



# 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.

Aceptar como solución

## 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!

👍 0 Útil

# 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**

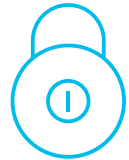


# Agenda



## 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.

<b>Cisco ISE Release</b>	<b>RHEL Release</b>
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-3.0PR-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. <a href="#">ise-urtbundle-3.2.0.542a-1.0.0.SPA.x86_64.tar.gz</a> <a href="#">Advisories</a>	27-Oct-2022	962.95 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>



# Validaciones antes de actualizar ISE

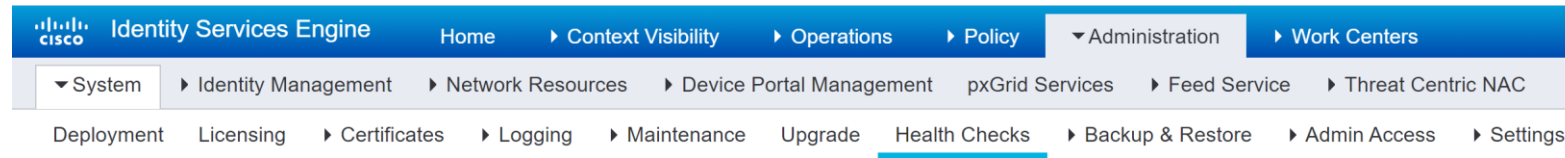
- Posteriormente este URT se debe guardar en un repositorio accesible desde ISE, y para ejecutar la verificación URT se usa el comando:

```
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.

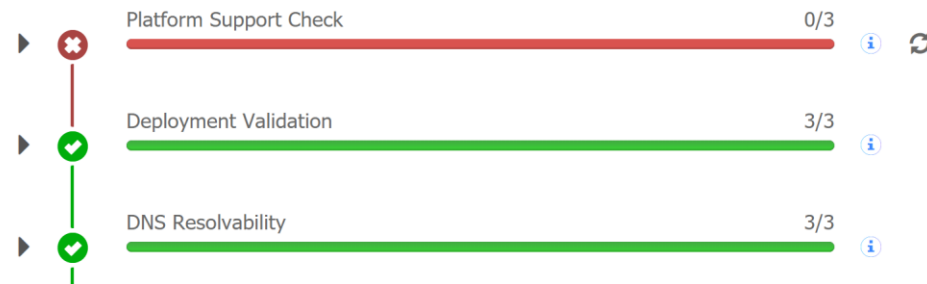
# Validaciones antes de actualizar ISE

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



## Health Checks

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



# 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:

Administration · System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore

Welcome Checklist Select Nodes Prepare to Upgrade Up

Estimated time of Upgrade process: 0hr 0min

Task	Progress	Status
Repository Validation	3/3	Completed
Bundle Download	2/2	Completed
Memory Check	3/3	Completed
PAN Failover Validation	1/1	Completed
Scheduled Backup Check	1/1	Completed



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

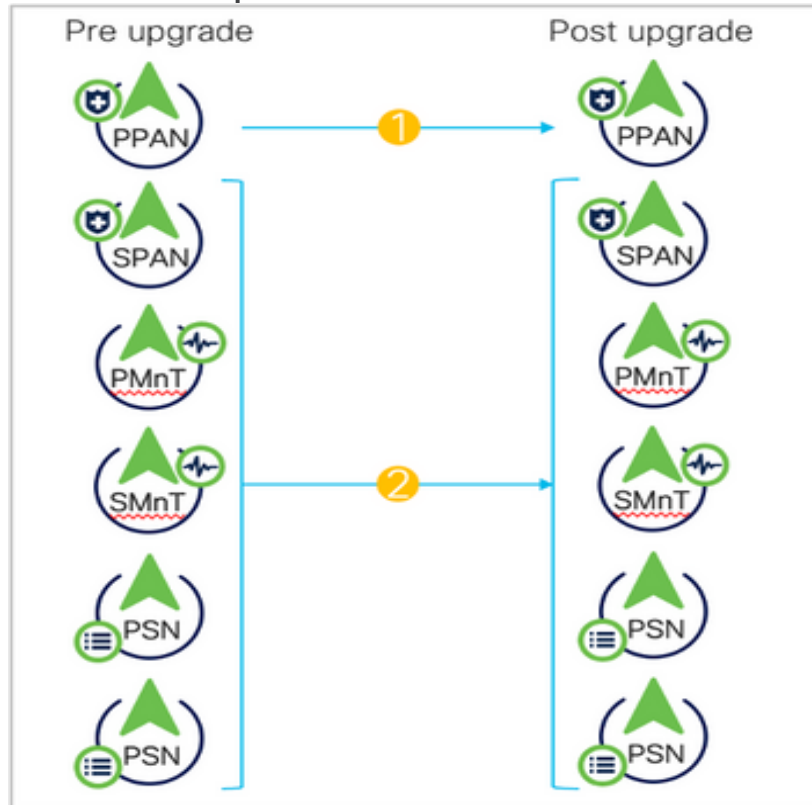
## Backup and restore

- 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 actualización 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

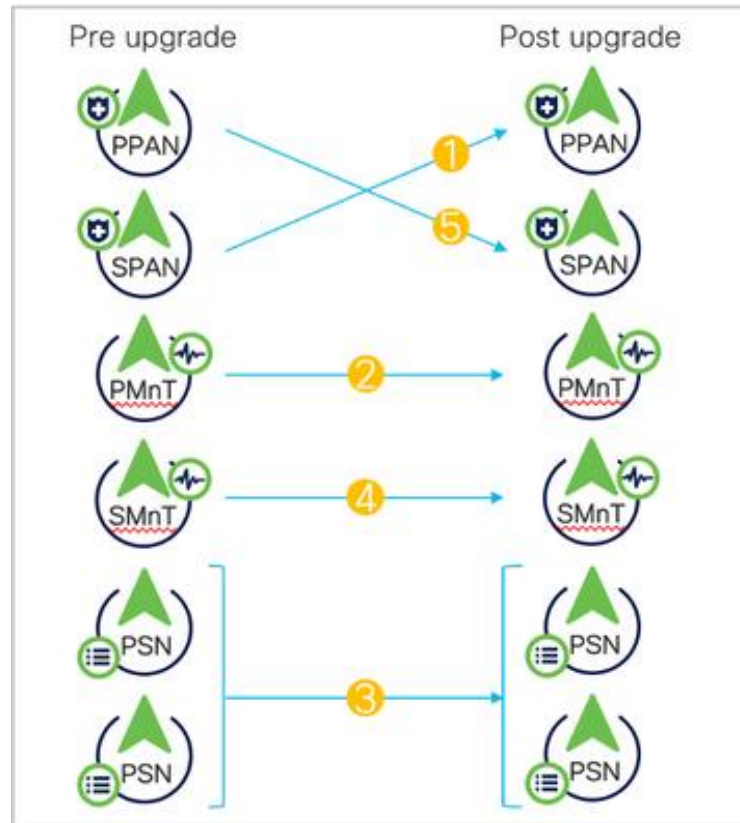
El método de Full Upgrade – es ideal cuando puede existir una ventana de mantenimiento en la cual no importe que los servicios estén fuera, el método full upgrade es el más rápido de todos ya que actualiza el nodo primario de administración y posterior a eso se actualizan todos los demás nodos al mismo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



Products & Services

Support

How to Buy

Training & Events

Partners



## 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 bundle for upgrading ISE version 2.7, 3.0,3.1 to 3.2. This is a signed bundle for image integrity. <a href="#">ise-upgradebundle-2.7.x-3.1.x-to-3.2.0.542b.SPA.x86_64.tar.gz</a> <a href="#">Advisories</a>	09-May-2023	15250.36 MB	<a href="#">↓</a>



# ¿Dónde empiezo la actualización?

## Upgrade Selection

Select the upgrade process you want to carry out:

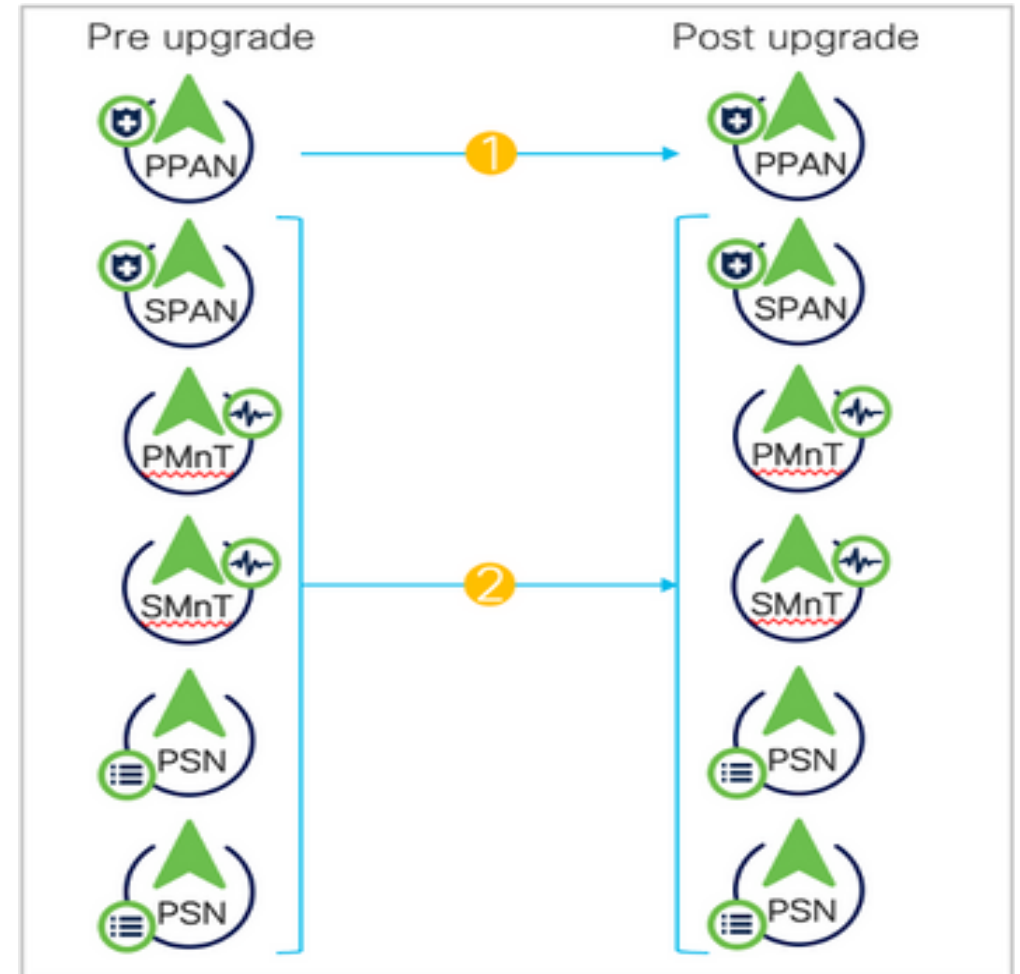
1. Full upgrade is a multi-step process that enables a complete upgrade of your Cisco ISE Deployment. This will upgrade all nodes in parallel so services will be down during the upgrade with this option. This is intended to upgrade the deployment as quickly as possible.
2. Split upgrade is a multi-step 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.

Full Upgrade

Split Upgrade

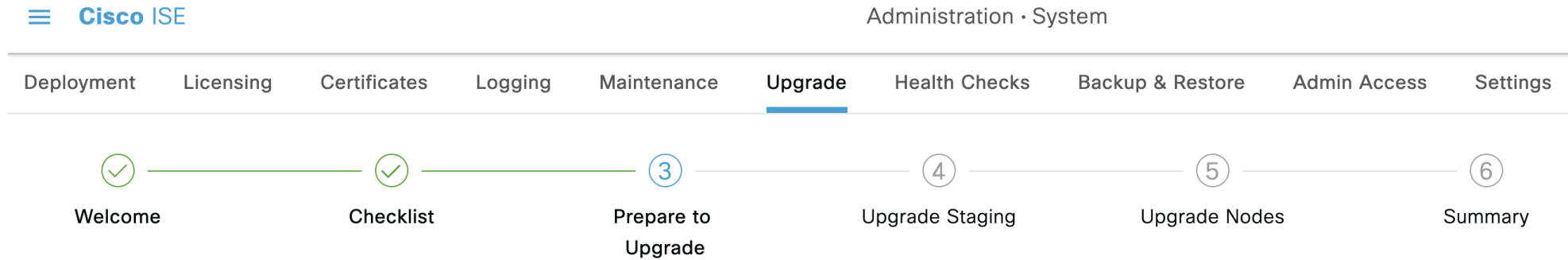
Start Upgrade

# Ejemplo de Full Upgrade





# Ejemplo – Full Upgrade 1/5



## Prepare to Upgrade

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

Bundle Download, Patch bundle Download, Platform Check, Configuration data upgrade and disk space check are valid for 12 hours. Other prechecks get expired after 3 hours and can be revalidated using refresh failed checks button or individual refresh button.

Repository\*  
local

Bundle\*  
ise-upgradebundle-3.0.x-3.2.x-to-...

