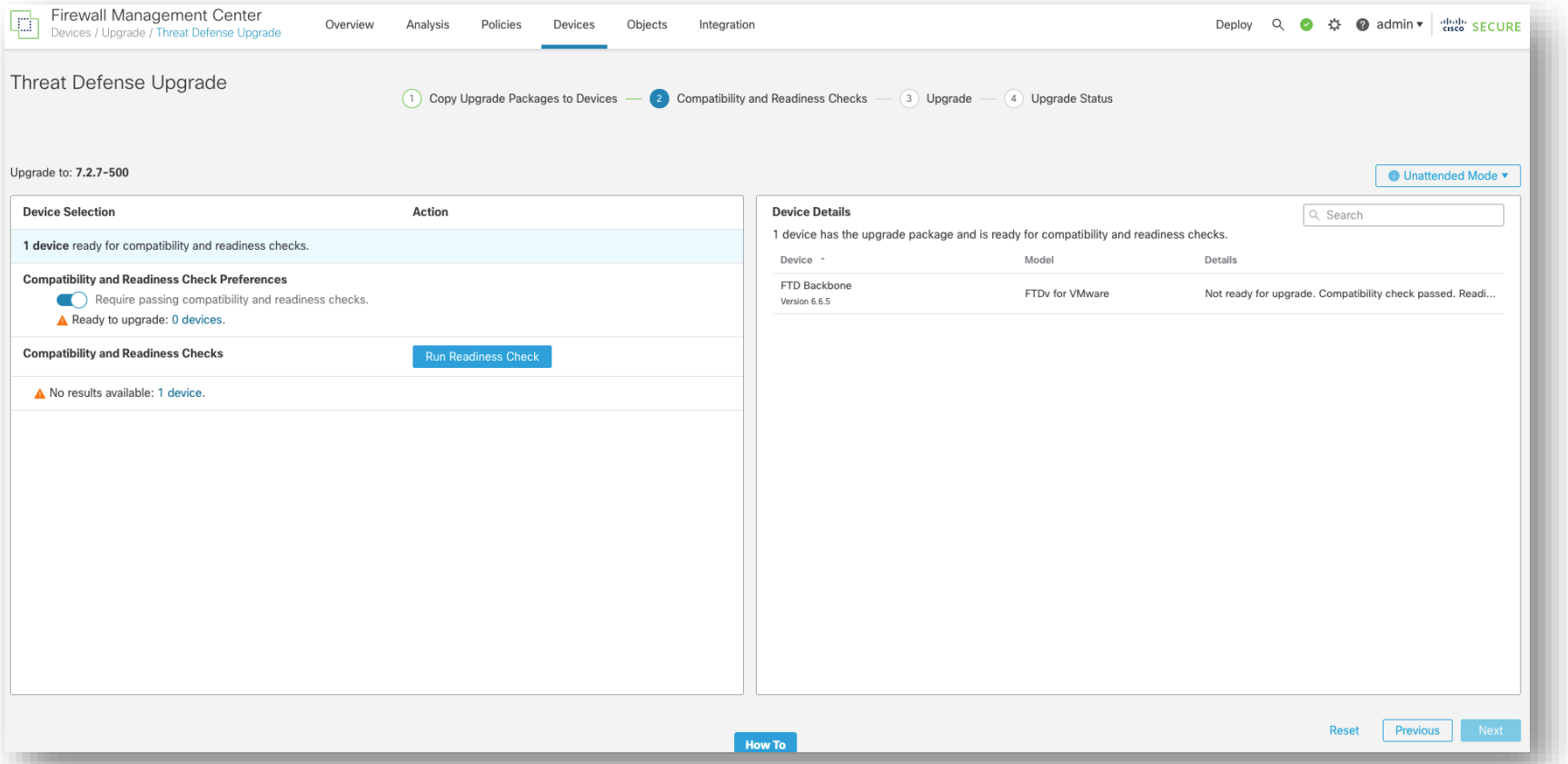
# Actualización de FTD

1. Haz click en “Copy Upgrade Package” para enviar el paquete de instalación al FTD



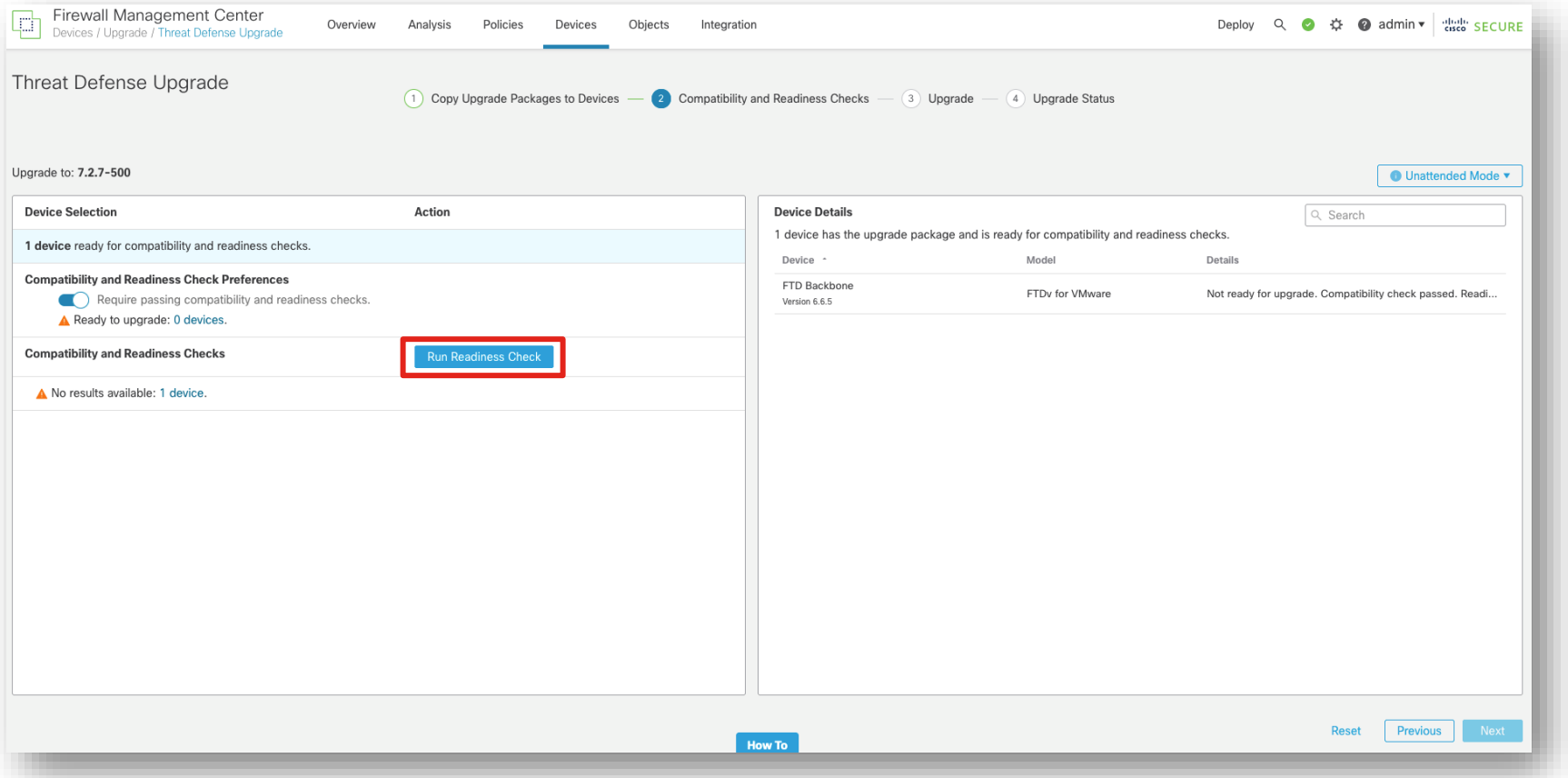
# Actualización de FTD

1. Haz click en “Run Readiness Check” para realizar las validaciones técnicas del firewall



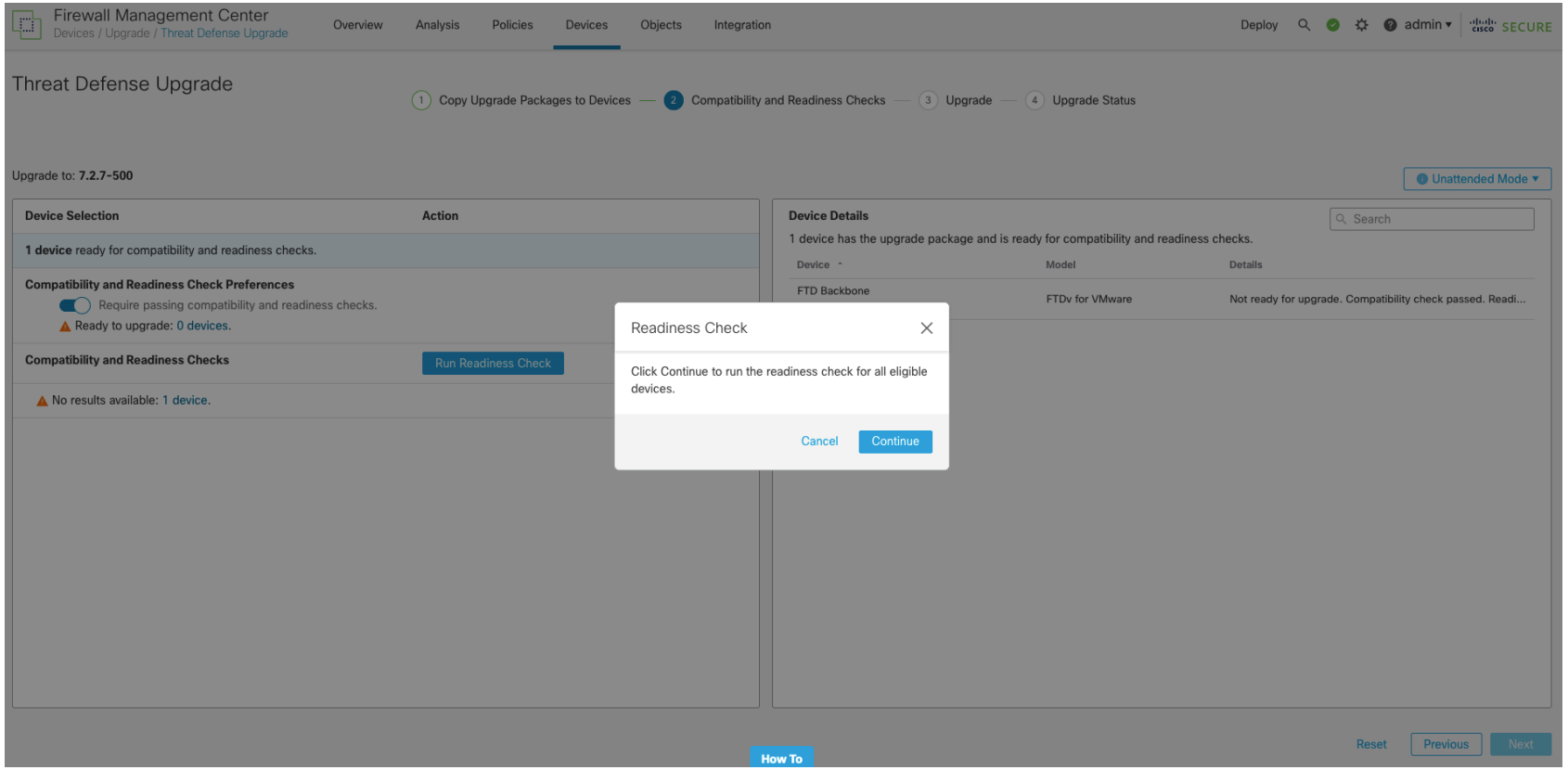
# Actualización de FTD

1. Haz click en “Run Readiness Check” para realizar las validaciones técnicas del firewall



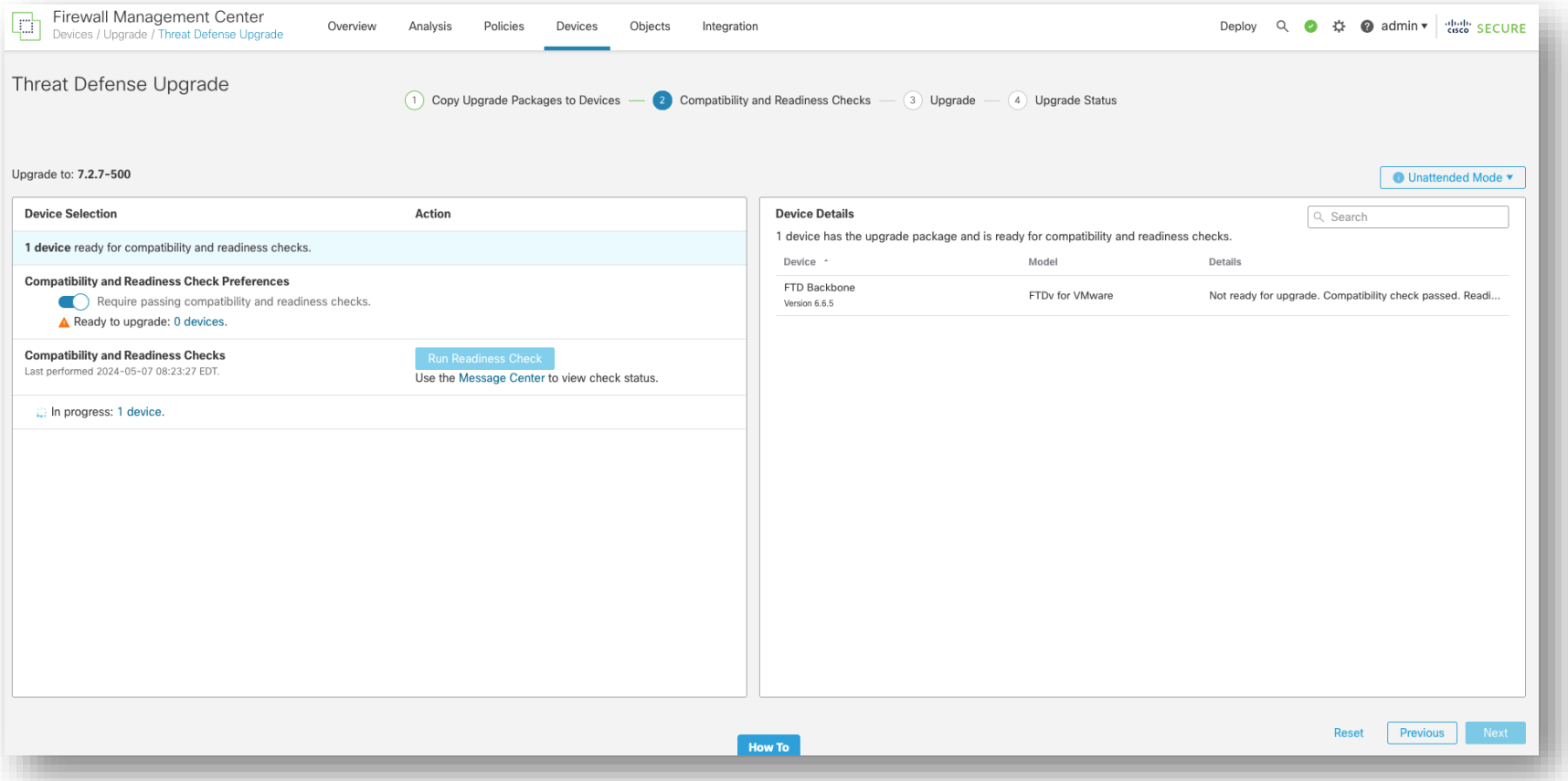
# Actualización de FTD

1. Haz click en “Run Readiness Check” para realizar las validaciones técnicas del firewall



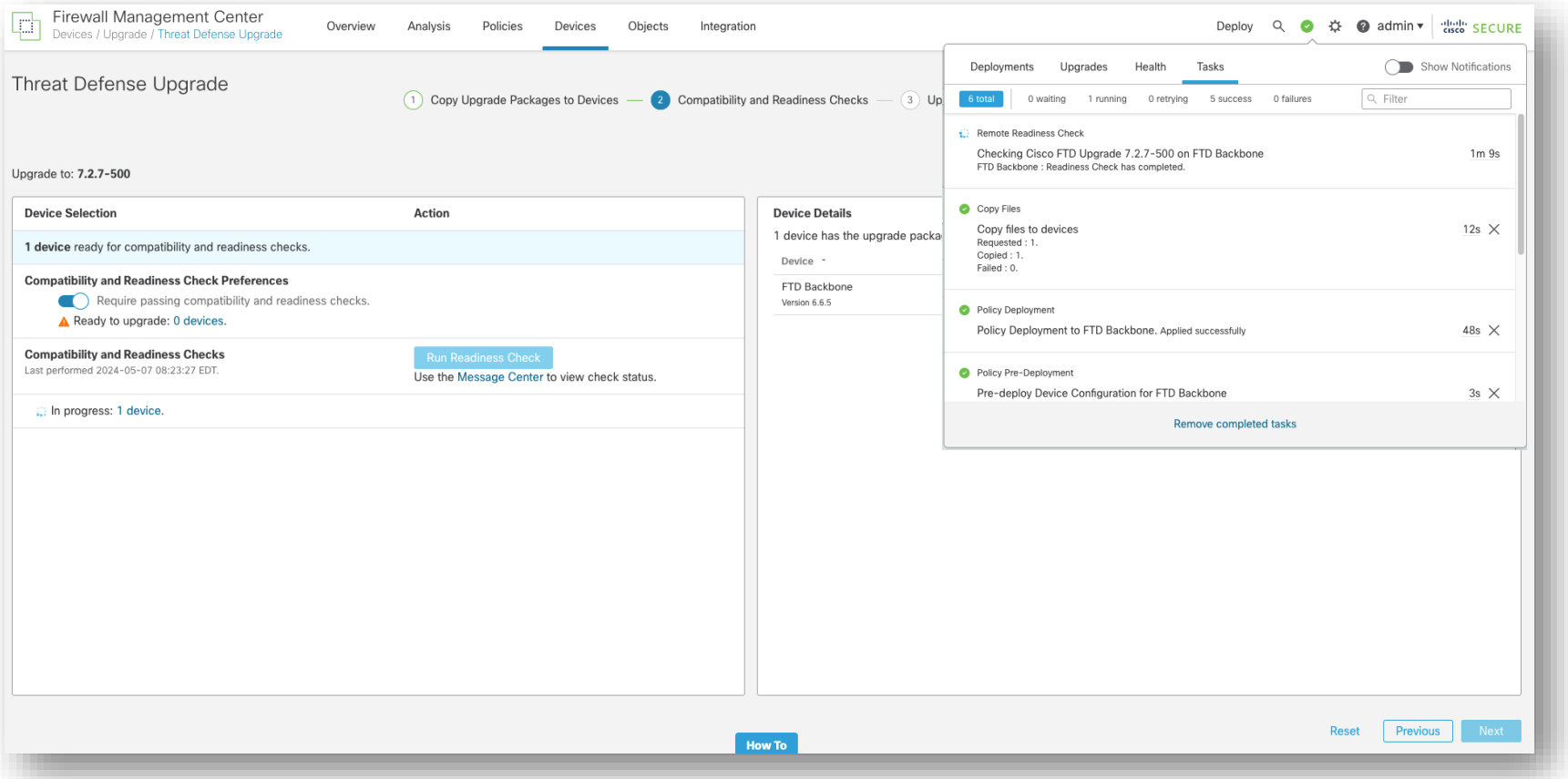
# Actualización de FTD

1. Haz click en “Run Readiness Check” para realizar las validaciones técnicas del firewall



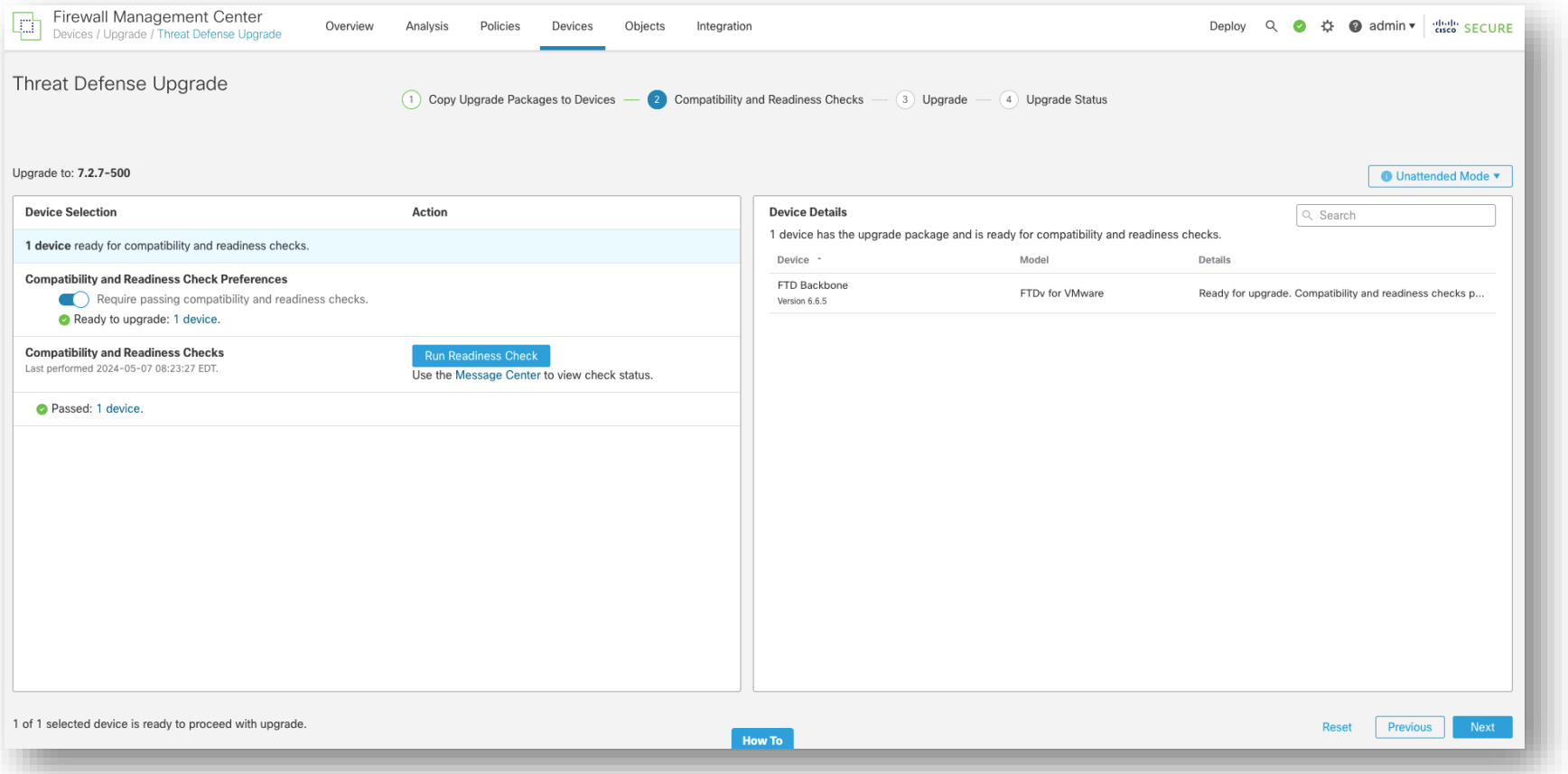