Patch  
None

Start Preparation

# Ejemplo – Full Upgrade 2/5

**Cisco ISE** Administration · System

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

Progress: Welcome (✓) | Checklist (✓) | **Prepare to Upgrade (3)** | Upgrade Staging (4) | Upgrade Nodes (5) | Summary (6)

[Download Report](#) [Refresh Failed Checks](#)

Estimated time of Upgrade process: 0hr 0min

Task	Progress	Status	Info
Repository Validation	3/3	Success	Info
Bundle Download	3/3	Success	Info
Memory Check	3/3	Success	Info
PAN Failover Validation	1/1	Success	Info
Scheduled Backup Check	1/1	Warning	Info, Refresh
Config Backup Check	0/1	Failure	Info, Refresh
Configuration Data Upgrade	0/1	Warning	Info

[Exit Wizard](#) [Back](#) [Start Staging](#)



# Ejemplo – Full Upgrade 3/5

Administration · System

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

Welcome Checklist Prepare to Upgrade Upgrade Staging Upgrade Nodes Summary

## Upgrade Staging

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

Refresh Failed Nodes Cancel Staging

- ise-demo-1.aaamex.com
- ise-demo-2.aaamex.com
- ise-demo-3.aaamex.com

Exit Wizard Back Next

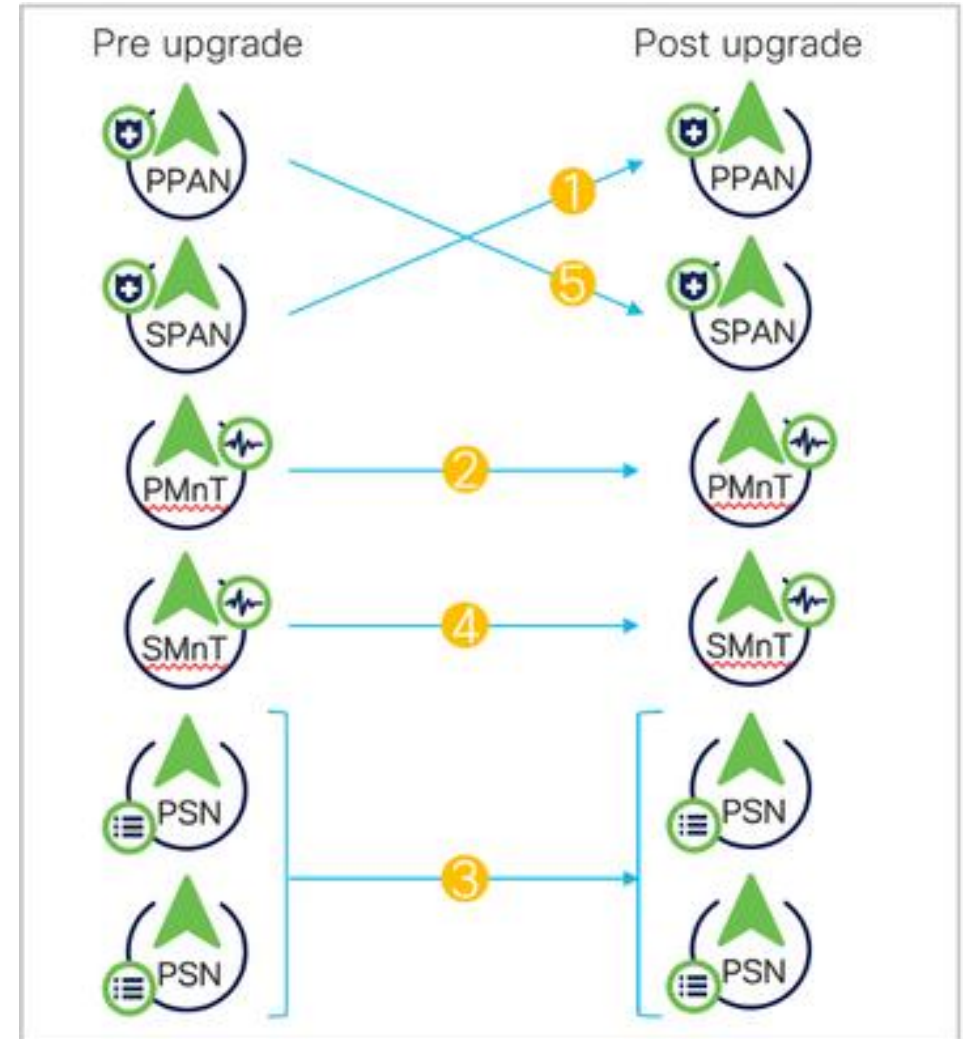
# Ejemplo – Full Upgrade 4/5

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration · System'. Below this, there are tabs for 'Deployment', 'Licensing', 'Certificates', and 'Logging'. A progress indicator shows 'Welcome' and 'Checklist' as completed steps. 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. Estimated time of Upgrade process: 5hr 28min'. A 'Start' button is visible. A 'Warning' dialog box is overlaid in the center, with the text: 'Warning: Initiating ISE Upgrade will cause a downtime in ISE Services. Do you want to continue with Upgrade?'. The dialog has 'Cancel' and 'Yes' buttons. At the bottom of the console, there are 'Exit Wizard', 'Back', and 'Next' buttons.

# Ejemplo – Full Upgrade 5/5

The screenshot shows the Cisco ISE Administration System interface during a full upgrade. The breadcrumb trail is Administration > System. The navigation menu includes Deployment, Licensing, Certificates, Logging, Maintenance, Admin Access, and Settings. The main content area shows a progress bar with three steps: Welcome, Checklist, and Prepare to Upgrade, all marked with green checkmarks. A modal dialog box titled "Information" is displayed in the center, containing the text "The system is about to upgrade. Logging out." and an "OK" button. Below the progress bar, the section "Upgrading Nodes" provides instructions on monitoring the upgrade process and lists three nodes: ise-demo-1.aaamex.com, ise-demo-2.aaamex.com, and ise-demo-3.aaamex.com, each with a progress indicator. The estimated time of the upgrade process is 5hr 28min. At the bottom, there are "Exit Wizard", "Back", and "Next" buttons.

# Ejemplo de Legacy Split Upgrade



# Ejemplo – Legacy Split Upgrade 1/7

ⓘ Read only mode. Click the Upgrade tab to proceed.

Node Group - Host Name	Persona	Version - Repository	Status
ise-demo-5.aaamex.com	Admin <b>SECONDARY</b> Monitor <b>PRIMARY</b> Policy service	3.2.0.542 - Patch 1,2	● Active
ise-demo-6.aaamex.com	Policy service	3.2.0.542 - Patch 1,2	● Active
ise-demo-4.aaamex.com	Admin <b>PRIMARY</b> Monitor <b>SECONDARY</b> Policy service	3.2.0.542 - Patch 1,2	● Active

# Ejemplo – Legacy Split Upgrade 2/7

☰ Cisco ISE Administration · System

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

① ————— ② ————— ③  
Review Checklist Download Bundle Upgrade Node(s)  
to Node(s)

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

**BACKUP ISE**

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

**SOFTWARE**

- Review the ISE Upgrade Guide and Release Notes for upgrade information (under <http://cisco.com/go/ise>)
- Confirm valid ISE upgrade paths. Ensure that a repository is available to store the ISE upgrade bundle (see [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 (see [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.
- We recommend that you enable PLR on your secondary PAN as well to avoid any Cisco ISE service disruption. If your secondary PAN does not have PLR enabled, you might have service disruption after upgrade process.

**Health Checks**

- Be sure that all your software is working stable, check your system on page ([Administration > System > Health Checks](#))

I have reviewed the checklist

**Continue**



# Ejemplo – Legacy Split Upgrade 3/7

**Confirm Repository and Bundle**

**Selected Repository**  
local [Change Repository](#)

**Selected Bundle**  
ise-upgradebundle-3.0.x-3.2.x-to-3.3.0.427.SPA.x86\_64.tar.gz

[Back](#) [Begin Download](#)

<input type="checkbox"/>	Node Group - Host Name	Persona	Version - Repository	Status
<input checked="" type="checkbox"/>	ise-demo-5.aamex.com	Admin <b>SECONDARY</b> Monitor <b>PRIMARY</b> Policy service	3.2.0.542 - Patch 1,2	● Active
<input type="checkbox"/>	ise-demo-6.aamex.com	Policy service	3.2.0.542 - Patch 1,2	● Active
<input type="checkbox"/>	ise-demo-4.aamex.com	Admin <b>PRIMARY</b> Monitor <b>SECONDARY</b> Policy service	3.2.0.542 - Patch 1,2	● Active

# Ejemplo – Legacy Split Upgrade 4/7

Cisco ISE
Administration · System

---

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

1

2

3

Review Checklist

Download Bundle to Node(s)

Upgrade Node(s)

Download

Terminate

Note: The bundle must be present in the repository.

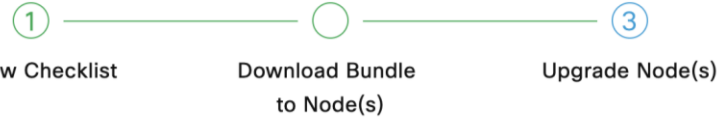
From the repository, download the bundle to one or more nodes simultaneously. To proceed with upgrade, download the bundle to the Secondary Administration and Primary Monitoring Nodes first.

<input type="checkbox"/>	Node Group - Host Name	Persona	Version - Repository	Status
<input checked="" type="checkbox"/>	ise-demo-5.aaamex.com	Admin <span style="font-weight: normal;">SECONDARY</span> Monitor <span style="border: 1px solid #0070C0; border-radius: 3px; padding: 0 2px;">PRIMARY</span> Policy service	3.2.0.542 - Patch 1,2	<span style="color: green;">■</span> Ready for upgrade
<input type="checkbox"/>	ise-demo-6.aaamex.com	Policy service	3.2.0.542 - Patch 1,2	<span style="color: green;">●</span> Active
<input type="checkbox"/>	ise-demo-4.aaamex.com	Admin <span style="border: 1px solid #0070C0; border-radius: 3px; padding: 0 2px;">PRIMARY</span> Monitor <span style="font-weight: normal;">SECONDARY</span> Policy service	3.2.0.542 - Patch 1,2	<span style="color: green;">●</span> Active

Back

Continue

# Ejemplo – Legacy Split Upgrade 5/7



Deployment (3.2.0.542 )

	Node Group - Host Na...	Persona
<input checked="" type="checkbox"/>	ise-demo-5.aaamex.com	Admin <b>SECONDARY</b> Monitor <b>PRIMARY</b> Policy service
<input type="checkbox"/>	ise-demo-6.aaamex.com <b>is not ready for upgrade</b>	Policy service
<input type="checkbox"/>	ise-demo-4.aaamex.com <b>is not ready for upgrade</b>	Admin <b>PRIMARY</b> Monitor <b>SECONDARY</b> Policy service



New Deployment Upgrade (3.3.0.427)

Total estimated time: **240 mins**

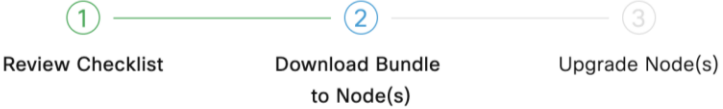
Seque...	Node Group - Host Na...	Persona	Status
1	ise-demo-5.aaamex.com	Admin <b>PRIMARY</b> Monitor <b>PRIMARY</b> Policy service	0%  Upgrading... ⓘ
2	Select nodes for sequence 2		

ⓘ Continue with the next node on upgrade failure (applicable for Policy Service Nodes only)

Back

Upgrade

# Ejemplo – Legacy Split Upgrade 6/7



Download

Terminate

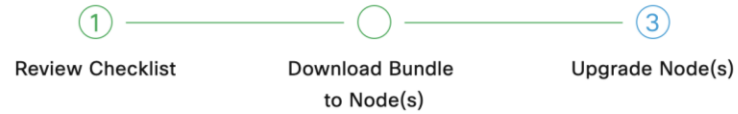
Note: The bundle must be present in the repository.  
 From the repository, download the bundle to one or more nodes simultaneously. To proceed with upgrade, download the bundle to the Secondary Administration and Primary Monitoring Nodes first.

<input type="checkbox"/>	Node Group - Host Name	Persona	Version - Repository	Status
<input type="checkbox"/>	ise-demo-5.aaamex.com	Admin <b>SECONDARY</b> Monitor <b>PRIMARY</b> Policy service	3.2.0.542 - Patch 1,2  local	5%  Upgrading... ⓘ
<input type="checkbox"/>	ise-demo-6.aaamex.com	Policy service	3.2.0.542 - Patch 1,2  local	Ready for upgrade ⓘ
<input type="checkbox"/>	ise-demo-4.aaamex.com	Admin <b>PRIMARY</b> Monitor <b>SECONDARY</b> Policy service	3.2.0.542 - Patch 1,2  local	Ready for upgrade ⓘ

Back

Continue

# Ejemplo – Legacy Split Upgrade 7/7



Deployment (3.2.0.542)

	Node Group - Host Na...	Persona
<input checked="" type="checkbox"/>	ise-demo-5.aaamex.com	Admin <b>SECONDARY</b> Monitor <b>PRIMARY</b> Policy service
<input checked="" type="checkbox"/>	ise-demo-6.aaamex.com	Policy service
<input checked="" type="checkbox"/>	ise-demo-4.aaamex.com	Admin <b>PRIMARY</b> Monitor <b>SECONDARY</b> Policy service



New Deployment Upgrade (3.3.0.427)

Total estimated time: **480 mins**

Seque...	Node Group - Host Na...	Persona	Status
1	ise-demo-5.aaamex.com	Admin <b>PRIMARY</b> Monitor <b>PRIMARY</b> Policy service	Upgrade complete ⓘ
2	ise-demo-6.aaamex.com	Policy service	240 min. est. time
3	ise-demo-4.aaamex.com	Admin <b>SECONDARY</b> Monitor <b>SECONDARY</b> Policy service	240 min. est. time ❌
4	Select nodes for sequence 4		

Continue with the next node on upgrade failure (applicable for Policy Service Nodes only)

# Ejemplo de New Split Upgrade



# Ejemplo – New Split Upgrade 1/9

Cisco ISE Administration · System

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

Progress: Welcome (✓) Checklist (✓) **Select Nodes (3)** Prepare to Upgrade (4) Upgrade Staging (5) Upgrade Nodes (6) Summary (7)

## Select Nodes (Iteration 1)

Select Nodes for Split Upgrade

P-PAN cannot be selected until all the other nodes are upgraded or selected for upgrade.

S-PAN will be selected by default in first iteration of upgrade.

Hostname	Personas	Role(s)
<input checked="" type="checkbox"/> ise-demo-8.aaamex.com	Secondary Administration,Secondary Monit...	SECONDARY
<input type="checkbox"/> ise-demo-9.aaamex.com	Policy Service	SECONDARY
<input type="checkbox"/> ise-demo-7.aaamex.com	Primary Administration,Primary Monitoring,P...	PRIMARY

[Exit Wizard](#)

[Back](#)

[Next](#)

# Ejemplo – New Split Upgrade 2/9

**Cisco ISE** Administration · System

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

Welcome Checklist Select Nodes **Prepare to Upgrade** Upgrade Staging Upgrade Nodes Summary

patch file. Then, click Start Preparation.  
ISE Services will continue to run while Prechecks are executed. Report will be valid for 12 hours during which Upgrade can be triggered. Proceeding to Upgrade Staging (by clicking Start Staging) step will not cause suspension of any ISE Services. Precheck will continue execution in the background even if ISE UI is closed.  
Bundle Download, Patch bundle Download, Platform Check, Configuration data upgrade and disk space check are valid for 12 hours. Other prechecks get expired after 3 hours and can be revalidated using refresh failed checks button or individual refresh button.

Repository\*  
local

Bundle\*  
ise-upgradebundle-3.0.x-3.2.x-to-...