# Actualización de FTD

1. Haz click en “Run Readiness Check” para realizar las validaciones técnicas del firewall



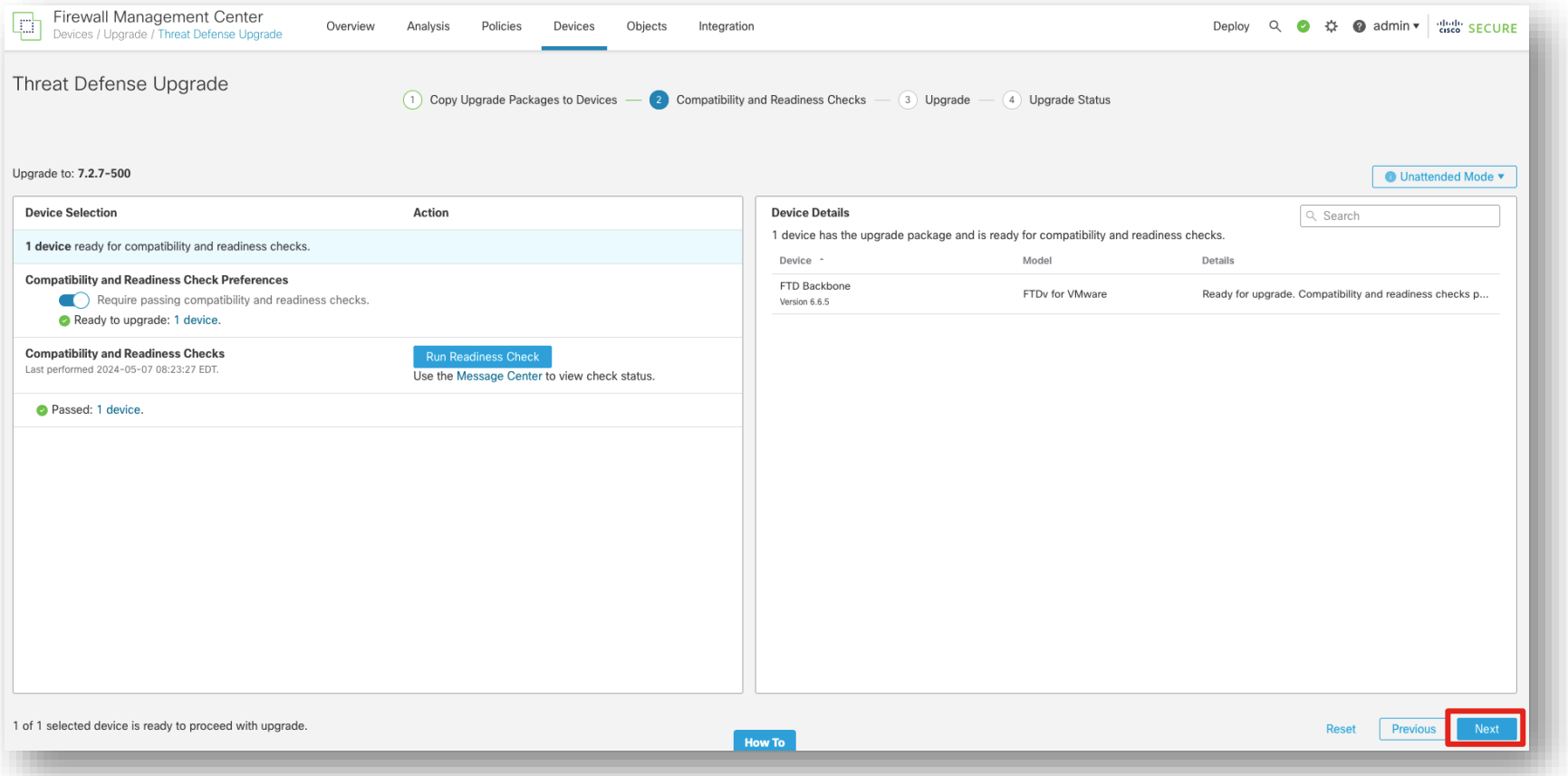
# Actualización de FTD

1. Haz click en “Run Readiness Check” para realizar las validaciones técnicas del firewall



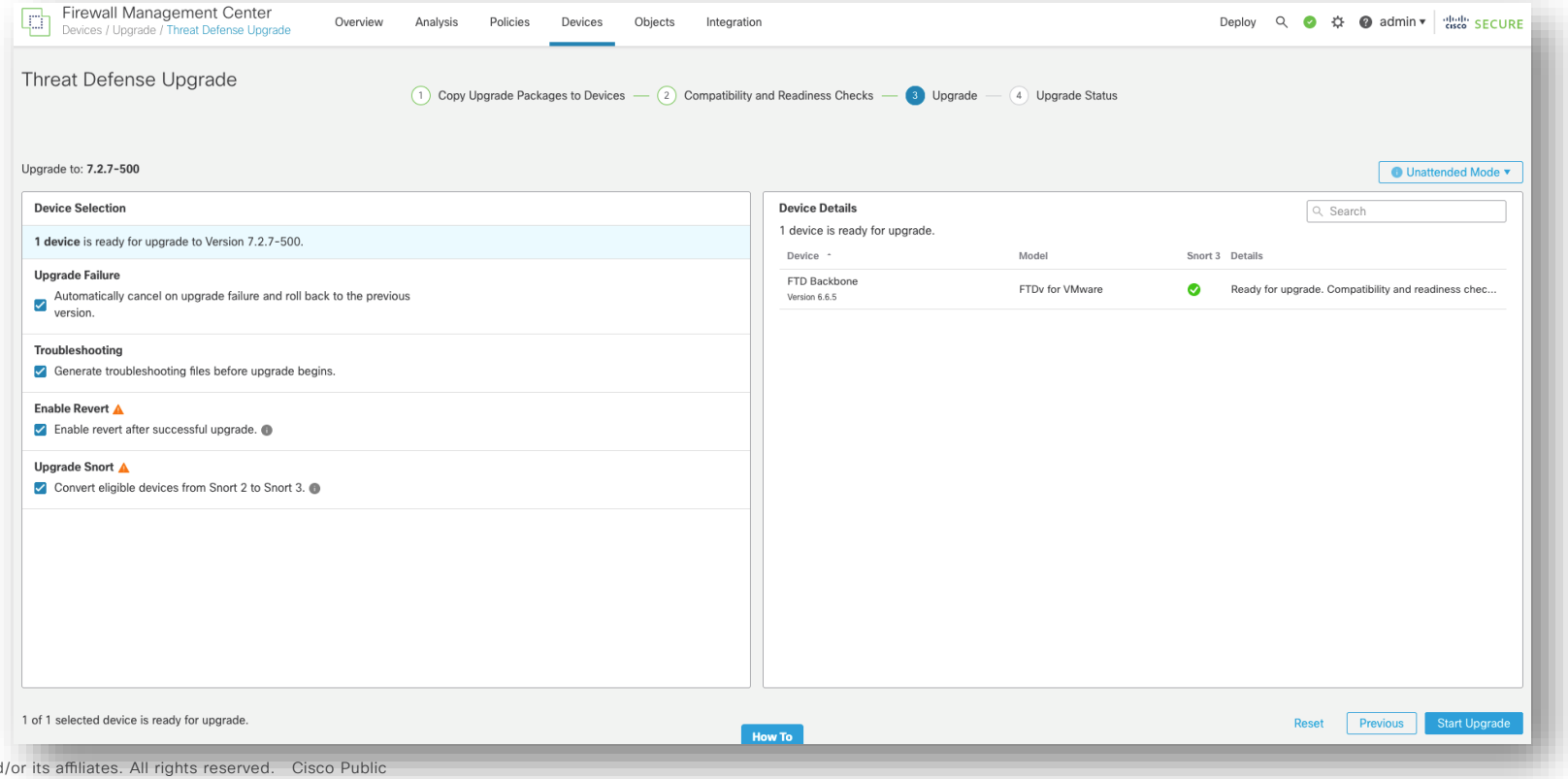
# Actualización de FTD

1. Haz click en “Run Readiness Check” para realizar las validaciones técnicas del firewall



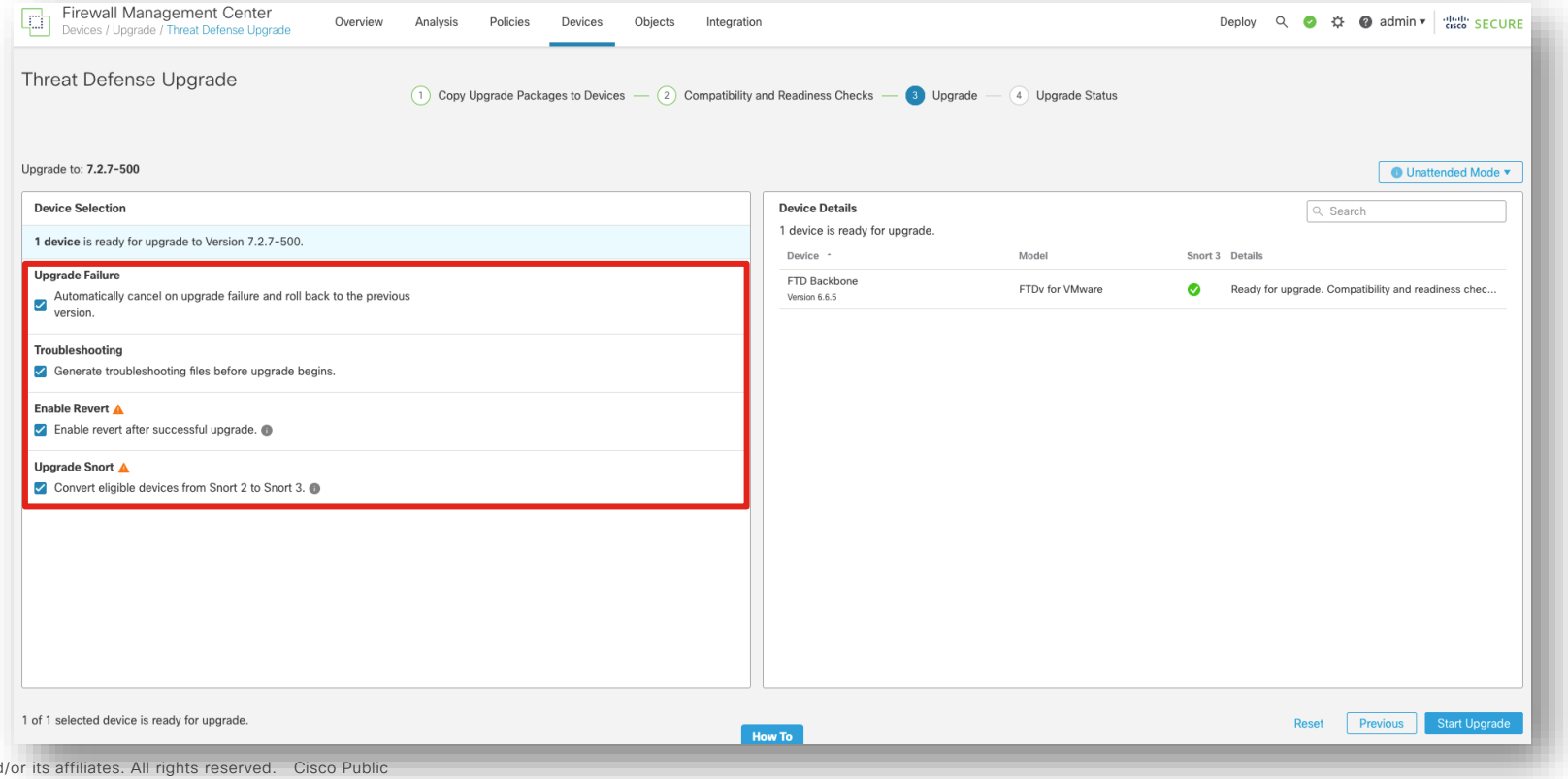
# Actualización de FTD

1. (Opcional) Selecciona las opciones que desees habilitar para realizar la actualización
2. Haz click en “Start Upgrade” para iniciar la actualización en el FTD



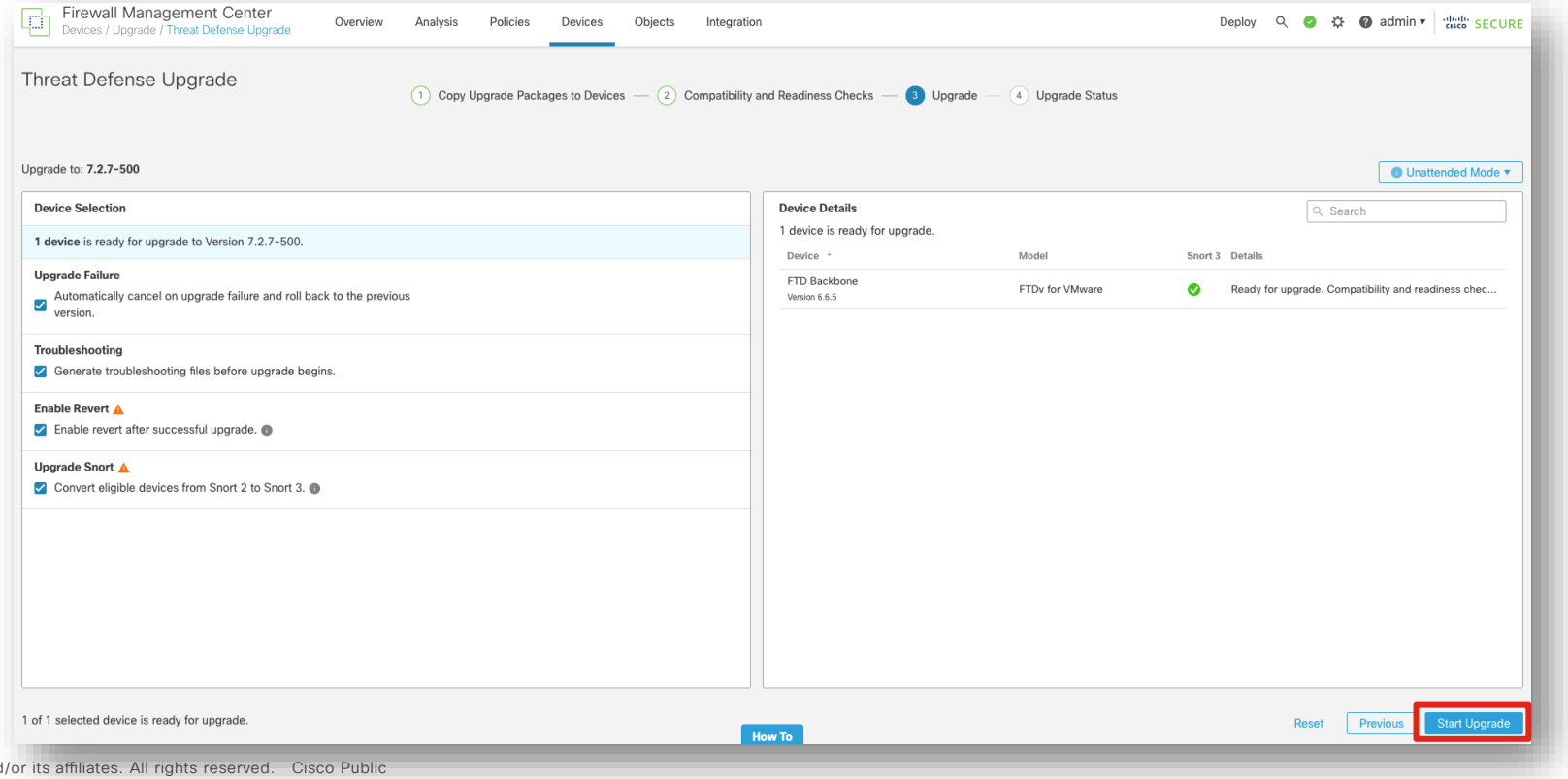
# Actualización de FTD

1. (Opcional) Selecciona las opciones que desees habilitar para realizar la actualización
2. Haz click en “Start Upgrade” para iniciar la actualización en el FTD