Patch  
None

[Download Report](#) [Refresh Failed Checks](#)

Estimated time of Upgrade process: 0hr 0min

[Exit Wizard](#)

**Cisco ISE** Administration · System

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

Welcome Checklist Select Nodes **Prepare to Upgrade** Upgrade Staging Upgrade Nodes Summary

Estimated time of Upgrade process: 0hr 0min

Repository Validation	3/3	0
Bundle Download	2/2	0
Memory Check	3/3	0
PAN Failover Validation	1/1	0
Scheduled Backup Check	1/1	0
Config Backup Check	1/1	0
Configuration Data Up	0/1	21%
Admin Certificate Check in Trusted store	1/1	0
Disk Corruption checks	3/3	0

[Exit Wizard](#) [Back](#) [Start Staging](#)



# Ejemplo – New Split Upgrade 3/9

**Cisco ISE** Administration • System

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

Welcome Checklist Select Nodes Prepare to Upgrade **Upgrade Staging** Upgrade Nodes Summary

## Upgrade Staging

The upgraded data is 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.

[Refresh Failed Nodes](#) [Cancel Staging](#)

ise-demo-8.aaamex.com

Operations:  
Config Files Backup  
Copy Upgrade DB dump

[Exit Wizard](#) [Back](#) [Next](#)

# Ejemplo – New Split Upgrade 4/9

**Cisco ISE** Administration · System

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

Welcome Checklist Select Nodes Prepare to Upgrade Upgrade Staging **Upgrade Nodes** Summary

## Upgrading Nodes (Iteration 1)

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.

Nodes selected for current iteration are: ise-demo-8.aaamex.com

Estimated time of Upgrade process: **2hr 48min**

Overall Upgrade Progress 2hr 35min

ise-demo-8.aaamex.com

STEP 3 OF 8 - IMPORTING CONFIG DB DUMP

[Exit Wizard](#) [Back](#) [Next](#)

# Ejemplo – New Split Upgrade 5/9

**Cisco ISE** Administration · System

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

Progress: Welcome Checklist Select Nodes Prepare to Upgrade Upgrade Staging Upgrade Nodes Summary (7)

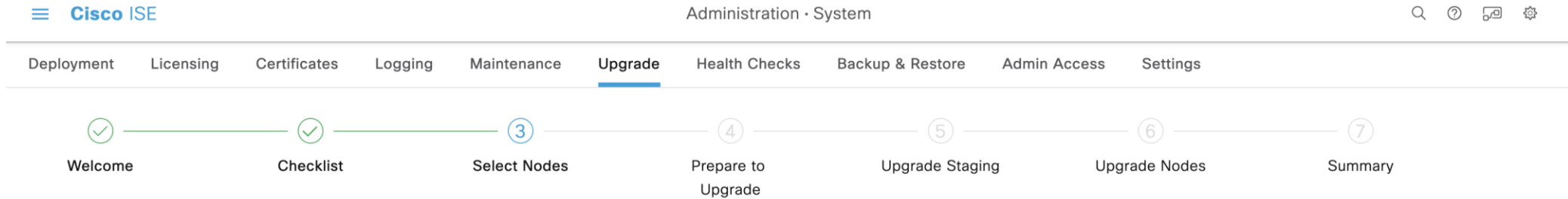
## Summary (Iteration 1)

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

- Selected Nodes [Download Report](#)  
Selected Nodes: ise-demo-8.aaamex.com
- Prepare to Upgrade [Download Report](#)  
Repository: local  
Bundle: ise-upgradebundle-3.0.x-3.2.x-to-3.3.0.427.SPA.x86\_64.tar.gz  
Patch:
- Upgrade Report [Download Report](#)  
Upgraded Nodes: ise-demo-8.aaamex.com

[Exit Wizard](#) [Back](#) [Continue](#)

# Ejemplo – New Split Upgrade 6/9



## Select Nodes (Iteration 2)

Select Nodes for Split Upgrade

P-PAN cannot be selected until all the other nodes are upgraded or selected for upgrade.

S-PAN will be selected by default in first iteration of upgrade.

Hostname	Personas	Role(s)
<input type="checkbox"/> ise-demo-8.aaamex.com	Secondary Administration,Secondary Monit...	SECONDARY
<input checked="" type="checkbox"/> ise-demo-9.aaamex.com	Policy Service	SECONDARY
<input checked="" type="checkbox"/> ise-demo-7.aaamex.com	Primary Administration,Primary Monitoring,P...	PRIMARY

[Exit Wizard](#)

[Back](#)

[Next](#)

# Ejemplo – New Split Upgrade 7/9

**Cisco ISE** Administration • System

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

Welcome Checklist Select Nodes Prepare to Upgrade Upgrade Staging **Upgrade Nodes** Summary

Estimated time of Upgrade process: 3hr 45min

Overall Upgrade Progress 3hr 3min

ise-demo-7.aaamex.com  
Upgrade Queued

ise-demo-9.aaamex.com  
STEP 5 OF 8 - REBOOT

Exit Wizard Back Next



# Ejemplo – New Split Upgrade 8/9

The screenshot shows the Cisco Identity Services Engine Administration / System interface. The top navigation bar includes the Cisco logo, the text "Identity Services Engine", and "Administration / System". On the right side of the top bar are icons for search, home, help, notifications, and user profile. Below the top bar is a secondary navigation bar with tabs for Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The "Deployment" tab is selected. On the left side, there is a sidebar menu with icons for various functions, including a "Deployment" section with sub-items "Deployment" and "PAN Failover". The main content area is titled "Deployment Nodes" and contains a table with columns: Hostname, Personas, Role(s), Services, and Node Status. Above the table are action buttons: Edit, Register, Syncup, and Deregister. The table lists three nodes: ise-demo-7 (warning status), ise-demo-8 (success status), and ise-demo-9 (warning status). The table also shows "Selected 0 Total 3" and "All" filter options.

<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	ise-demo-7	Administration, Monitoring, Policy Service	SEC(A), PRI(M)	SESSION,PROFILER	⚠
<input type="checkbox"/>	ise-demo-8	Administration, Monitoring, Policy Service	PRI(A), SEC(M)	SESSION,PROFILER	✅
<input type="checkbox"/>	ise-demo-9	Policy Service		SESSION,PROFILER	⚠

# Ejemplo – New Split Upgrade 9/9

**Identity Services Engine Administration / System**

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

Progress: Welcome Checklist Select Nodes Prepare to Upgrade Upgrade Staging **Upgrade Nodes** Summary

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.

Iteration 1 [Download Report](#)  
Nodes selected for current iteration are: ise-demo-9.aaamex.com,ise-demo-7.aaamex.com

Estimated time of Upgrade process: **3hr 45min**

Overall Upgrade Progress  1hr 37min

**ise-demo-7.aaamex.com** ⓘ

STEP 7 OF 8 - POST OS UPGRADE COMPLETED

**ise-demo-9.aaamex.com** ⓘ

[Exit Wizard](#) [Back](#) [Next](#)



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, reimagine

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.

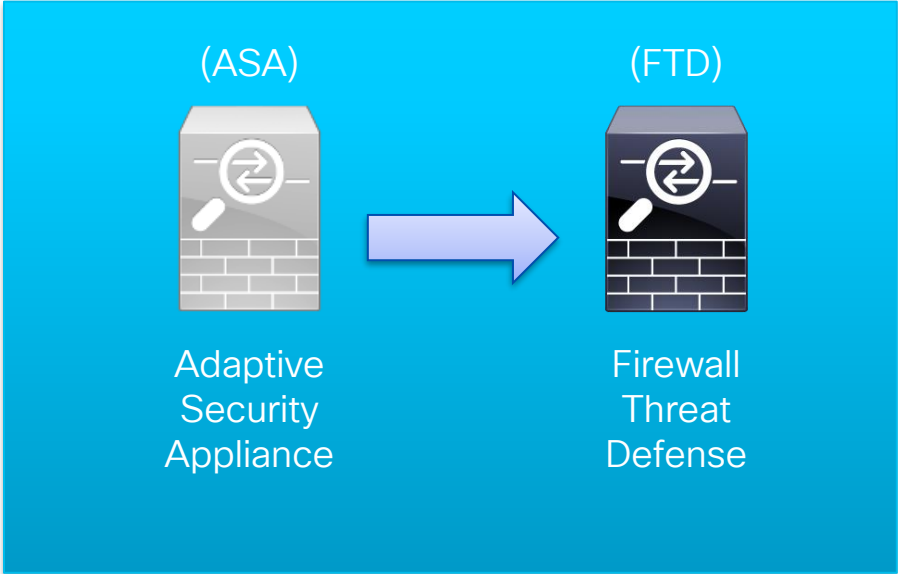
- ISE 3.0 ó anterior usa pxGrid versión 1 y 2.
- ISE 3.1 ó superior solo usa pxGrid versión 2.
- FMC 6.6 ó anterior solo usa pxGrid versión 1.
- FMC 6.7 ó superior solo usa pxGrid versión 2.

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.

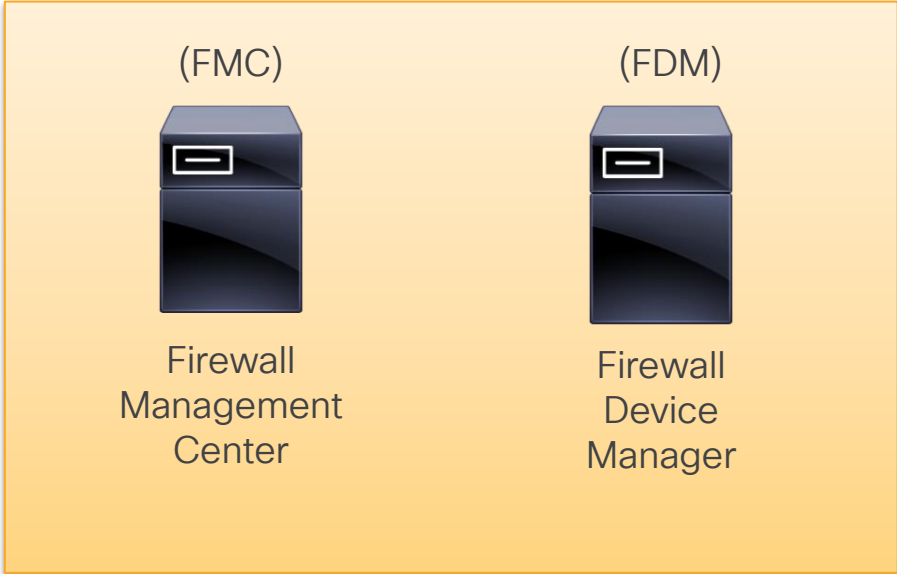
# Actualización de Secure Firewall

# Descripción general de FTD, FDM y FMC

## Cisco Firewalls



## Gestor del FTD

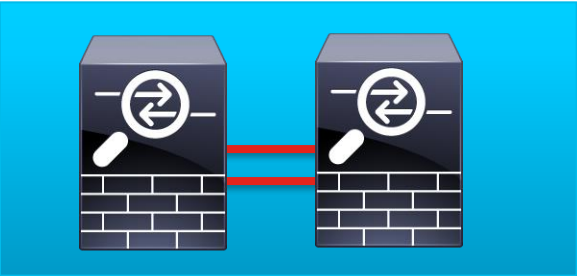


# Tipos de implementaciones en FTD y FMC

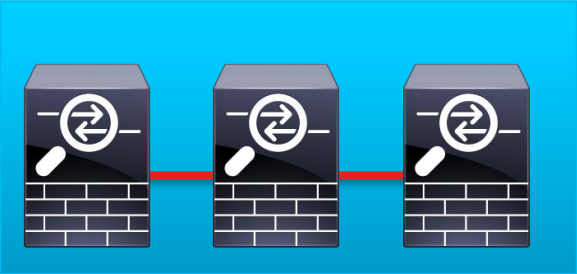
FTD



Standalone



High Availability

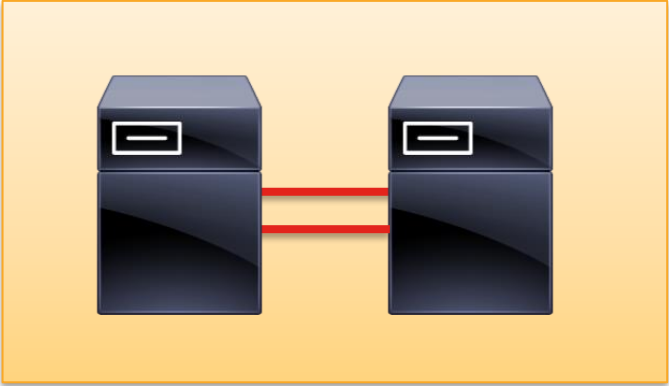


Cluster

FMC

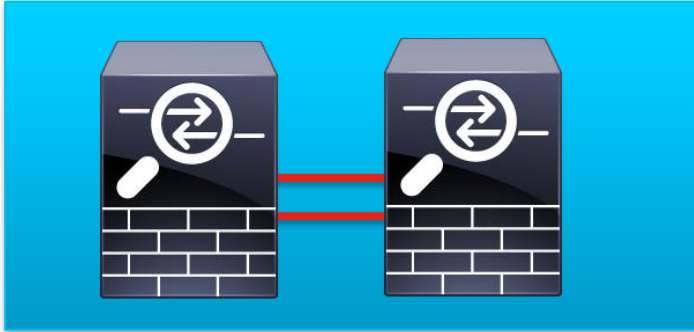


Standalone



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
```

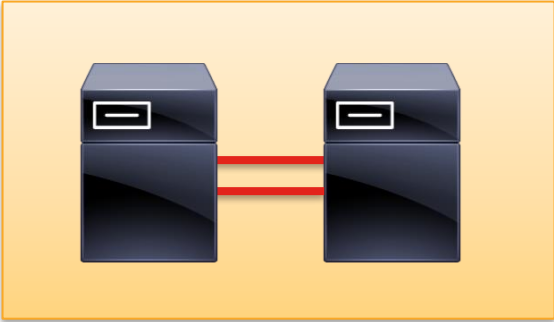
```
====Configuration State====
Sync Skipped
====Communication State====
Mac set
```



```
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



Firewall Management Center  
Integration / Other Integrations / High Availability

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ ? admin | **SECURE**

Peer Manager

Cloud Services Realms Identity Sources **High Availability** eStreamer Host Input Client Smart Software Manager On-Prem

Switch Peer Roles Break HA Pause Synchronization

Summary		System Status		
Status	🟢 Healthy	Local <b>Active - Primary</b> (10.18.19.31)	Remote <b>Standby - Secondary</b> (10.18.19.32)	
Synchronization	🟢 OK	Operating System	7.2.5	7.2.5
Active System	10.18.19.31	Software Version	7.2.5-208	7.2.5-208
Standby System	10.18.19.32	Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

# Prerrequisitos para una actualización

TAC Tip



Validar compatibilidad de actualización



Generar un respaldo de las configuraciones



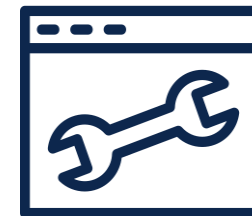
Descargar y subir el paquete de instalación al gestor del firewall



Ejecutar la verificación de preparación 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 (📦)

Firepower Management Center  
System / Updates / Product Updates

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy ✓ ⚙️ ? admin

Product Updates Rule Updates Geolocation Updates

Currently running software version: 6.6.5

Updates

Type	Version	Date	Release Notes	Reboot	
Cisco FTD Upgrade	7.2.7-500	Sat Apr 27 04:09:29 UTC 2024		Yes	
Cisco Secure FW Mgmt Center Upgrade	7.2.7-500	Sat Apr 27 03:56:22 UTC 2024		Yes	

Upload Update

Download updates

# Actualización de FMC

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

Firepower Management Center  
System / Updates / Upload Update

Deploy  admin

Product Updates Rule Updates Geolocation Updates

Currently running software version: 6.6.5

**Selected Update**

Type	Cisco Secure FW Mgmt Center Upgrade
Version	7.2.7-500
Date	Sat Apr 27 03:56:22 UTC 2024
Release Notes	
Reboot	Yes

By Group

Ungrouped(1 total)

firepower  
192.168.1.3 - Cisco Firepower Management Center for VMWare v6.6.5

**Health Policy**  
Initial\_Health\_Policy  
2021-05-21 14:10:56

# Actualización de FMC

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

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The main window is titled 'Firepower Management Center' and shows the 'Upload Update' page. The 'Selected Update' table is as follows:

Selected Update	
Type	Cisco Secure FW Mgmt Center Upgrade
Version	7.2.7-500
Date	Sat Apr 27 03:56:22 UTC 2024
Release Notes	
Reboot	Yes

Below the table, there is a list of devices with a checkbox for each. The 'firepower' device is selected. The modal window titled 'Readiness Check Status' shows the current version (6.6.5) and the update version (7.2.7-500). The status log indicates that the readiness check is being initiated for the device 'firepower'.

Health Policy Initial\_Health\_Policy 2021-05-21 14:10:56

Buttons: Cancel, Launch Readiness Check, Install

# Actualización de FMC

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

Firepower Management Center  
System / Updates / Upload Update

Deploy  admin ▼

Product Updates Rule Updates Geolocation Updates

Currently running software version: 6.6.5

**Selected Update**

Type	Cisco Secure FW Mgmt Center Upgrade
Version	7.2.7-500
Date	Sat Apr 27 03:56:22 UTC 2024
Release Notes	
Reboot	Yes

By Group ▼

Ungrouped(1 total)

<input checked="" type="checkbox"/> firepower 192.168.1.3 - Cisco Firepower Management Center for VMWare v6.6.5	<b>Health Policy</b> Initial_Health_Policy 2021-05-21 14:10:56 <input checked="" type="checkbox"/>
--	--

Cancel Launch Readiness Check Install

# Actualización de FMC

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

Firepower Management Center  
System / Updates / Upload Update

Deploy  admin

Product Updates Rule Updates Geolocation Updates

Currently running software version: **6.6.5**

**Selected Update**

Type	Cisco Secure FW Mgmt Center Upgrade
Version	7.2.7-500
Date	Sat Apr 27 03:56:22 UTC 2024
Release Notes	
Reboot	Yes

By Group

Ungrouped(1 total)

**firepower**  
192.168.1.3 - Cisco Firepower Management Center for VMWare v6.6.5

Deployments Health **Tasks**  Show Notifications

**20+** total | 0 waiting | **1** running | 0 retrying | **20+** success | 0 failures

**Local Install** 2m 23s

Readiness Check For version: 7.2.7-500  
[57%] Running script 000\_start/110\_DB\_integrity\_check.sh...

**Health Policy**  
Initial\_Health\_Policy  
2021-05-21 14:10:56

Cancel **Launch Readiness Check** Install

# Actualización de FMC

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

Firepower Management Center  
System / Updates / Upload Update

Deploy ✓ ⚙️ ? admin ▼

Product Updates Rule Updates Geolocation Updates

Currently running software version: **6.6.5**

**Selected Update**

Type	Cisco Secure FW Mgmt Center Upgrade
Version	7.2.7-500
Date	Sat Apr 27 03:56:22 UTC 2024
Release Notes	
Reboot	Yes

Deployments Health **Tasks** Show Notifications

20+ total | 0 waiting | 0 running | 0 retrying | 20+ success | 0 failures

Local Install 2m 56s ✕

Readiness Check For version: 7.2.7-500  
Readiness Check Completed Successfully

By Group ▼

Ungrouped(1 total)

firepower  
192.168.1.3 - Cisco Firepower Management Center for VMWare v6.6.5

**Health Policy**  
Initial\_Health\_Policy  
2021-05-21 14:10:56 ✓

Cancel Launch Readiness Check Install

# Actualización de FMC

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

Firepower Management Center  
System / Updates / Upload Update

Deploy  admin

Product Updates Rule Updates Geolocation Updates

Currently running software version: 6.6.5

Selected Update	
Type	Cisco Secure FW Mgmt Center Upgrade
Version	7.2.7-500
Date	Sat Apr 27 03:56:22 UTC 2024
Release Notes	
Reboot	Yes

**Task Notification**

[Message Center Tasks Tab](#) Your task Readiness Check For version: 7.2.7-500 (Local Install) succeeded at Tue May 7 00:07:21 2024  
Readiness Check Completed Successfully

By Group

Ungrouped(1 total)

firepower  
192.168.1.3 - Cisco Firepower Management Center for VMWare v6.6.5

**Health Policy**  
Initial\_Health\_Policy  
2021-05-21 14:10:56



# Actualización de FMC

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

The screenshot displays the Cisco Firepower Management Center (FMC) interface. At the top, the navigation bar includes the Cisco logo, the text "Firepower Management Center", and a search icon. The main menu contains "Overview", "Analysis", "Policies", "Devices", "Objects", "AMP", and "Intelligence". On the right side of the navigation bar, there are icons for "Deploy", a green checkmark, a gear, and a user profile labeled "admin".

Below the navigation bar, there are three tabs: "Product Updates", "Rule Updates", and "Geolocation Updates". The "Product Updates" tab is selected. Below the tabs, it states "Currently running software version: 6.6.5".

A "Selected Update" box contains the following information:

Type	Cisco Secure FW Mgmt Center Upgrade
Version	7.2.7-500
Date	Sat Apr 27 03:56:22 UTC 2024
Release Notes	
Reboot	Yes

Below the update details, there is a "By Group" dropdown menu. Underneath, a list of updates is shown. The first update is selected and is labeled "firepower" with a checkmark. The details for this update are:

192.168.1.3 - Cisco Firepower Management Center for VMWare v6.6.5	<b>Health Policy</b> Initial_Health_Policy 2021-05-21 14:10:56
---	--

At the bottom right of the interface, there are three buttons: "Cancel", "Launch Readiness Check", and "Install".

# Actualización de FMC

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

Firepower Management Center  
System / Updates / Upload Update

Deploy ✓ ⚙️ ? admin ▾

Product Updates Rule Updates Geolocation Updates

Currently running software version: **6.6.5**

**Selected Update**

Type	Cisco Secure FW Mgmt Center Upgrade
Version	7.2.7-500
Date	Sat Apr 27 03:56:22 UTC 2024
Release Notes	
Reboot	Yes

By Group ▾

Ungrouped(1 total)

firepower  
192.168.1.3 - Cisco Firepower Management Center for VMWare v6.6.5

**Health Policy**  
Initial\_Health\_Policy  
2021-05-21 14:10:56 ✓

Update installation will reboot the system(s). Are you sure you want to continue?

Cancel OK

Cancel Launch Readiness Check Install

# Actualización de FMC

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

Firepower Management Center  
System / Updates / Upload Update

Deploy admin

Product Updates Rule Updates Geolocation Updates

Upload Update

**Task Notification**  
Message Center Tasks Tab Local Update queued

Currently running software version: **6.6.5**

Updates

Type	Version	Date	Release Notes	Reboot	
Cisco FTD Upgrade	7.2.7-500	Sat Apr 27 04:09:29 UTC 2024		Yes	
Cisco Secure FW Mgmt Center Upgrade	7.2.7-500	Sat Apr 27 03:56:22 UTC 2024		Yes	

Download updates

# Actualización de FMC

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

Firepower Management Center  
System / Updates / Upload Update





Overview Analysis Policies Devices Objects AMP Intelligence

Product Updates Rule Updates Geolocation Updates




Task Notification  
Message Center Tasks Tab Local Update queued


Currently running software version: 6.6.5

Updates

Type	Version	Date	Release Notes	Reboot	
Cisco FTU Upgrade	7.2.7-500	Sat Apr 27 04:09:29 UTC 2024		Yes	 
Cisco Secure FW Mgmt Center Upgrade	7.2.7-500	Sat Apr 27 03:56:22 UTC 2024		Yes	 

Download updates

Deploy    admin

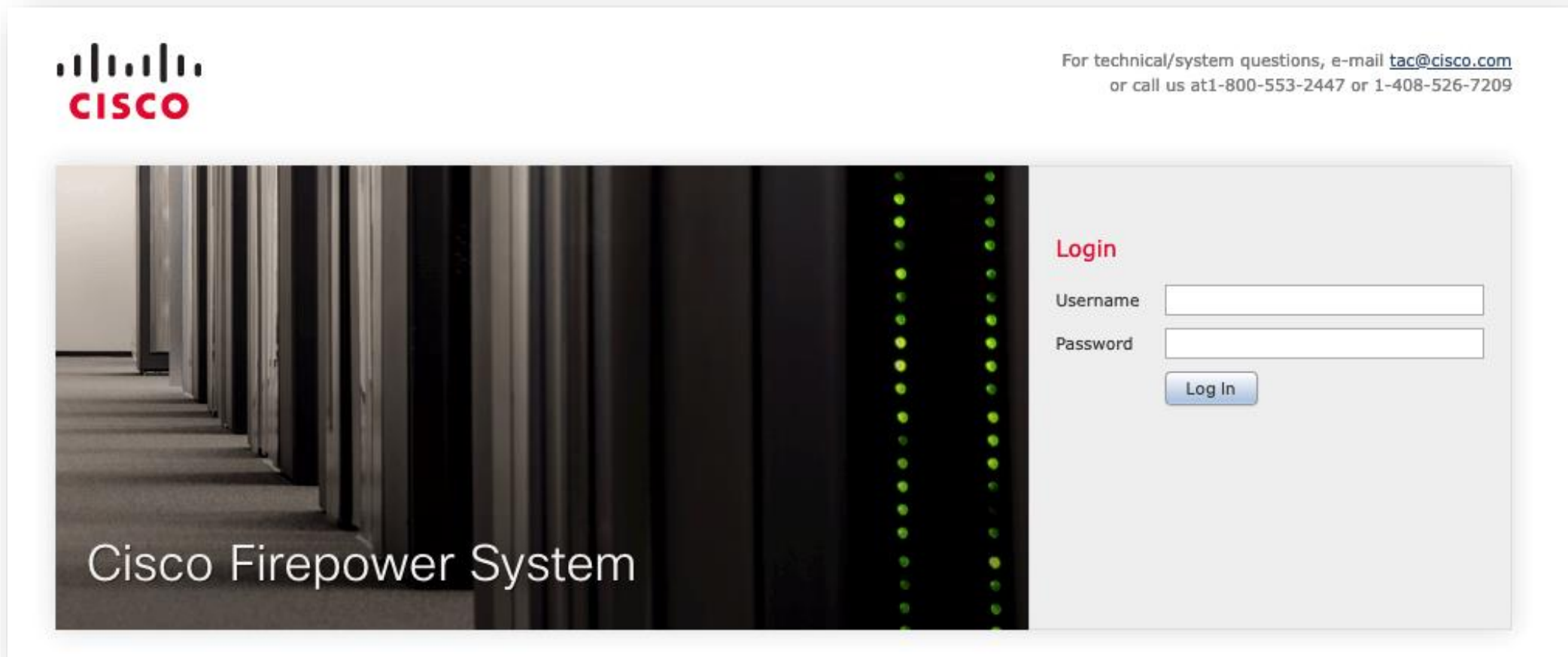
Deployments  Health **Tasks**  Show Notifications

20+ total | 0 waiting | 0 running | 1 retrying | 20+ success | 0 failures

Local Install  
Installing Cisco Secure FW Mgmt Center Upgrade version: 7.2.7-500  
Installing Cisco Secure FW Mgmt Center Upgrade version: 7.2.7-500 3m 24s

# 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

Firewall Management Center  
System / Updates / Upgrade Status

Logout | CISCO SECURE

Current Version: 6.6.5-81  
Upgrade Version: 7.2.7-500  
Elapsed Time: 4 minutes  
Estimated Time Remaining: 28 mins to go for reboot

20 %

**(Updating Operating System)**

**Running script 300\_os/070\_setup\_partition.sh...**

[\(show log for current script\)](#)

# Actualización de FMC

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

Firewall Management Center  
System / Updates / Upgrade Status

Logout | CISCO SECURE

Current Version: **6.6.5-81**  
Upgrade Version: **7.2.7-500**  
Elapsed Time: **4 minutes**  
Estimated Time Remaining: **28 mins to go for reboot**

20 %

**(Updating Operating System)**

**Running script 300\_os/070\_setup\_partition.sh...**  
(hide log for current script)

```
[240507 04:27:55:990] functions.sfos::runme: Step 1
[240507 04:27:55:991] functions.sfos::runme: Step 2
[240507 04:27:55:992] functions.sfos::runme: Step 3
[240507 04:27:55:993] Command [chmod 755 /new-root/ /new-root/usr /new-root/etc/ /new-root/usr/local] succeeded!
[240507 04:27:55:993] functions.sfos::runme: Step 4
[240507 04:27:55:994] functions.sfos::copy_root: Step 13
[240507 04:27:55:995] functions.sfos::create_new_partitions: Step 8
[240507 04:27:55:995] functions.sfos::copy_var: Step 1
[240507 04:27:55:996] functions.sfos::copy_var: Step 2
[240507 04:27:55:996] functions.sfos::copy_var: Step 3
[240507 04:27:55:997] functions.sfos::copy_var: Step 4
[240507 04:27:55:997] functions.sfos::copy_var: Step 5
[240507 04:27:55:998] functions.sfos::runme: Step 1
[240507 04:27:55:999] functions.sfos::runme: Step 2
[240507 04:27:56:000] functions.sfos::runme: Step 3
[240507 04:27:56:001] Command [rm -rf /var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade=7.2.7/copy_var.log] succeeded
[240507 04:27:56:001] functions.sfos::runme: Step 4
[240507 04:27:56:002] functions.sfos::copy_var: Step 6
[240507 04:27:56:003] functions.sfos::copy_var: Step 7
[240507 04:27:56:003] Copying var, exclude --exclude=sf/updates/* --exclude=sf/apply/* --exclude=sf/fireamp/fireamp.