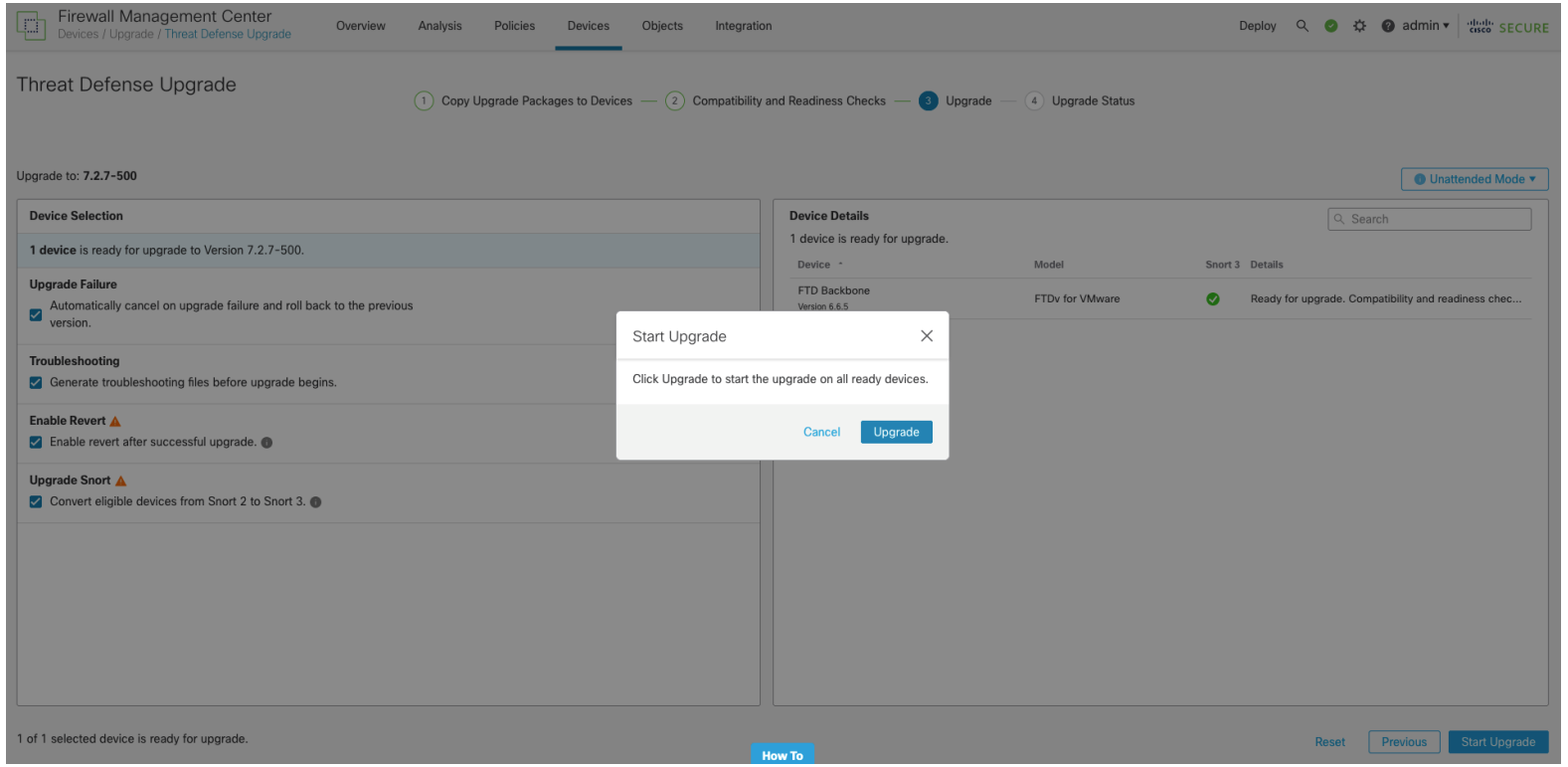
# Actualización de FTD

1. (Opcional) Selecciona las opciones que desees habilitar para realizar la actualización
2. Haz click en “Start Upgrade” para iniciar la actualización en el FTD



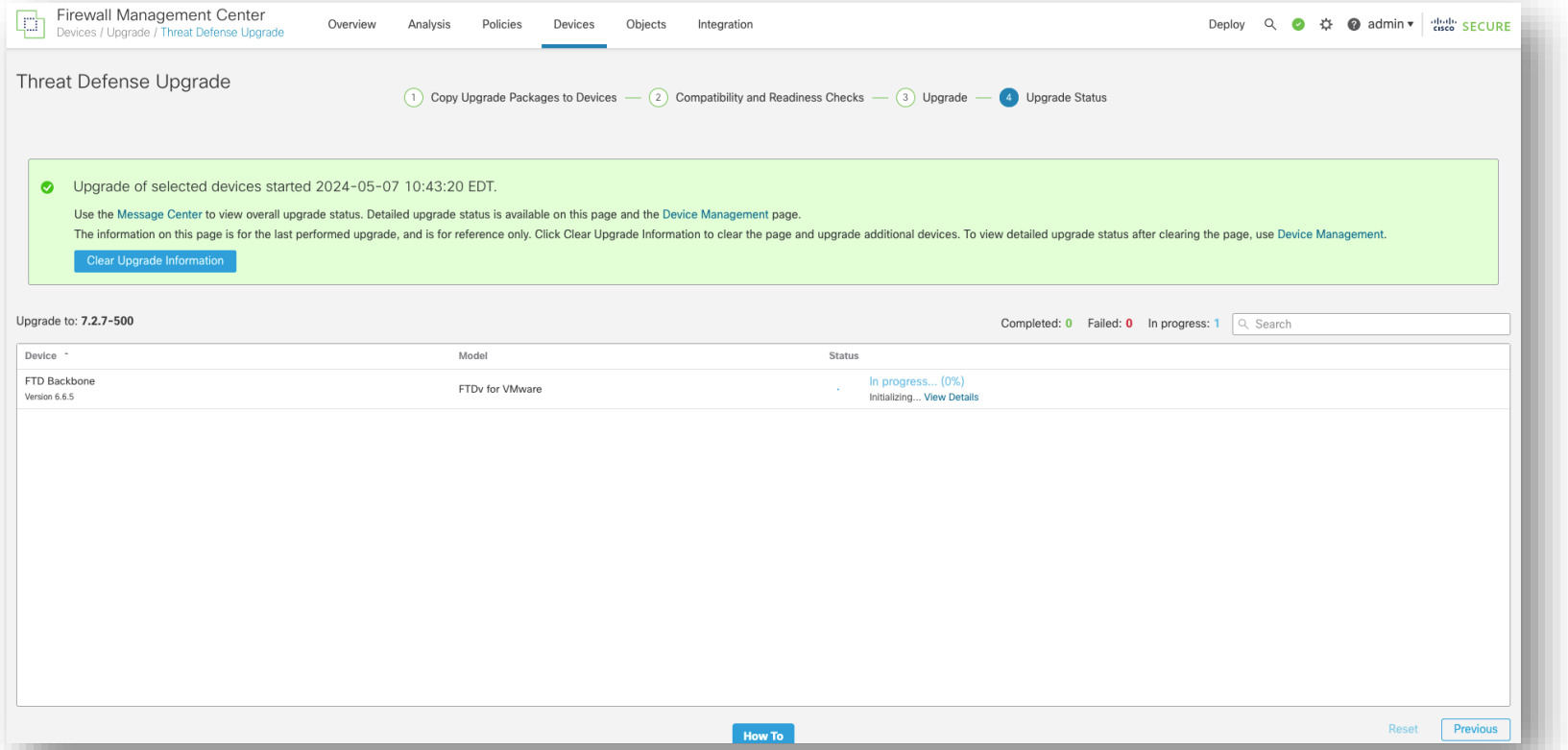
# Actualización de FTD

1. (Opcional) Selecciona las opciones que desees habilitar para realizar la actualización
2. Haz click en “Start Upgrade” para iniciar la actualización en el FTD



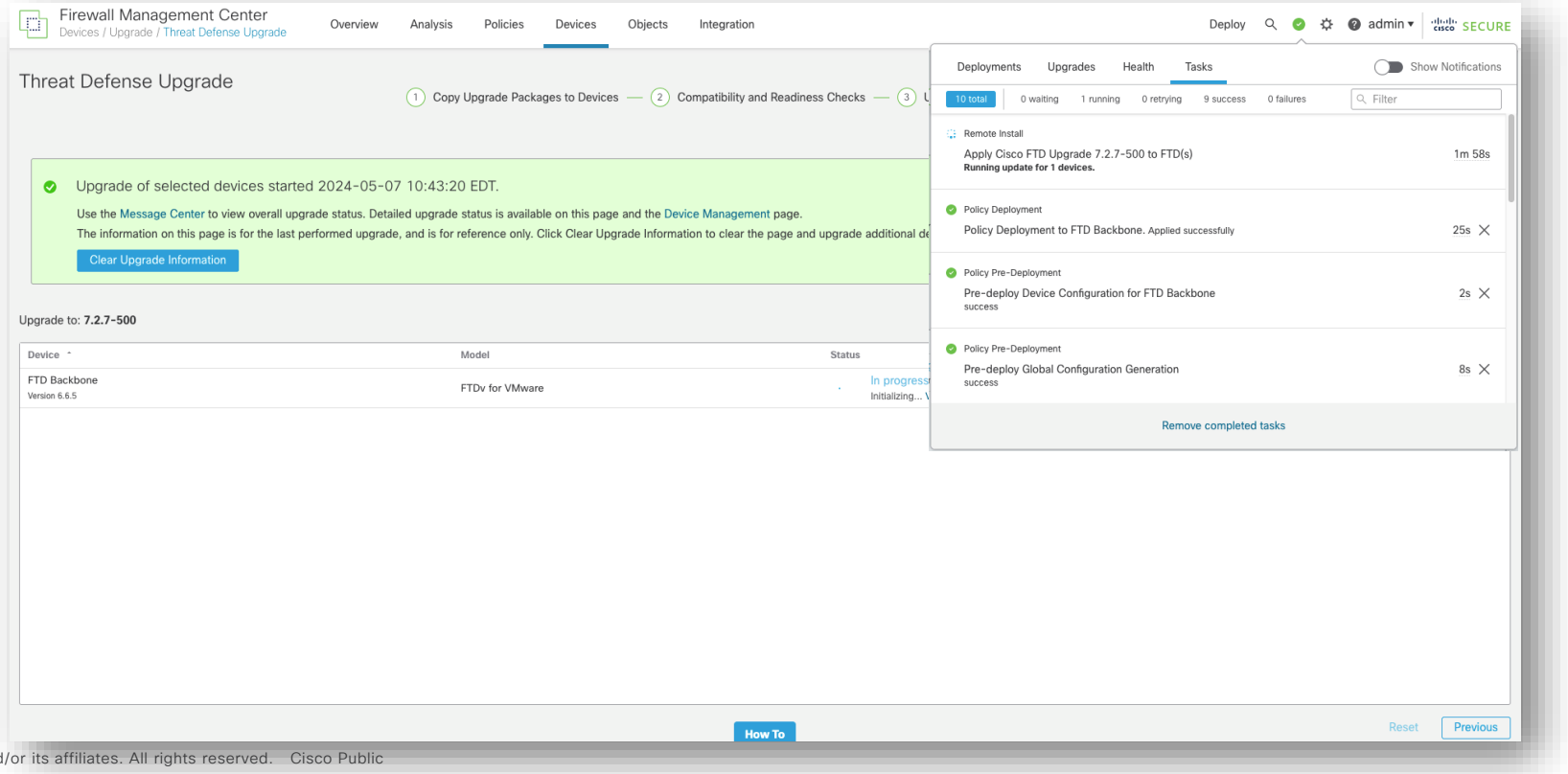
# Actualización de FTD

1. (Opcional) Selecciona las opciones que desees habilitar para realizar la actualización
2. Haz click en “Start Upgrade” para iniciar la actualización en el FTD