[240507 04:27:56:004] functions.sfos::copy_var: Step 8
[240507 04:27:56:005] functions.sfos::copy_var: Step 8a
```

Log is current

# Actualización de FMC

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

Firewall Management Center  
System / Updates / Upgrade Status

Logout | Cisco SECURE

Current Version: 6.6.5-81  
Upgrade Version: 7.2.7-500  
Elapsed Time: 27 minutes  
Estimated Time Remaining: 1 min to go for reboot

100 %

**The appliance is rebooting.**  
This will take several minutes after which the upgrade will be complete. There will be no further reboot status updates on this page and it can be closed.

**Reboot started Less than a minute ago.**  
[\(hide log for current script\)](#)

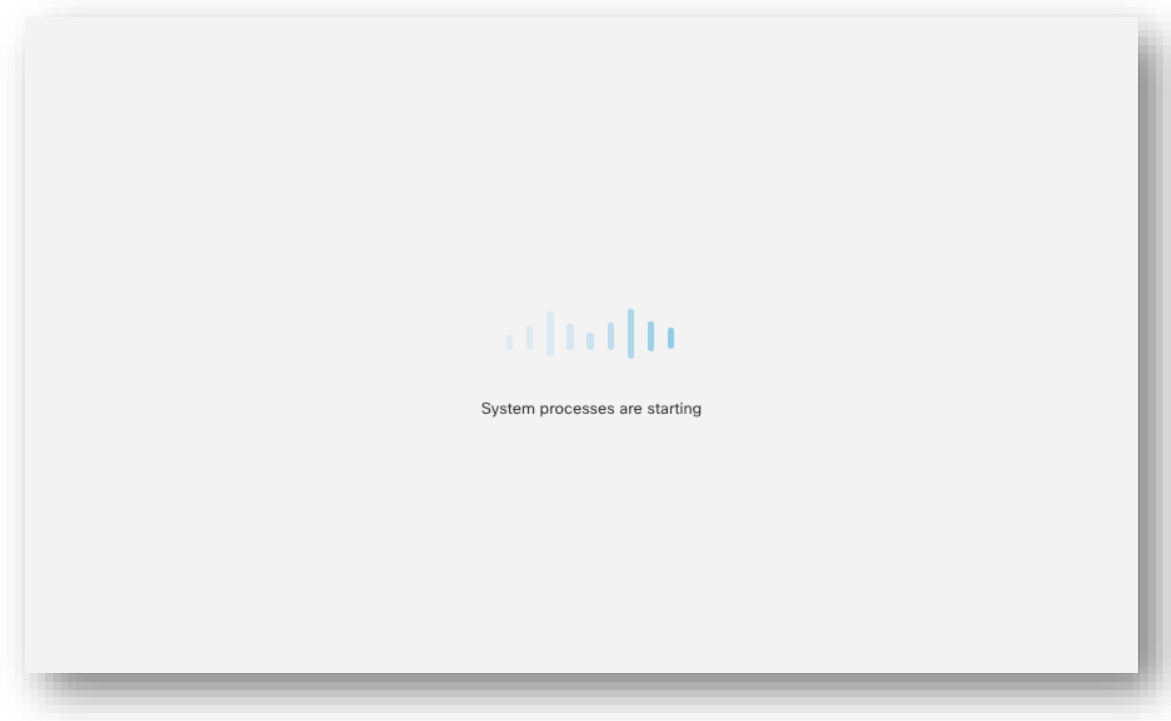
```
*****  
[240507 04:51:42:015] Starting script: 999_finish/999_disable_upgrade_ui.sh  
Entering 999_finish/999_disable_upgrade_ui.sh...  
writing reboot file to lock dir
```

Log is current



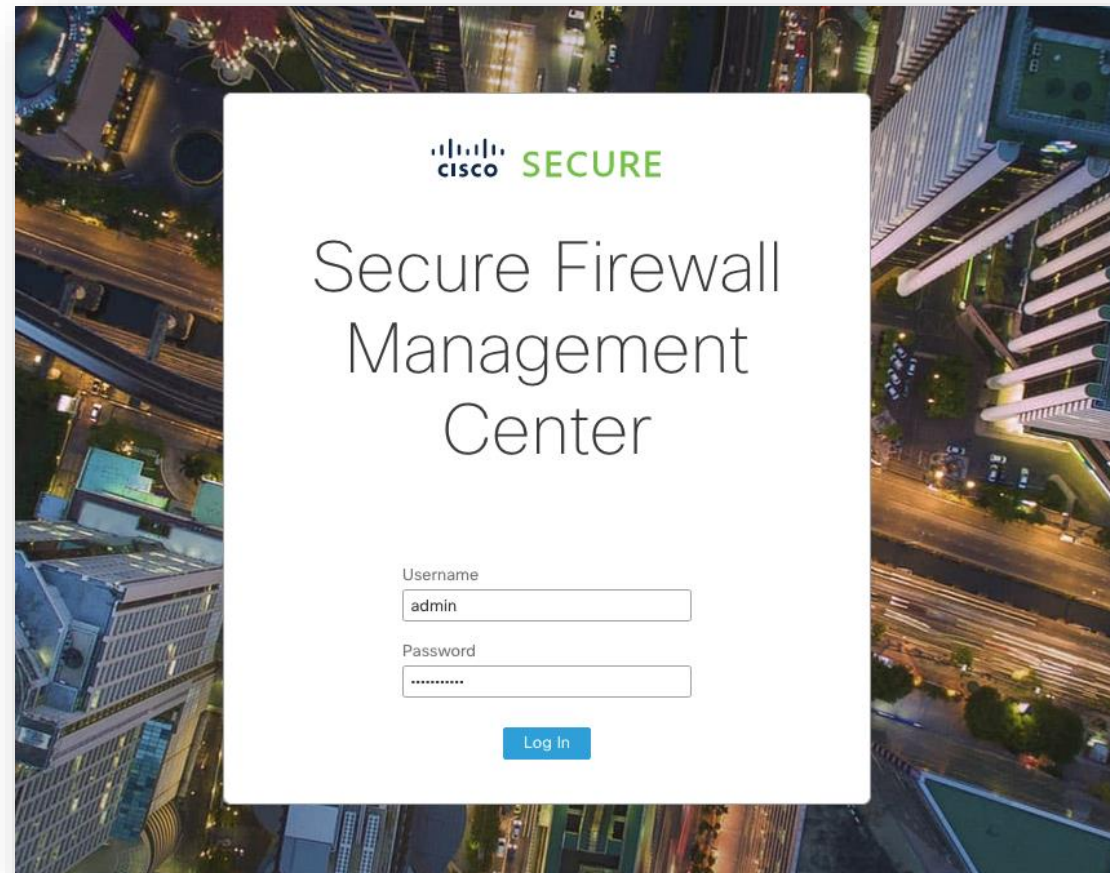
# Actualización de FMC

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



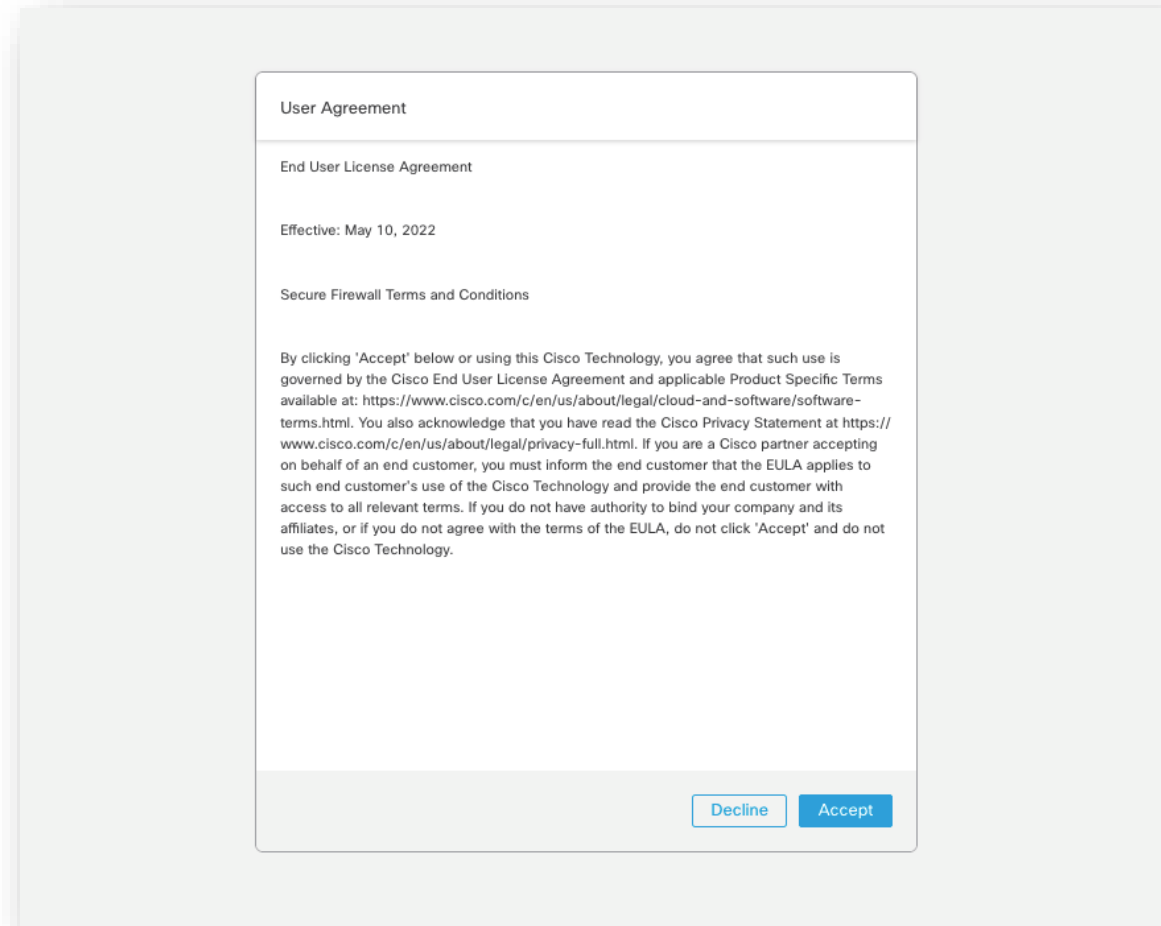
# Actualización de FMC

- 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

The screenshot displays the Cisco Firewall Management Center (FMC) interface. At the top, the navigation bar includes 'Firewall Management Center' and 'Overview / Dashboards / Dashboard'. The main navigation menu contains 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The user is logged in as 'admin'. A 'Task Notification' box in the center of the page reports: 'Installing Cisco Secure FW Mgmt Center Upgrade version: 7.2.7-500 (Local Install) succeeded at Tue May 7 00:55:45 2024 Successfully Installed'. Below the notification, the 'Summary Dashboard' is visible, showing 'No Data' for 'Indications of Compromise by Host', 'Indications of Compromise by User', and 'Connections by Security Intelligence Category'. The interface also features a 'Deploy' button, a search icon, and a 'Reporting' link.

# Actualización de FMC

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

The screenshot displays the Cisco Firewall Management Center (FMC) interface. At the top, the navigation menu includes Overview, Analysis, Policies, Devices, Objects, and Integration. The main content area features a Summary Dashboard with a central Task Notification box. The notification states: "Task Notification: Message Center Tasks Tab Your task Installing Cisco Secure FW Mgmt Center Upgrade version: 7.2.7-500 (Local Install) succeeded at Tue May 7 00:55:45 2024 Successfully Installed". To the right, a deployment panel shows a search bar, an "Advanced Deploy" link, and a "Deploy All" button. Below this, a table lists "FTD Backbone" with a status of "Ready for Deployment". At the bottom of the deployment panel, it indicates "1 inspect interruption" and "1 pending". The main dashboard area contains three widgets: "Indications of Compromise by Host", "Indications of Compromise by User", and "Connections by Security Intelligence Category", all of which currently display "No Data".

# Actualización de FMC

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

The screenshot displays the Cisco Firewall Management Center (FMC) interface. At the top, the navigation menu includes Overview, Analysis, Policies, Devices, Objects, and Integration. The main content area features a Summary Dashboard with a central Task Notification box. The notification states: "Task Notification: Message Center Tasks Tab Your task Installing Cisco Secure FW Mgmt Center Upgrade version: 7.2.7-500 (Local Install) succeeded at Tue May 7 00:55:45 2024 Successfully Installed". To the right, a deployment panel shows "Advanced Deploy" options for "FTD Backbone", which is "Ready for Deployment". Below the notification, there are three widget panels: "Indications of Compromise by Host", "Indications of Compromise by User", and "Connections by Security Intelligence Category", all displaying "No Data". The interface also includes a bottom navigation bar with "Network", "Threats", "Intrusion Events", "Status", "Geolocation", and "QoS".

# Actualización de FMC

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

The screenshot displays the Cisco Firewall Management Center (FMC) interface. At the top, the navigation menu includes Overview, Analysis, Policies, Devices, Objects, and Integration. The main content area features a Summary Dashboard with a central Task Notification box. The notification states: "Task Notification: Message Center Tasks Tab Your task Installing Cisco Secure FW Mgmt Center Upgrade version: 7.2.7-500 (Local Install) succeeded at Tue May 7 00:55:45 2024 Successfully Installed". To the right, a deployment progress window shows "Advanced Deploy" for "FTD Backbone" with "In Progress... (8%)". Below the notification, there are three widget panels: "Indications of Compromise by Host", "Indications of Compromise by User", and "Connections by Security Intelligence Category", all displaying "No Data". The interface also includes a top navigation bar with "Deploy" and "Reporting" options, and a bottom status bar with "Add Widgets".

# Actualización de FMC

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

The screenshot displays the Cisco Firewall Management Center (FMC) interface. At the top, the navigation menu includes Overview, Analysis, Policies, Devices, Objects, and Integration. The main content area features a Summary Dashboard with a central Task Notification box. The notification states: "Task Notification: Message Center Tasks Tab Your task Installing Cisco Secure FW Mgmt Center Upgrade version: 7.2.7-500 (Local Install) succeeded at Tue May 7 00:55:45 2024 Successfully Installed". To the right, a deployment window shows the status for "FTD Backbone" as "Completed". Below the notification, there are three widget panels: "Indications of Compromise by Host", "Indications of Compromise by User", and "Connections by Security Intelligence Category", all displaying "No Data". The interface also includes a top navigation bar with "Deploy" and "Reporting" options, and a bottom status bar with "1 inspect interruption" and "1 succeeded".