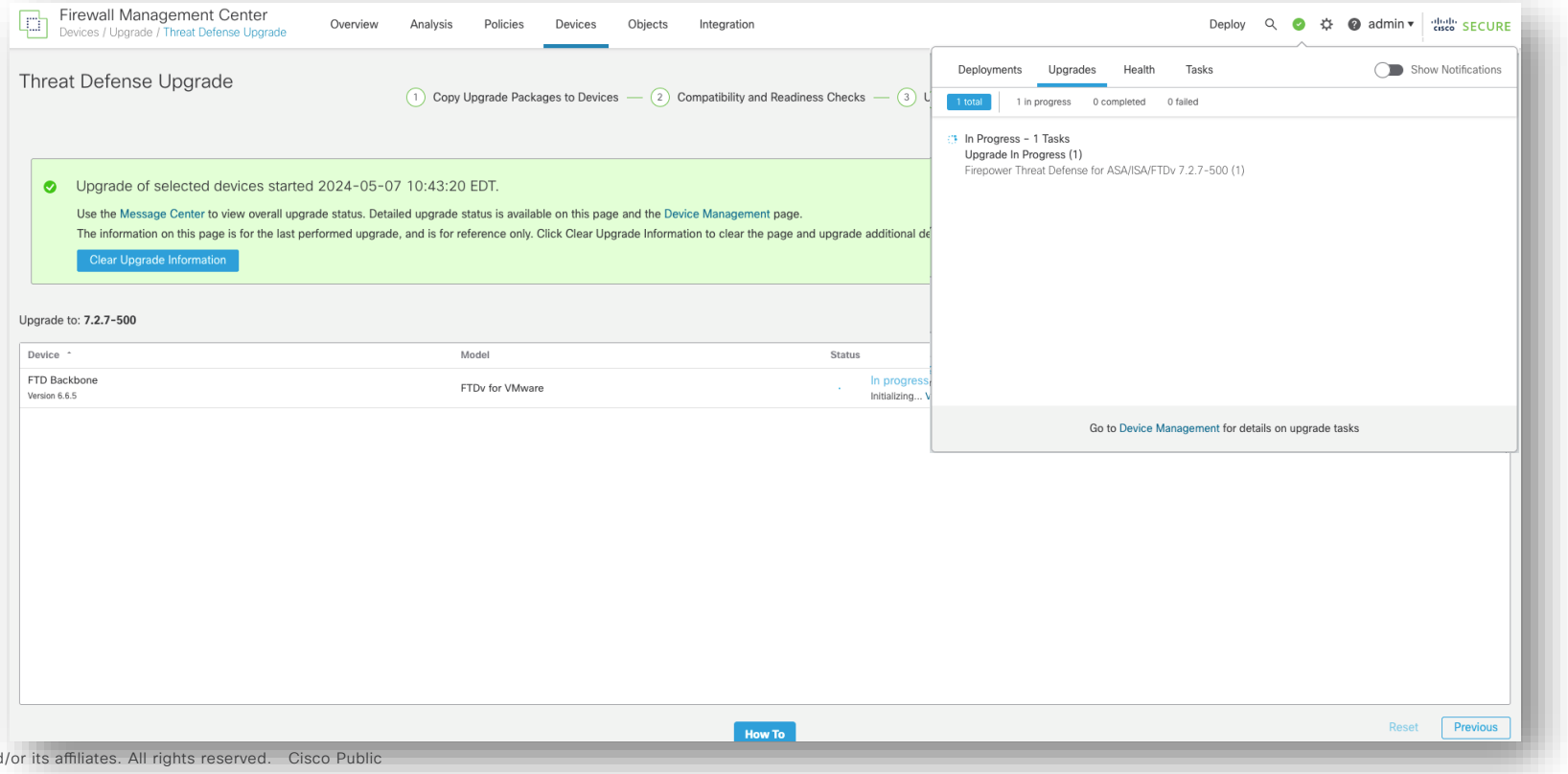
# Actualización de FTD

1. (Opcional) Selecciona las opciones que desees habilitar para realizar la actualización
2. Haz click en “Start Upgrade” para iniciar la actualización en el FTD



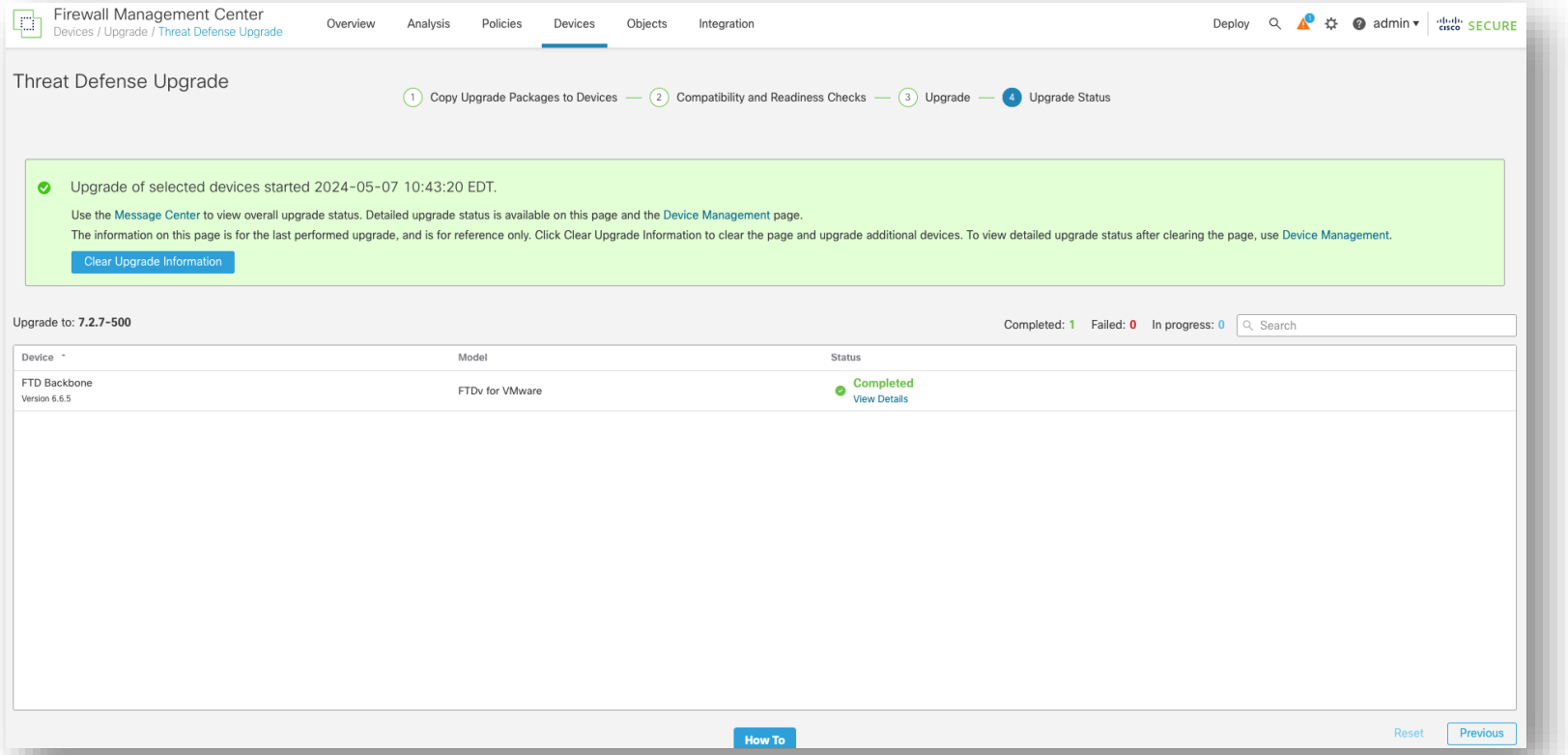
# Actualización de FTD

1. (Opcional) Selecciona las opciones que desees habilitar para realizar la actualización
2. Haz click en “Start Upgrade” para iniciar la actualización en el FTD



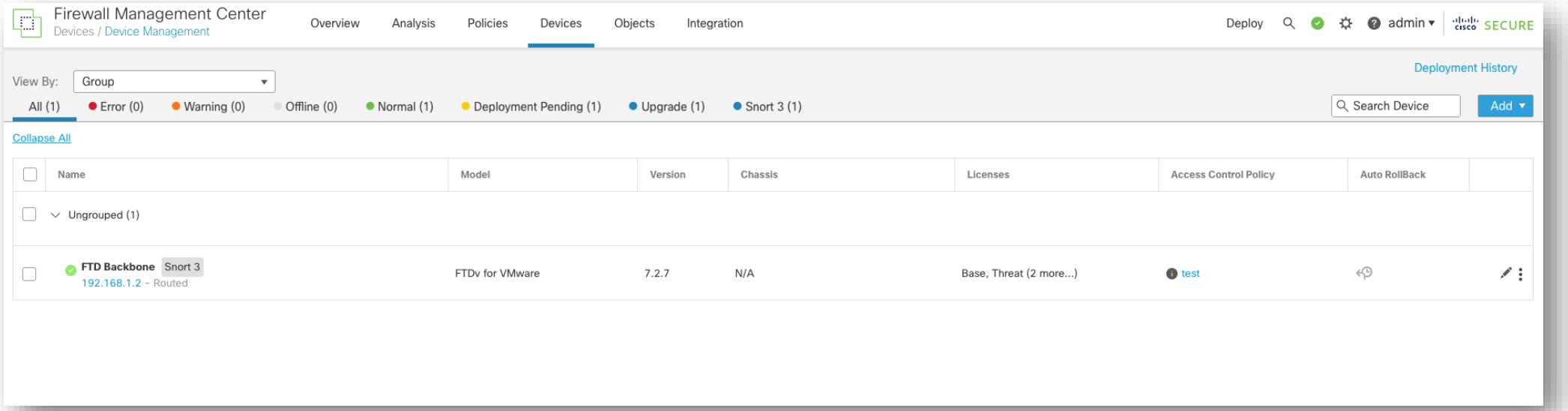
# Actualización de FTD

1. (Opcional) Selecciona las opciones que desees habilitar para realizar la actualización
2. Haz click en “Start Upgrade” para iniciar la actualización en el FTD