# Actualización de FMC

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

The screenshot displays the Cisco Firewall Management Center (FMC) interface. At the top, the navigation bar includes 'Firewall Management Center' with sub-links for 'Overview / Dashboards / Dashboard', and tabs for 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. On the right, there are options for 'Deploy', a search icon, a status indicator, a user profile for 'admin', and the 'cisco SECURE' logo.

The main content area is titled 'Summary Dashboard' with a '(switch dashboard)' link. Below this, a central notification box titled 'Task Notification' contains the following text: 'Message Center Tasks Tab Your task Installing Cisco Secure FW Mgmt Center Upgrade version: 7.2.7-500 (Local Install) succeeded at Tue May 7 00:55:45 2024 Successfully Installed'. The notification has a close button (X) in the top right corner.

Below the notification, there is a horizontal menu with 'Network', 'Threats' (selected), 'Intrusion Events', 'Status', 'Geolocation', and 'QoS'. To the right of this menu is a 'Show the Last' dropdown menu set to '1 hour' and a pause icon. An 'Add Widgets' button is located in the top right corner of the dashboard area.

The dashboard features three widget panels, each displaying 'No Data':

- 'Indications of Compromise by Host': Last updated 4 minutes ago.
- 'Indications of Compromise by User': Last updated 4 minutes ago.
- 'Connections by Security Intelligence Category': Last updated 3 minutes ago.

# Actualización de FMC

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

The screenshot displays the Cisco Firewall Management Center (FMC) interface. At the top, the navigation bar includes 'Overview / Dashboards / Dashboard' and tabs for 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The user is logged in as 'admin'. A central notification box states: 'Task Notification: Message Center Tasks Tab Your task Installing Cisco Secure FW Mgmt Center Upgrade version: 7.2.7-500 (Local Install) succeeded at Tue May 7 00:55:45 2024 Successfully Installed'. A help menu is open, listing options like 'Page-level Help', 'How-Tos', 'Documentation on Cisco.com', 'What's New in This Release', 'Software Download', 'Secure Firewall YouTube', 'Secure Firewall on Cisco.com', 'Firepower Migration Tool', 'Partner Ecosystem', 'Application Detectors', 'Ask a Question', and 'TAC Support Cases'. The main content area shows a 'Summary Dashboard' with a 'Threats' tab selected. Below the dashboard are three widget panels: 'Indications of Compromise by Host', 'Indications of Compromise by User', and 'Connections by Security Intelligence Category', all displaying 'No Data'. The interface also features a search bar, a 'Deploy' button, and a 'Show the Last 1 hour' filter.

# Actualización de FMC

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

The screenshot displays the Cisco Firewall Management Center (FMC) interface. At the top, the navigation bar includes 'Overview / Dashboards / Dashboard', 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. A 'Task Notification' message is visible, stating: 'Installing Cisco Secure FW Mgmt Center Upgrade version: 7.2.7-500 (Local Install) succeeded at Tue May 7 00:55:45 2024 Successfully Installed'. A central pop-up window titled 'Cisco Secure Firewall Management Center' provides system details:

Version 7.2.7 (build 500)	
Model	Secure Firewall Management Center for VMware
Serial Number	None
Snort Version	2.9.20 (Build 6102)
Snort3 Version	3.1.21.600 (Build 26)
Rule Pack Version	2993
Module Pack Version	3377
LSP Version	lsp-rel-20220511-1540
VDB Version	build 353 (2022-03-07 22:13:19)
Rule Update Version	2024-05-01-001-vrt
Geolocation Update Version	Country Code: 2024-04-07-030, IP: None
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.12.1 (build 73)
Hostname	FMC_Backbone

Additional text in the pop-up includes: 'For technical/system questions, email [tac@cisco.com](mailto:tac@cisco.com) phone: 1-800-553-2447 or 1-408-526-7209. Copyright 2004-2024, Cisco and/or its affiliates. All rights reserved.' and buttons for 'Copy' and 'Close'.

# 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.

Firewall Management Center  
System / Product Upgrades

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 🟢 ⚙️ ⓘ admin | cisco SECURE

### Product Upgrades

System Overview

**Management Center:** 7.2.7-500  
New upgrade available: 7.4.1-172  
Last upgrade performed: 6.6.5-81 → 7.2.7-500

**Threat Defense:** 1 device  
Visit [Device Management](#) to view your devices.  
**Upgrade:** Active (7.2.7-500) [Resume](#)

### Available Upgrade Packages

These are the downloadable upgrades that apply to your current deployment, and the upgrade packages you have manually uploaded or configured. [Upgrade Guide](#)

Upgrade	Release Date	Required Minimum Version	Availability	Actions
> 7.4.1-172	2023-12-13	7.0.0	Available for download	<a href="#">Download</a> ...
> 7.3.1-19	2023-03-09	6.7.0	Available for download	<a href="#">Download</a> ...
> 7.3.0-69	2022-11-28	6.7.0	Available for download	<a href="#">Download</a> ...
> 7.2.7-500	2024-04-27	6.6.0	Downloaded for all devices	<a href="#">Upgrade</a> ...

# 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.

Firewall Management Center  
System / Product Upgrades

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 🟢 ⚙️ ⓘ admin | cisco SECURE

## Product Upgrades

### System Overview

**Management Center:** 7.2.7-500  
New upgrade available: 7.4.1-172  
Last upgrade performed: 6.6.5-81 → 7.2.7-500

**Threat Defense:** 1 device  
Visit [Device Management](#) to view your devices.  
**Upgrade:** Active (7.2.7-500) [Resume](#)

### Available Upgrade Packages

These are the downloadable upgrades that apply to your current deployment, and the upgrade packages you have manually uploaded or configured. [Upgrade Guide](#)

Upgrade	Release Date	Required Minimum Version	Availability	Actions
> 7.4.1-172	2023-12-13	7.0.0	Available for download	<a href="#">Download</a> ...
> 7.3.1-19	2023-03-09	6.7.0	Available for download	<a href="#">Download</a> ...
> 7.3.0-69	2022-11-28	6.7.0	Available for download	<a href="#">Download</a> ...
▼ 7.2.7-500	2024-04-27	6.6.0	Downloaded for all devices	<a href="#">Upgrade</a> ...
Cisco Secure Firewall Management Center			Downloaded	...
Firepower Threat Defense for ASA/ISA/FTDv			Downloaded	...

# 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.

Firewall Management Center  
System / Product Upgrades

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 🟢 ⚙️ ⓘ admin ▾ | cisco SECURE

## Product Upgrades

### System Overview

**Management Center:** 7.2.7-500  
New upgrade available: 7.4.1-172  
Last upgrade performed: 6.6.5-81 → 7.2.7-500

**Threat Defense:** 1 device  
Visit [Device Management](#) to view your devices.  
**Upgrade:** Active (7.2.7-500) [Resume](#)

### Available Upgrade Packages

These are the downloadable upgrades that apply to your current deployment, and the upgrade packages you have manually uploaded or configured. [Upgrade Guide](#)

Upgrade	Release Date	Required Minimum Version	Availability	Actions
> 7.4.1-172	2023-12-13	7.0.0	Available for download	<a href="#">Download</a> ...
> 7.3.1-19	2023-03-09	6.7.0	Available for download	<a href="#">Download</a> ...
> 7.3.0-69	2022-11-28	6.7.0	Available for download	<a href="#">Download</a> ...
▼ 7.2.7-500	2024-04-27	6.6.0	Downloaded for all devices	<a href="#">Upgrade</a> ...
Cisco Secure Firewall Management Center			Downloaded	...
Firepower Threat Defense for ASA/ISA/FTDv			Downloaded	...

# Actualización de FTD

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

The screenshot shows the 'Threat Defense Upgrade' page in the Cisco Firewall Management Center. The page is divided into two main sections: 'Device Selection' and 'Device Details'.

**Device Selection:** This section contains a table with two columns: 'Device Selection' and 'Action'. The table is currently empty, with the message 'No devices selected.' and instructions: 'Use the Device Details pane to select devices to upgrade to the selected version. Or, use Device Management to select more devices.'

**Device Details:** This section contains a search bar and an 'Add to Selection' button. Below the search bar, there is a table with the following data:

Device	Model	Details
<input type="checkbox"/> FTD Backbone Version 6.6.5	FTDv for VMware	

At the bottom of the page, there are buttons for 'How To', 'Reset', and 'Next'.



# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Manage Upgrade Packages Unattended Mode

Device Selection	Action
1 device is a candidate to add to your upgrade list.	
No devices selected.	Use the Device Details pane to select devices to upgrade to the selected version. Or, use <a href="#">Device Management</a> to select more devices.

#### Device Details

1 device is a candidate to add to your upgrade list.

Search Add to Selection

Device	Model	Details
<input checked="" type="checkbox"/> FTD Backbone Version 6.6.5	FTDv for VMware	

How To Reset Next

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Manage Upgrade Packages Unattended Mode

Device Selection	Action
1 device is a candidate to add to your upgrade list.	
No devices selected.	Use the Device Details pane to select devices to upgrade to the selected version. Or, use <a href="#">Device Management</a> to select more devices.

#### Device Details

1 device is a candidate to add to your upgrade list.

Search

Device	Model	Details
<input checked="" type="checkbox"/> FTD Backbone Version 6.5.5	FTDv for VMware	

How To Reset Next

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin | CISCO SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Manage Upgrade Packages

Unattended Mode

Device Selection	Action
1 device selected to upgrade to Version 7.2.7-500.	Use Device Management to select more devices.
▲ 1 device still needs an upgrade package.	Copy Upgrade Package

Device Details	Model	Details
1 device selected for upgrade.		
<input type="checkbox"/> Device -		
<input type="checkbox"/> FTD Backbone Version 6.6.5	FTDv for VMware	Device is missing upgrade package.

How To Reset Next

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 cisco SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Manage Upgrade Packages Unattended Mode

Device Selection	Action
1 device selected to upgrade to Version 7.2.7-500.	Use Device Management to select more devices.
▲ 1 device still needs an upgrade package.	<a href="#">Copy Upgrade Package</a>

Device Details	Model	Details
1 device selected for upgrade.		
<input type="checkbox"/> Device		
<input type="checkbox"/> FTD Backbone Version 6.6.5	FTDv for VMware	Device is missing upgrade package.

How To Reset Next

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 cisco SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Manage Upgrade Packages Unattended Mode

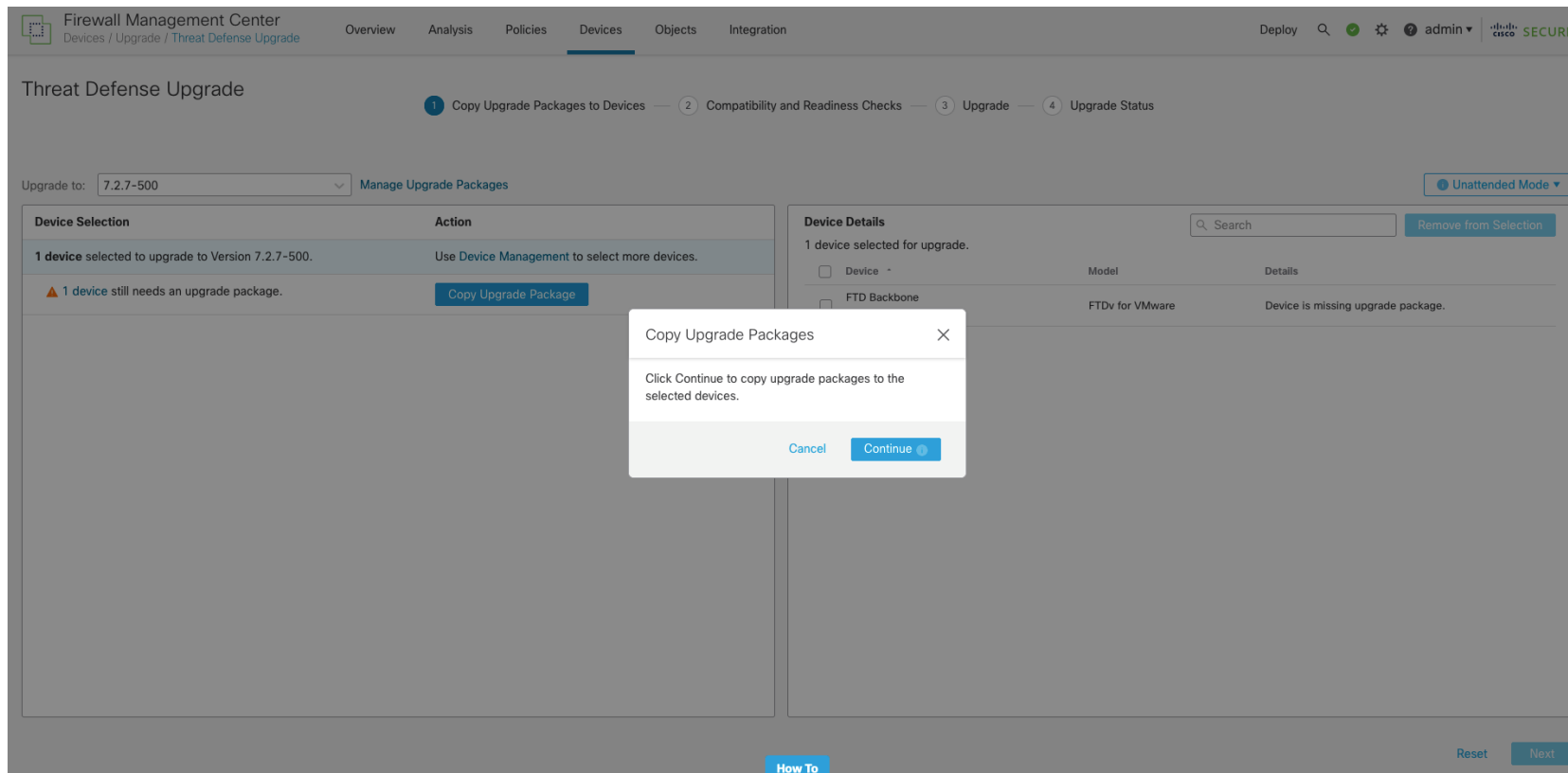
Device Selection	Action
1 device selected to upgrade to Version 7.2.7-500.	Use Device Management to select more devices.
▲ 1 device still needs an upgrade package.	<b>Copy Upgrade Package</b>

Device Details		
1 device selected for upgrade.		
<input type="checkbox"/> Device	Model	Details
<input type="checkbox"/> FTD Backbone Version 6.6.5	FTDv for VMware	Device is missing upgrade package.

How To Reset Next

# 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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Manage Upgrade Packages Unattended Mode

Device Selection	Action
1 device selected to upgrade to Version 7.2.7-500.	Use <a href="#">Device Management</a> to select more devices.