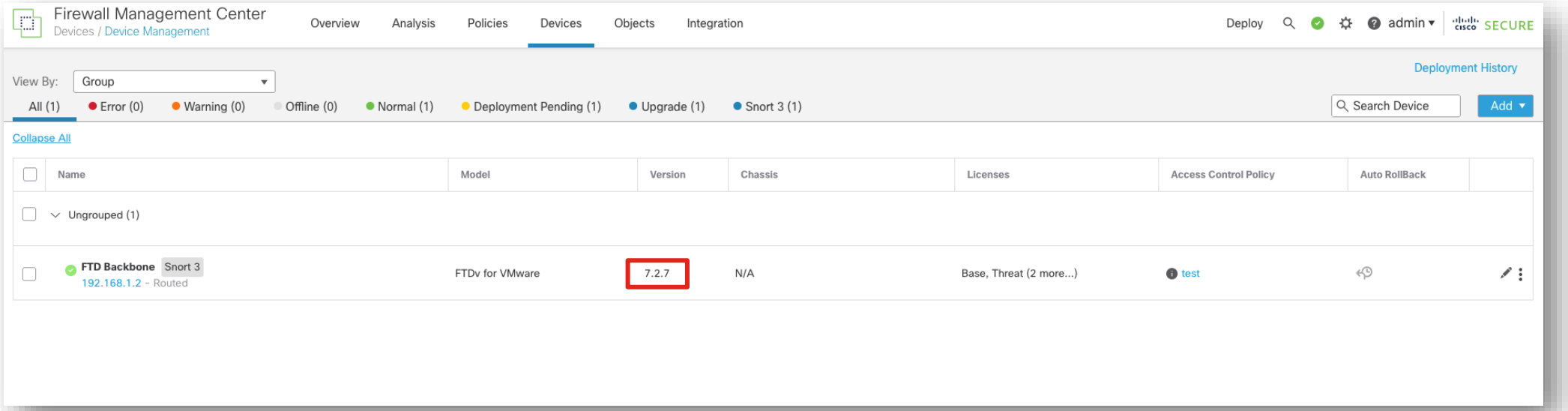
# Actualización de FTD

1. Dirigete a Devices > Device Management para validar la nueva versión del FTD
2. Realiza las implementaciones de configuración pendientes



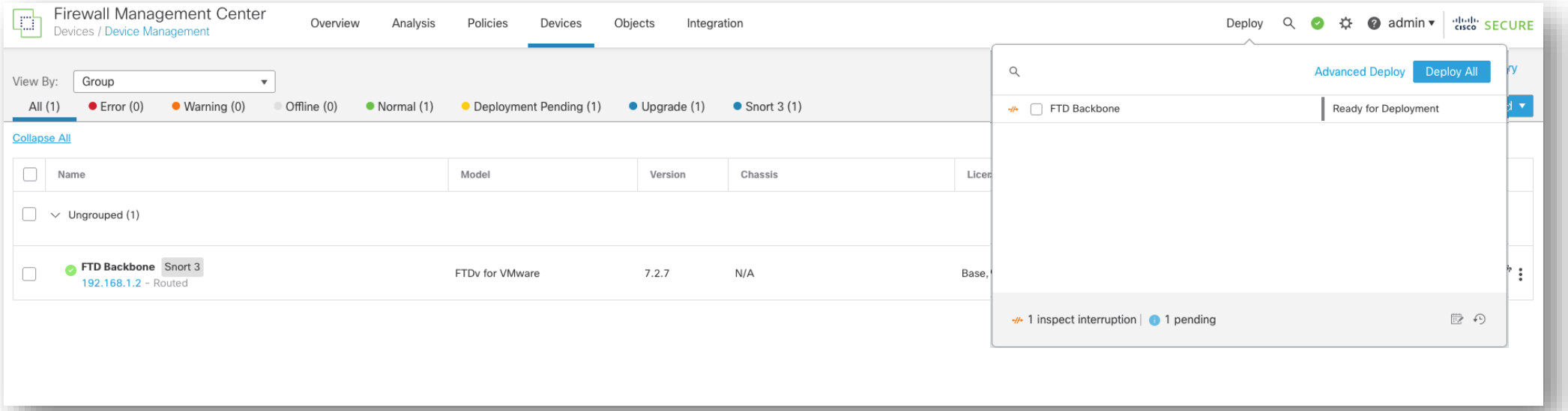
# Actualización de FTD

1. Dirigete a Devices > Device Management para validar la nueva versión del FTD
2. Realiza las implementaciones de configuración pendientes



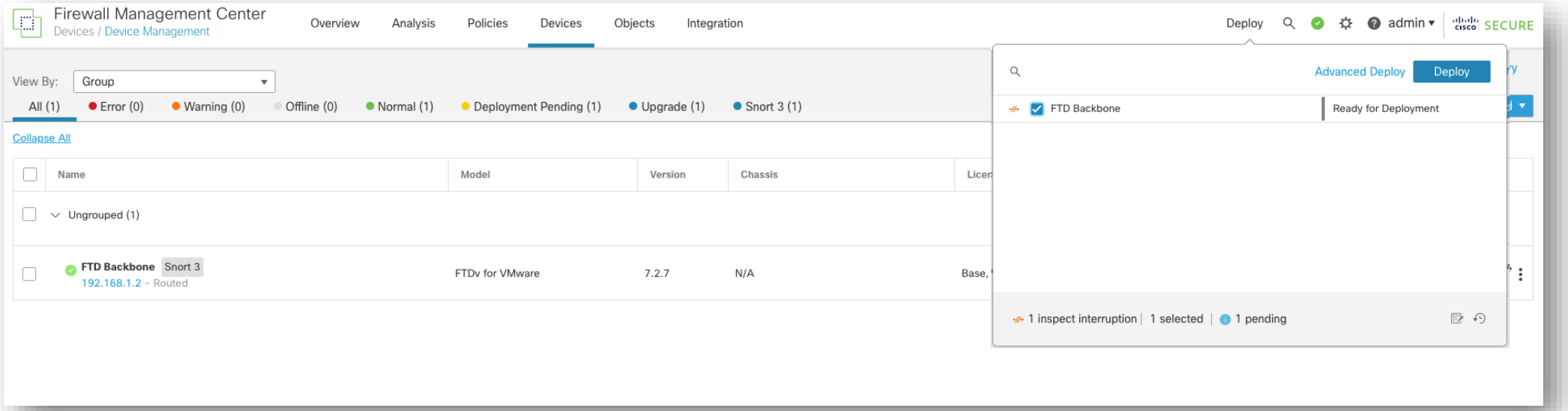
# Actualización de FTD

1. Dirigete a Devices > Device Management para validar la nueva versión del FTD
2. Realiza las implementaciones de configuración pendientes



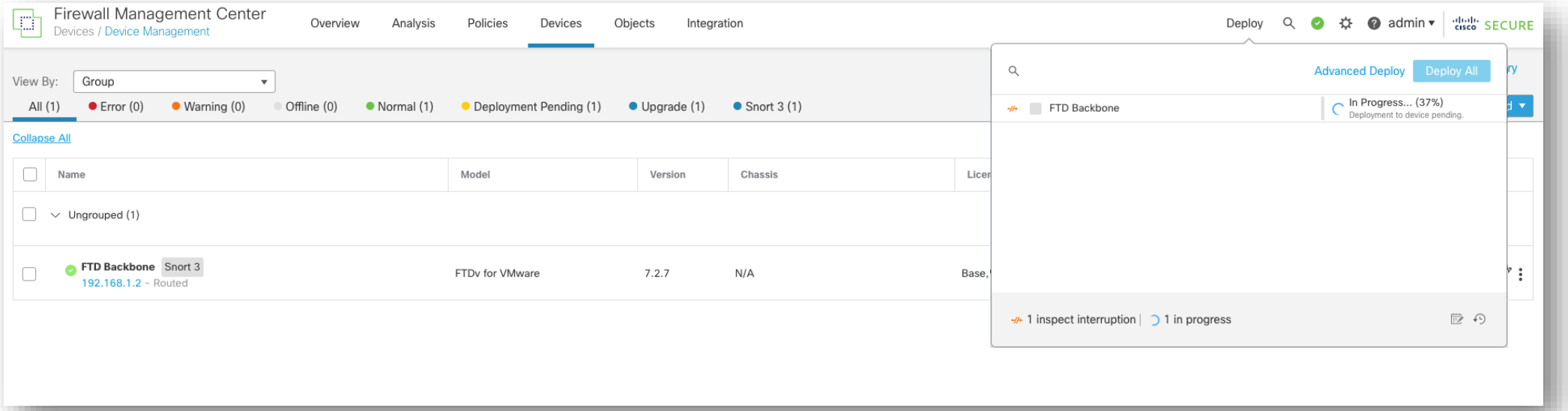
# Actualización de FTD

1. Dirigete a Devices > Device Management para validar la nueva versión del FTD
2. Realiza las implementaciones de configuración pendientes



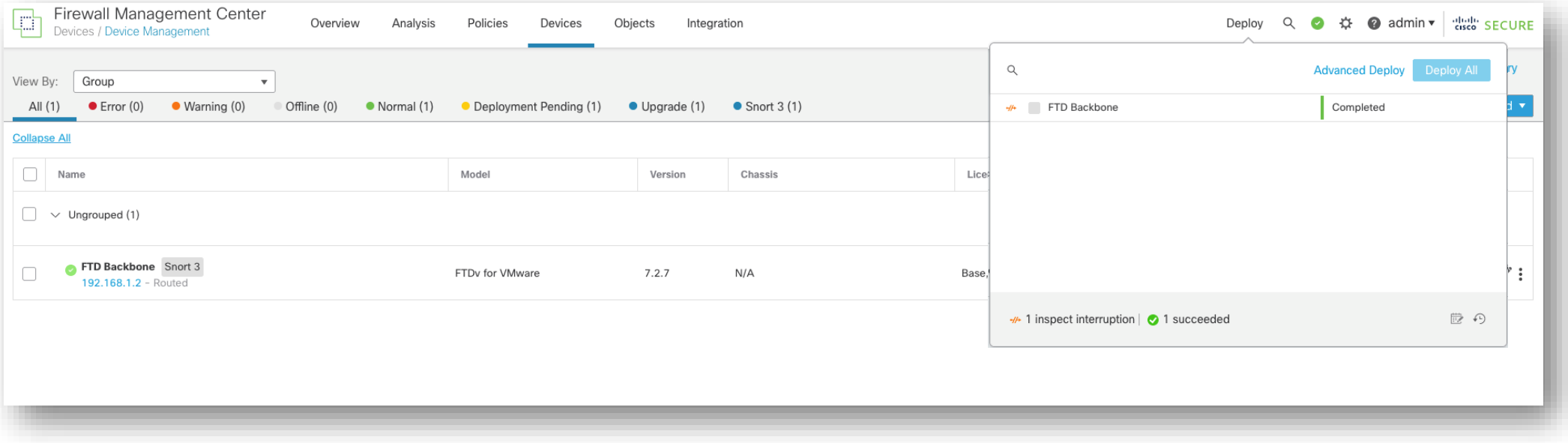
# Actualización de FTD

1. Dirigete a Devices > Device Management para validar la nueva versión del FTD
2. Realiza las implementaciones de configuración pendientes