1 device still needs an upgrade package. Last performed 2024-05-07 08:07:41 EDT.	<a href="#">Copy Upgrade Package</a> Use the <a href="#">Message Center</a> to view copy status.

Device Details		
1 device selected for upgrade.		
<input type="checkbox"/>	Device -	Model
<input type="checkbox"/>	FTD Backbone Version 6.6.5	FTDv for VMware Last copy: in progress.

[How To](#) Reset Next

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Manage Upgrade Packages Unattended Mode

Device Selection	Action
1 device selected to upgrade to Version 7.2.7-500.	Use Device Management to select more devices.
1 device has the upgrade package and is ready for compatibility and readiness checks.	

Device Details	Model	Details
1 device selected for upgrade.		
<input type="checkbox"/> Device -		
<input type="checkbox"/> FTD Backbone Version 6.6.5	FTDv for VMware	Ready for checks.

1 of 1 selected device has the upgrade package.

How To Reset Next



# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 cisco SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Manage Upgrade Packages Unattended Mode

Device Selection	Action
1 device selected to upgrade to Version 7.2.7-500.	Use Device Management to select more devices.
1 device has the upgrade package and is ready for compatibility and readiness checks.	

Device Details	Model	Details
1 device selected for upgrade.		
<input type="checkbox"/> Device -		
<input type="checkbox"/> FTD Backbone Version 6.6.5	FTDv for VMware	Ready for checks.

1 of 1 selected device has the upgrade package.

How To Reset **Next**

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin | Cisco SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 **Compatibility and Readiness Checks** — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Unattended Mode

#### Device Selection

**Action**

1 device ready for compatibility and readiness checks.

#### Compatibility and Readiness Check Preferences

Require passing compatibility and readiness checks.

▲ Ready to upgrade: 0 devices.

#### Compatibility and Readiness Checks

[Run Readiness Check](#)

▲ No results available: 1 device.

#### Device Details

1 device has the upgrade package and is ready for compatibility and readiness checks.

Device	Model	Details
FTD Backbone Version 6.6.5	FTDv for VMware	Not ready for upgrade. Compatibility check passed. Read...

[How To](#) [Reset](#) [Previous](#) [Next](#)

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin | Cisco SECURE

Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Unattended Mode

**Device Selection** **Action**

1 device ready for compatibility and readiness checks.

**Compatibility and Readiness Check Preferences**

Require passing compatibility and readiness checks.

▲ Ready to upgrade: 0 devices.

**Compatibility and Readiness Checks** Run Readiness Check

▲ No results available: 1 device.

**Device Details**

1 device has the upgrade package and is ready for compatibility and readiness checks.

Device	Model	Details
FTD Backbone Version 6.6.5	FTDv for VMware	Not ready for upgrade. Compatibility check passed. Read...

[How To](#) Reset Previous Next

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco SECURE

### Threat Defense Upgrade

① Copy Upgrade Packages to Devices — ② Compatibility and Readiness Checks — ③ Upgrade — ④ Upgrade Status

Upgrade to: 7.2.7-500 Unattended Mode

#### Device Selection

**Action**

1 device ready for compatibility and readiness checks.

#### Compatibility and Readiness Check Preferences

Require passing compatibility and readiness checks.

▲ Ready to upgrade: 0 devices.

#### Compatibility and Readiness Checks

[Run Readiness Check](#)

▲ No results available: 1 device.

#### Device Details

1 device has the upgrade package and is ready for compatibility and readiness checks.

Device	Model	Details
FTD Backbone	FTDv for VMware	Not ready for upgrade. Compatibility check passed. Read...

#### Readiness Check

Click Continue to run the readiness check for all eligible devices.

[Cancel](#) [Continue](#)

[How To](#) [Reset](#) [Previous](#) [Next](#)

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin | Cisco SECURE

### Threat Defense Upgrade

① Copy Upgrade Packages to Devices — ② **Compatibility and Readiness Checks** — ③ Upgrade — ④ Upgrade Status

Upgrade to: 7.2.7-500 Unattended Mode

#### Device Selection

**Action**

1 device ready for compatibility and readiness checks.

#### Compatibility and Readiness Check Preferences

Require passing compatibility and readiness checks.

▲ Ready to upgrade: 0 devices.

#### Compatibility and Readiness Checks

[Run Readiness Check](#)

Last performed 2024-05-07 08:23:27 EDT.  
Use the Message Center to view check status.

In progress: 1 device.

#### Device Details

1 device has the upgrade package and is ready for compatibility and readiness checks.

Device	Model	Details
FTD Backbone Version 6.6.5	FTDv for VMware	Not ready for upgrade. Compatibility check passed. Read...

[How To](#) Reset Previous Next

# Actualización de FTD

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

The screenshot shows the Cisco Firewall Management Center interface for a Threat Defense Upgrade. The main panel is titled "Threat Defense Upgrade" and shows a progress bar with three steps: 1. Copy Upgrade Packages to Devices, 2. Compatibility and Readiness Checks (current step), and 3. Upgrade. Below the progress bar, it indicates "Upgrade to: 7.2.7-500".

The "Device Selection" section shows "1 device ready for compatibility and readiness checks." The "Compatibility and Readiness Check Preferences" section has a toggle for "Require passing compatibility and readiness checks." and shows "Ready to upgrade: 0 devices." The "Compatibility and Readiness Checks" section has a "Run Readiness Check" button and shows "Last performed 2024-05-07 08:23:27 EDT." and "In progress: 1 device."

The "Device Details" section shows "1 device has the upgrade packa" and "FTD Backbone Version 6.6.5".

The task pane on the right shows a list of tasks:

- Remote Readiness Check: Checking Cisco FTD Upgrade 7.2.7-500 on FTD Backbone. FTD Backbone: Readiness Check has completed. 1m 9s
- Copy Files: Copy files to devices. Requested: 1. Copied: 1. Failed: 0. 12s
- Policy Deployment: Policy Deployment to FTD Backbone. Applied successfully. 48s
- Policy Pre-Deployment: Pre-deploy Device Configuration for FTD Backbone. 3s

At the bottom of the task pane, there is a "Remove completed tasks" button. The main panel has a "How To" button at the bottom center and "Reset", "Previous", and "Next" buttons at the bottom right.

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin | 🔒 Cisco SECURE

### Threat Defense Upgrade

① Copy Upgrade Packages to Devices — ② **Compatibility and Readiness Checks** — ③ Upgrade — ④ Upgrade Status

Upgrade to: 7.2.7-500 Unattended Mode ▾

**Device Selection** **Action**

1 device ready for compatibility and readiness checks.

**Compatibility and Readiness Check Preferences**

Require passing compatibility and readiness checks.  
 Ready to upgrade: 1 device.

**Compatibility and Readiness Checks** [Run Readiness Check](#)

Last performed 2024-05-07 08:23:27 EDT.  
Use the Message Center to view check status.

Passed: 1 device.

**Device Details** Search

1 device has the upgrade package and is ready for compatibility and readiness checks.

Device	Model	Details
FTD Backbone Version 6.6.5	FTDv for VMware	Ready for upgrade. Compatibility and readiness checks p...

1 of 1 selected device is ready to proceed with upgrade.

[How To](#) [Reset](#) [Previous](#) [Next](#)

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Unattended Mode

#### Device Selection

**Action**

1 device ready for compatibility and readiness checks.

#### Compatibility and Readiness Check Preferences

Require passing compatibility and readiness checks.  
 Ready to upgrade: 1 device.

#### Compatibility and Readiness Checks

Last performed 2024-05-07 08:23:27 EDT.

[Run Readiness Check](#)  
Use the Message Center to view check status.

Passed: 1 device.

#### Device Details

1 device has the upgrade package and is ready for compatibility and readiness checks.

Device	Model	Details
FTD Backbone Version 6.6.5	FTDv for VMware	Ready for upgrade. Compatibility and readiness checks p...

1 of 1 selected device is ready to proceed with upgrade.

[How To](#) [Reset](#) [Previous](#) [Next](#)



# 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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin | CISCO SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Unattended Mode

#### Device Selection

1 device is ready for upgrade to Version 7.2.7-500.

#### Upgrade Failure

Automatically cancel on upgrade failure and roll back to the previous version.

#### Troubleshooting

Generate troubleshooting files before upgrade begins.

#### Enable Revert

Enable revert after successful upgrade.

#### Upgrade Snort

Convert eligible devices from Snort 2 to Snort 3.

#### Device Details

1 device is ready for upgrade.

Device	Model	Snort 3	Details
FTD Backbone Version 6.6.5	FTDv for VMware	✓	Ready for upgrade. Compatibility and readiness chec...

1 of 1 selected device is ready for upgrade.

[How To](#) [Reset](#) [Previous](#) [Start Upgrade](#)

# 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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin | CISCO SECURE

Threat Defense Upgrade

1 Copy Upgrade Packages to Devices 2 Compatibility and Readiness Checks 3 Upgrade 4 Upgrade Status

Upgrade to: 7.2.7-500 Unattended Mode

**Device Selection**

1 device is ready for upgrade to Version 7.2.7-500.

**Upgrade Failure**

- Automatically cancel on upgrade failure and roll back to the previous version.

**Troubleshooting**

- Generate troubleshooting files before upgrade begins.

**Enable Revert** ⚠️

- Enable revert after successful upgrade. ⚙️

**Upgrade Snort** ⚠️

- Convert eligible devices from Snort 2 to Snort 3. ⚙️

**Device Details**

1 device is ready for upgrade.

Device	Model	Snort 3	Details
FTD Backbone Version 6.6.5	FTDv for VMware	✔️	Ready for upgrade. Compatibility and readiness chec...

1 of 1 selected device is ready for upgrade.

[How To](#) [Reset](#) [Previous](#) [Start Upgrade](#)

# 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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin | Cisco SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 Unattended Mode

#### Device Selection

1 device is ready for upgrade to Version 7.2.7-500.

#### Upgrade Failure

Automatically cancel on upgrade failure and roll back to the previous version.

#### Troubleshooting

Generate troubleshooting files before upgrade begins.

#### Enable Revert

Enable revert after successful upgrade.

#### Upgrade Snort

Convert eligible devices from Snort 2 to Snort 3.

#### Device Details

1 device is ready for upgrade.

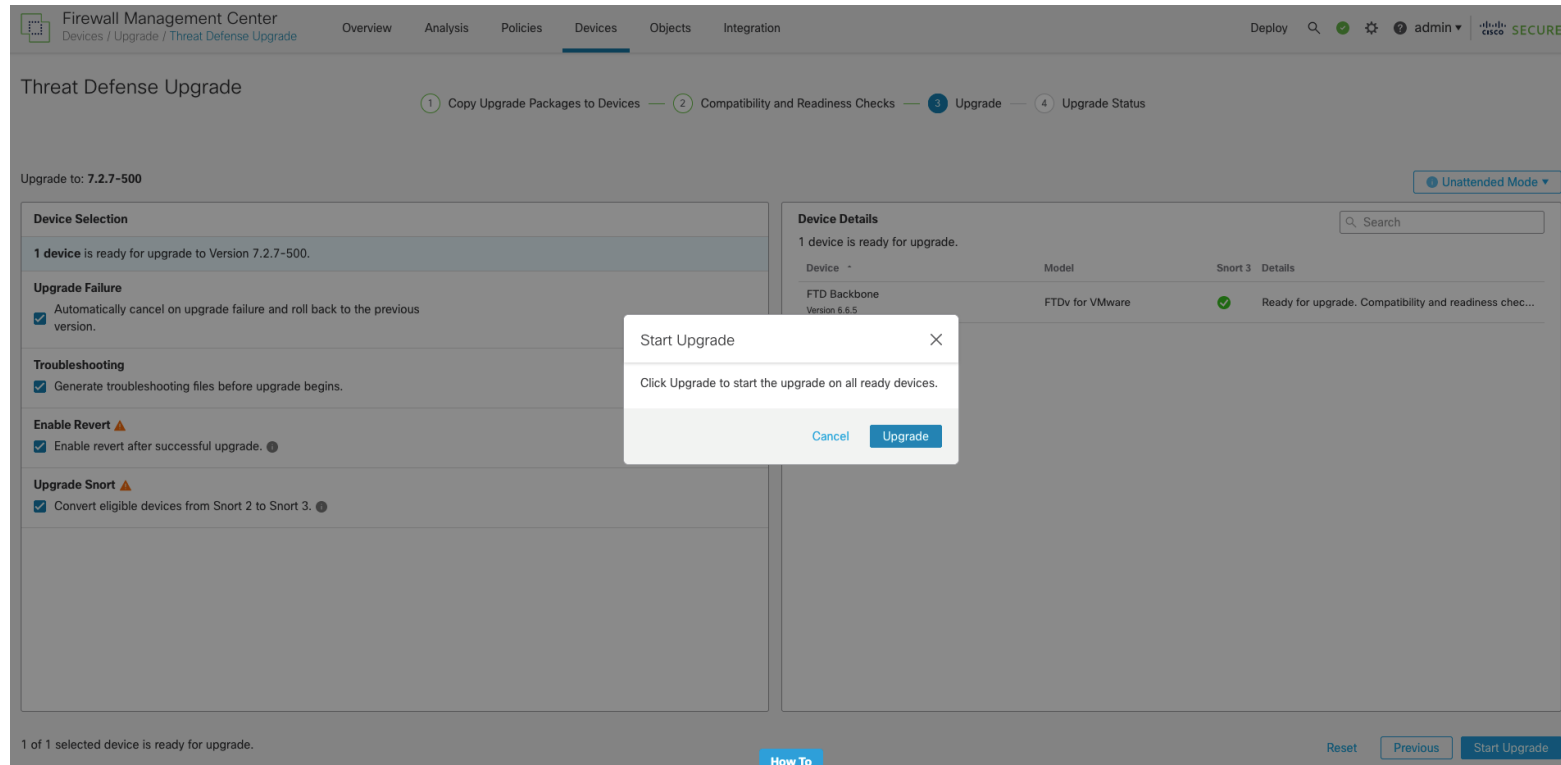
Device	Model	Snort 3	Details
FTD Backbone Version 6.6.5	FTDv for VMware	✓	Ready for upgrade. Compatibility and readiness chec...

1 of 1 selected device is ready for upgrade.

[How To](#) [Reset](#) [Previous](#) [Start Upgrade](#)

# 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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco SECURE

### Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

✔ Upgrade of selected devices started 2024-05-07 10:43:20 EDT.  
Use the [Message Center](#) to view overall upgrade status. Detailed upgrade status is available on this page and the [Device Management](#) page.  