# Actualización de FTD

1. Dirígete a Devices > Device Management para validar la nueva versión del FTD
2. Realiza las implementaciones de configuración pendientes



# Plan de Contingencia

## Cosas que debes hacer

- Recolectar los logs de la falla del upgrade
- En caso de urgencia reinstalar y recuperar funcionalidad con backup
- Levantar un caso con TAC

## Cosas que no debes hacer

- Apagar o reiniciar el equipo
- Reinstalar sin resolver el problema previo
- Intentar instalar una versión distinta
- Eliminar firewalls del FMC

# Guías y otras referencias (1)

## Upgrade FTD via FDM

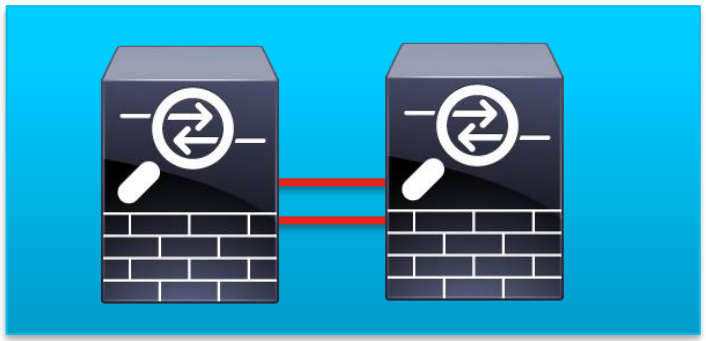
### Upgrade Standalone FTD

Use this procedure to upgrade a standalone FTD device. If you need to update FXOS, do that first. To upgrade high availability threat defense, see Upgrade High Availability FTD.

⚠ **Caution** Traffic is dropped while you upgrade. Even if the system appears inactive or unresponsive, do not manually reboot or shut down during upgrade; you could place the system in an unusable state and require a reimage. You can manually cancel failed or in-progress major and maintenance upgrades, and retry failed upgrades. If you continue to have issues, contact Cisco TAC.

For details on these and other issues you may encounter during upgrade, see Troubleshooting Threat Defense Upgrades.

**Before you begin**



## Upgrade FTD HA via FMC

**Introduction**

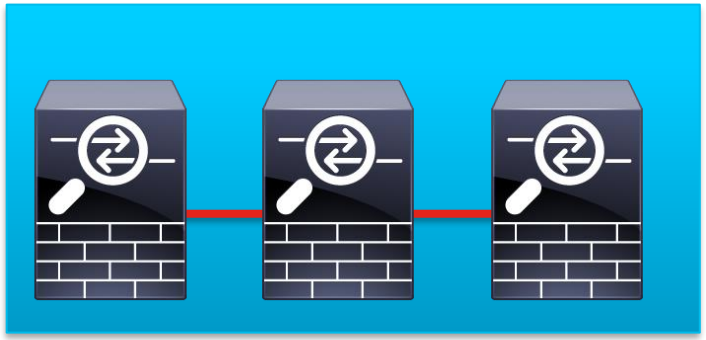
This document describes the upgrade process for a Cisco Secure Firewall Threat Defense in High Availability managed by a Firewall Management Center.

**Prerequisites**

**Requirements**

Cisco recommends you have knowledge of these topics:

- High Availability (HA) concepts and configuration
- Secure Firewall Management Center (FMC) configuration
- Cisco Secure Firewall Threat Defense (FTD) configuration



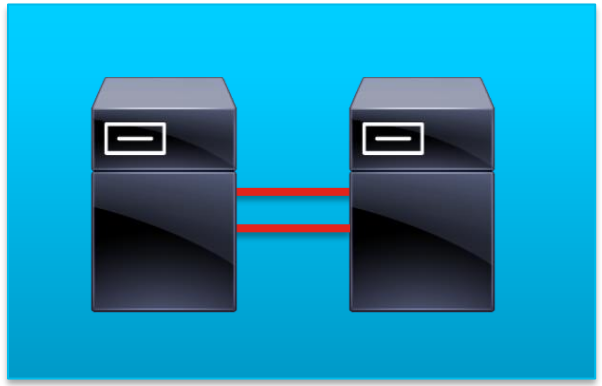
## Upgrade FTD Cluster via FMC

### Upgrade Threat Defense with System > Updates (Enable Revert)

Use this procedure to upgrade threat defense using the System Updates page.

⚠ **Caution** Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive Upgrades.

# Guías y otras referencias (2)



## Upgrade FMC HA

**Introduction**

This document describes the steps to upgrade an environment of Firewall Management Center (FMC) in High Availability (HA).

**Requirements**

Cisco recommends you have knowledge of these topics:

- High Availability concepts
- FMC configuration

## Compatibility Guide

**Cisco Secure Firewall Threat Defense Compatibility Guide**

This guide provides software and hardware compatibility for Cisco Secure Firewall Threat Defense. For related compatibility guides, see the following table.

**Note** Not all software versions, especially patches, apply to all platforms. A quick way to tell if a version is supported is that its upgrade/installation packages are posted on the Cisco Support & Download site. If the site is "missing" an upgrade or installation package, that version is not supported. You can also check the release notes and End-of-Life Announcements. If you feel a version is missing in error, contact Cisco TAC.

# Guías y otras referencias (3)


[ArcaneDoor Vulnerability]

Cisco Event Response: Attacks Against Cisco Firewall Platforms

## Summary

In early 2024, the Cisco Product Security Incident Response Team (PSIRT) became aware of attacks that were targeting certain devices that were running Cisco Adaptive Security Appliance (ASA) Software or Cisco Firepower Threat Defense (FTD) Software to implant malware, execute commands, and potentially exfiltrate data from the compromised devices.

Active poll

0

Join at

**slido.com**

**#4114 200**

Passcode:

**u9jada**

**¿Cuál es la mejor manera de hacer un upgrade en un Cisco FTD?**

a) Realizar backup, agendar ventana de mantenimiento, correr readiness check, instalar upgrade

0%

b) Correr readiness check, realizar backup, agendar ventana de mantenimiento, instalar upgrade

0%

c) Agendar ventana de mantenimiento, correr readiness check, Instalar upgrade y realizar backup

0%

# Q&A

# ¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar ¡Nuestros expertos aún pueden ayudarlo!

**Participe en el foro Ask Me Anything (AMA) antes del viernes 17 de mayo de 2024**

https://bit.ly/CL2ama-may24

# Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

**¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!**

Al término de esta sesión, se abrirá una encuesta en su navegador.

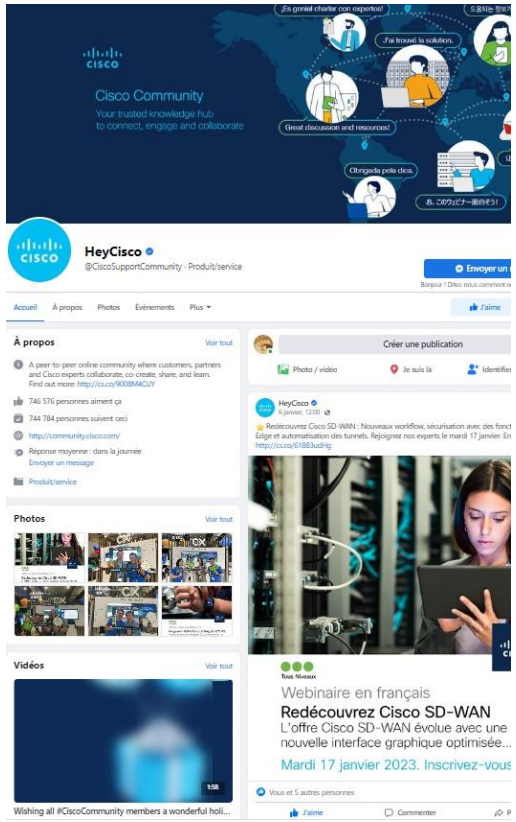
# Nuestras Redes Sociales

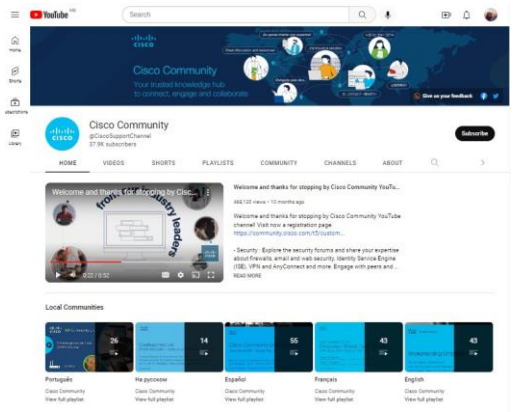
LinkedIn
[Cisco Community]

Twitter
[@CiscoCommunity]

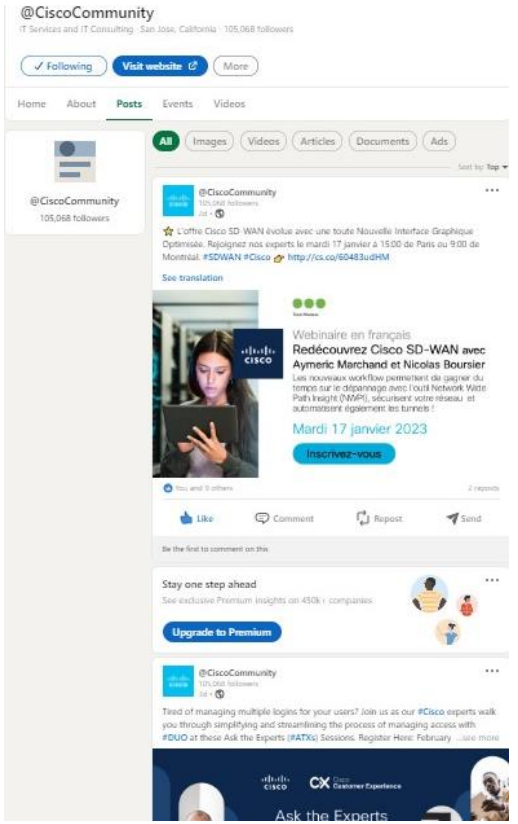
YouTube
[CiscoCommunity]

Facebook
[CiscoCommunity]








The bridge to possible