The information on this page is for the last performed upgrade, and is for reference only. Click [Clear Upgrade Information](#) to clear the page and upgrade additional devices. To view detailed upgrade status after clearing the page, use [Device Management](#).

[Clear Upgrade Information](#)

Upgrade to: **7.2.7-500** Completed: 0 Failed: 0 In progress: 1 🔍 Search

Device	Model	Status
FTD Backbone Version 6.6.5	FTDv for VMware	In progress... (0%) Initializing... <a href="#">View Details</a>

[How To](#) [Reset](#) [Previous](#)

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies Devices Objects Integration

Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade

✓ Upgrade of selected devices started 2024-05-07 10:43:20 EDT.  
Use the [Message Center](#) to view overall upgrade status. Detailed upgrade status is available on this page and the [Device Management](#) page.  
The information on this page is for the last performed upgrade, and is for reference only. Click [Clear Upgrade Information](#) to clear the page and upgrade additional devices.

Clear Upgrade Information

Upgrade to: 7.2.7-500

Device	Model	Status
FTD Backbone Version 6.6.5	FTDv for VMware	In progress Initializing...

Deployments Upgrades Health Tasks

10 total | 0 waiting | 1 running | 0 retrying | 9 success | 0 failures | Filter

Remote Install  
Apply Cisco FTD Upgrade 7.2.7-500 to FTD(s)  
Running update for 1 devices. 1m 58s

Policy Deployment  
Policy Deployment to FTD Backbone. Applied successfully 25s X

Policy Pre-Deployment  
Pre-deploy Device Configuration for FTD Backbone  
success 2s X

Policy Pre-Deployment  
Pre-deploy Global Configuration Generation  
success 8s X

Remove completed tasks

How To Reset Previous

# Actualización de FTD

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

Firewall Management Center  
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies Devices Objects Integration

Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade

✓ Upgrade of selected devices started 2024-05-07 10:43:20 EDT.  
Use the [Message Center](#) to view overall upgrade status. Detailed upgrade status is available on this page and the [Device Management](#) page.  
The information on this page is for the last performed upgrade, and is for reference only. Click [Clear Upgrade Information](#) to clear the page and upgrade additional devices.

Clear Upgrade Information

Upgrade to: 7.2.7-500

Device	Model	Status
FTD Backbone Version 6.6.5	FTDv for VMware	In progress Initializing...

Deployments Upgrades Health Tasks

1 total 1 in progress 0 completed 0 failed

In Progress - 1 Tasks  
Upgrade In Progress (1)  
Firepower Threat Defense for ASA/ISA/FTDv 7.2.7-500 (1)

Go to [Device Management](#) for details on upgrade tasks

How To Reset Previous

# 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

The screenshot displays the 'Threat Defense Upgrade' interface in the Firewall Management Center. The page shows a progress bar with four steps: 1. Copy Upgrade Packages to Devices, 2. Compatibility and Readiness Checks, 3. Upgrade, and 4. Upgrade Status. A green notification box indicates that the upgrade of selected devices started on 2024-05-07 at 10:43:20 EDT. Below this, a table shows the upgrade details for 'FTD Backbone Version 6.5.5' to '7.2.7-500', with a status of 'Completed'. The table also includes columns for 'Device', 'Model', and 'Status'. A search bar and a 'Search' button are visible above the table. At the bottom of the page, there are buttons for 'How To', 'Reset', and 'Previous'.

Device	Model	Status
FTD Backbone Version 6.5.5	FTDv for VMware	Completed <a href="#">View Details</a>



# Actualización de FTD

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

Firewall Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 🟢 ⚙️ 👤 admin | 🔒 CISCO SECURE

View By: Group

All (1) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (1) ● Deployment Pending (1) ● Upgrade (1) ● Snort 3 (1)

🔍 Search Device **Add** ▾

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	▼ Ungrouped (1)							
<input type="checkbox"/>	● <b>FTD Backbone</b> Snort 3 192.168.1.2 - Routed	FTDv for VMware	7.2.7	N/A	Base, Threat (2 more...)	● test	↶	✎ ⋮

# Actualización de FTD

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

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active. The interface displays a table of devices with the following columns: Name, Model, Version, Chassis, Licenses, Access Control Policy, and Auto RollBack. A device named 'FTD Backbone' is highlighted, and its version '7.2.7' is circled in red. The device is associated with the model 'FTDv for VMware' and the chassis 'N/A'. The license is 'Base, Threat (2 more...)'. The access control policy is 'test'. The auto rollback is 'test'. The device is also associated with the snort 3 version 'Snort 3 (1)'. The interface also shows a search bar for devices and an 'Add' button.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FTD Backbone 192.168.1.2 - Routed	FTDv for VMware	7.2.7	N/A	Base, Threat (2 more...)	test	test

# Actualización de FTD

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

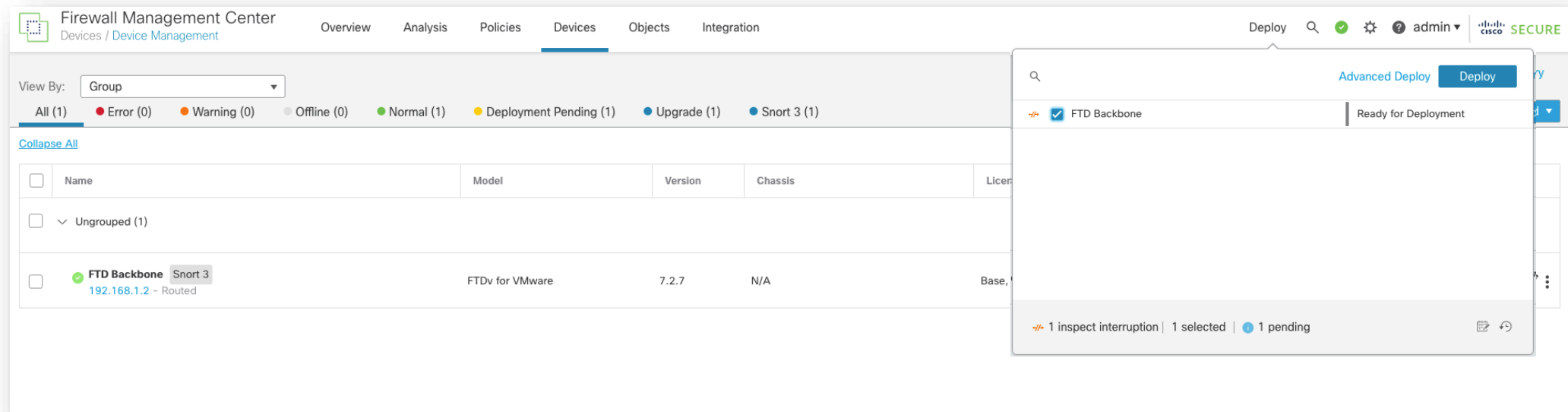
The screenshot displays the Cisco Firewall Management Center (FMC) interface. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active, showing a list of devices. The 'View By' dropdown is set to 'Group'. The status bar indicates: All (1), Error (0), Warning (0), Offline (0), Normal (1), Deployment Pending (1), Upgrade (1), and Snort 3 (1). A table lists the devices:

Name	Model	Version	Chassis	License
Ungrouped (1)				
FTD Backbone Snort 3 192.168.1.2 - Routed	FTDv for VMware	7.2.7	N/A	Base,

A 'Deploy' modal window is open, showing a search bar, 'Advanced Deploy' and 'Deploy All' buttons, and a status bar indicating '1 inspect interruption' and '1 pending'.

# Actualización de FTD

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



The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active, showing a table of devices. The table has columns for Name, Model, Version, Chassis, and License. A device named 'FTD Backbone' is highlighted, with a status of 'Normal (1)'. A deployment modal is open over the table, showing a search bar, a 'Deploy' button, and a status of 'Ready for Deployment'. The modal also displays a summary: '1 inspect interruption | 1 selected | 1 pending'.

Name	Model	Version	Chassis	License
Ungrouped (1)				
FTD Backbone Snort 3 192.168.1.2 - Routed	FTDv for VMware	7.2.7	N/A	Base,

# Actualización de FTD

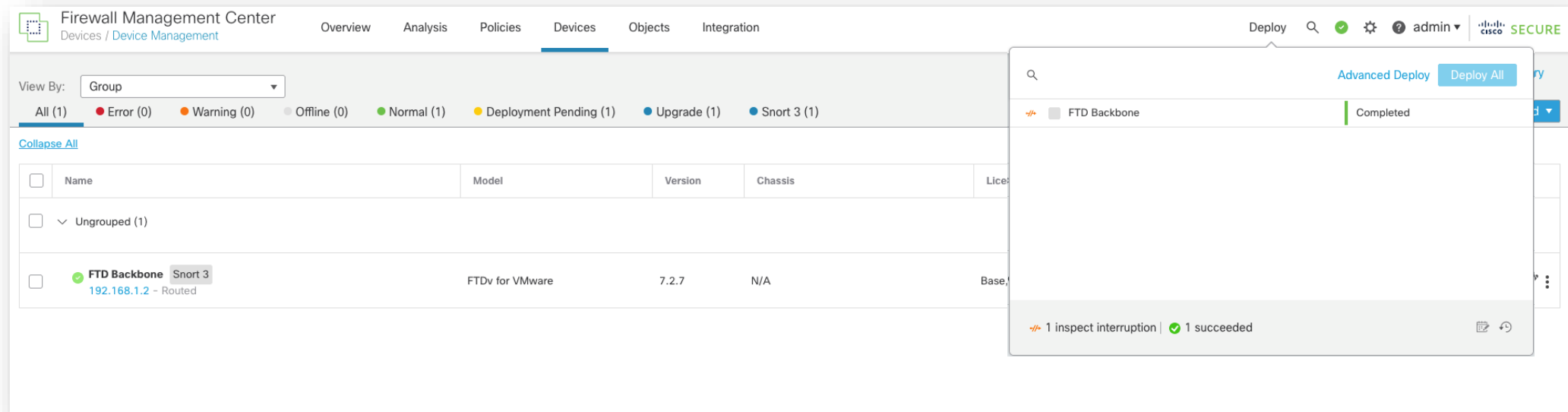
1. Dirigete a Devices > Device Management para validar la nueva versión del FTD
2. Realiza las implementaciones de configuración pendientes

The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active, showing a table of devices. The table has columns for Name, Model, Version, Chassis, and License. A device named 'FTD Backbone' is highlighted, with a status of 'Snort 3' and a deployment progress indicator. A modal window titled 'Advanced Deploy' is open, showing a progress bar for 'FTD Backbone' at 37% completion, with the text 'In Progress... (37%) Deployment to device pending.' Below the progress bar, it indicates '1 inspect interruption' and '1 in progress'.

Name	Model	Version	Chassis	License
FTD Backbone	FTDv for VMware	7.2.7	N/A	Base

# Actualización de FTD

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



The screenshot displays the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active, showing a list of devices. The 'View By' dropdown is set to 'Group'. The status bar indicates: All (1), Error (0), Warning (0), Offline (0), Normal (1), Deployment Pending (1), Upgrade (1), and Snort 3 (1). A table lists the devices:

Name	Model	Version	Chassis	License
FTD Backbone Snort 3 192.168.1.2 - Routed	FTDv for VMware	7.2.7	N/A	Base

A deployment summary window is open on the right, showing a progress bar for 'FTD Backbone' which is 'Completed'. The summary indicates: 1 inspect interruption | 1 succeeded.

# 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

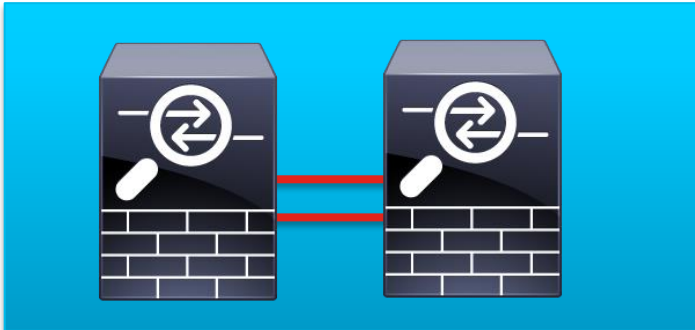
Use this procedure to upgrade a standalone FTD device. If you need to update FXOS, do that first. To upgrade high availability threat defense, see [Upgrade High Availability FTD](#).



**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

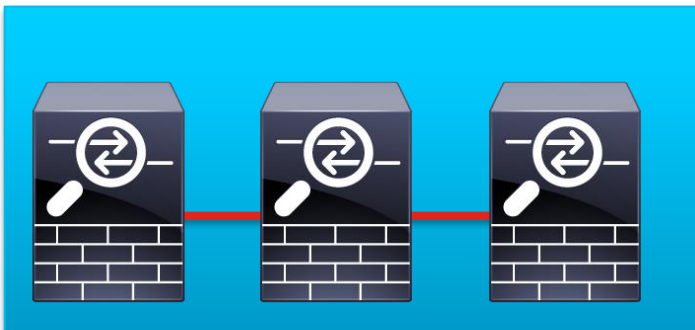
This document describes the upgrade process for a Cisco Secure Firewall Threat Defense in High Availability managed by a Firewall Management Center.

### 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)

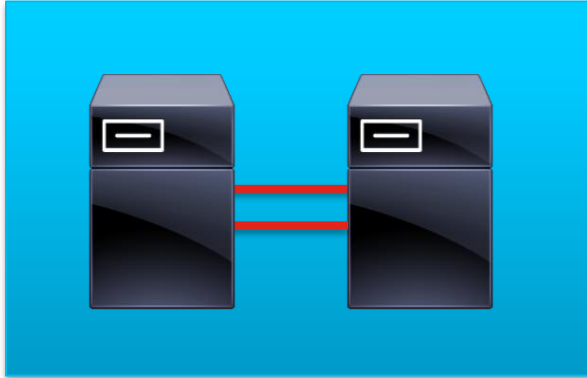
Use this procedure to upgrade threat defense using the System Updates page.



**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](#)

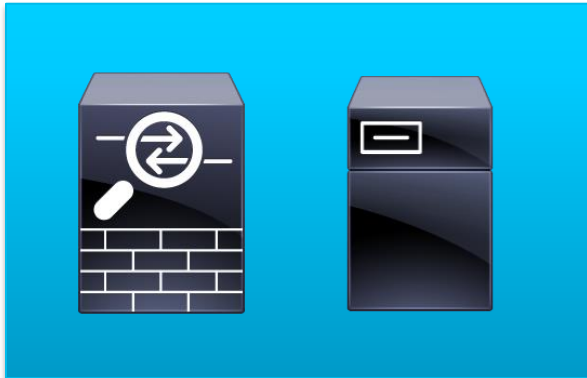
### Introduction

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.



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