Migración de FDM a FMC mediante FMT mediante el archivo Configuration.zip

Contenido

Introducción

En este documento se describe cómo generar el archivo de configuración .zip de un administrador de dispositivos de firewall seguro (FDM) que se migrará a un FMC mediante FMT.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Firewall Threat Defence (FTD)
- Cisco Firewall Management Center (FMC)
- Herramienta de migración de firewall (FMT)
- Plataforma API Postman

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software.

FTD 7.4.2

CSP 7.4.2

FMT 7.7.0.1

Cartero 11.50.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

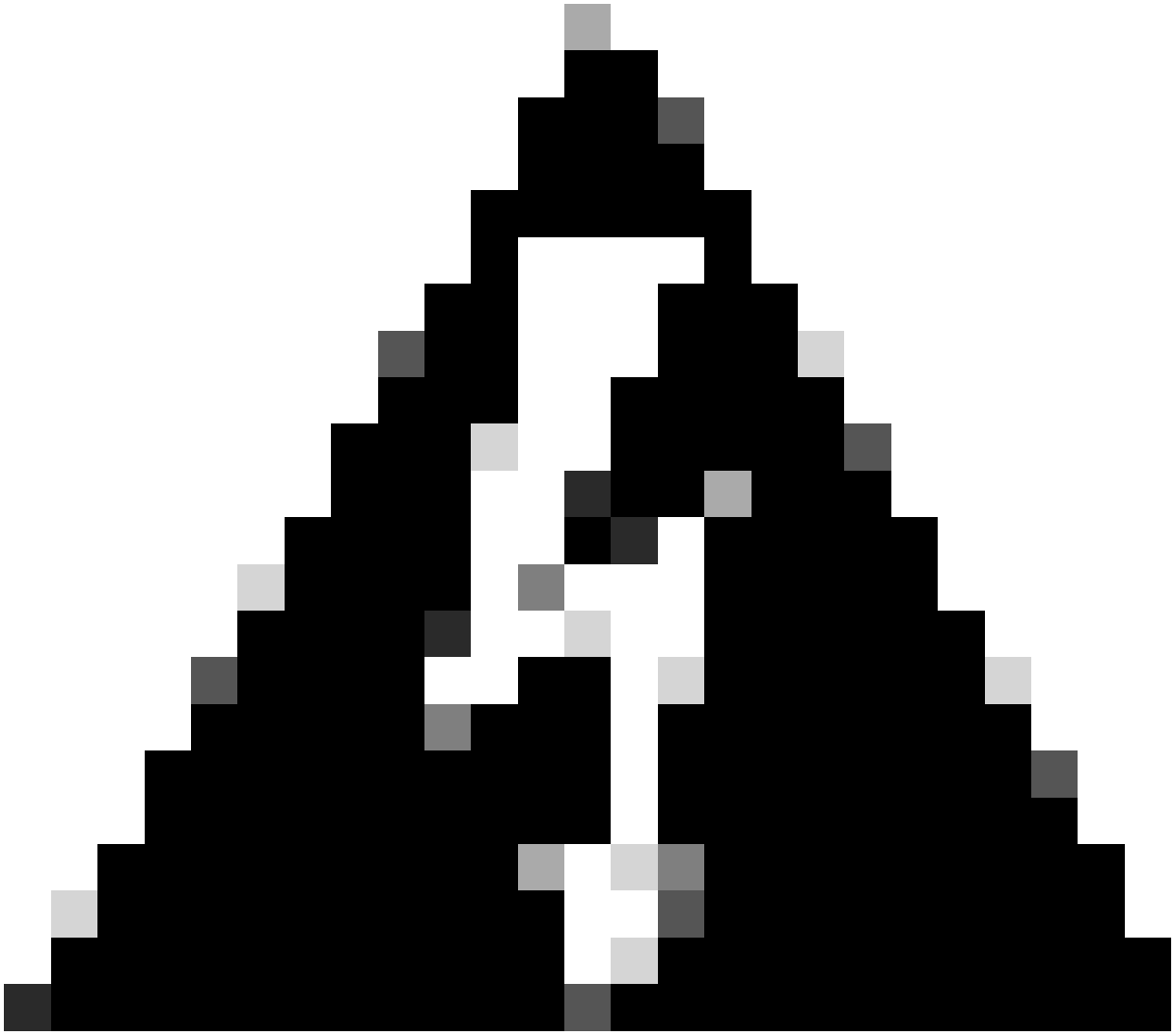
de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

- FDM se puede migrar ahora a FMC de diferentes formas. En este documento, el escenario que se va a explorar es la generación del archivo .zip de configuración mediante solicitudes de API y la carga posterior de ese archivo a FMT para migrar la configuración a FMC.
- Los pasos que se muestran en este documento comienzan a utilizar Postman directamente, por lo que se recomienda tener Postman ya instalado. El PC o portátil que vaya a utilizar debe tener acceso a FDM y FMC, y FMT debe estar instalado y ejecutándose.

Consideraciones

- Este documento se centra en la generación del archivo .zip de configuración más que en el uso de FMT.
- La migración de FDM mediante el archivo .zip de configuración es para migraciones que no son en tiempo real y no requieren inmediatamente un FTD de destino.

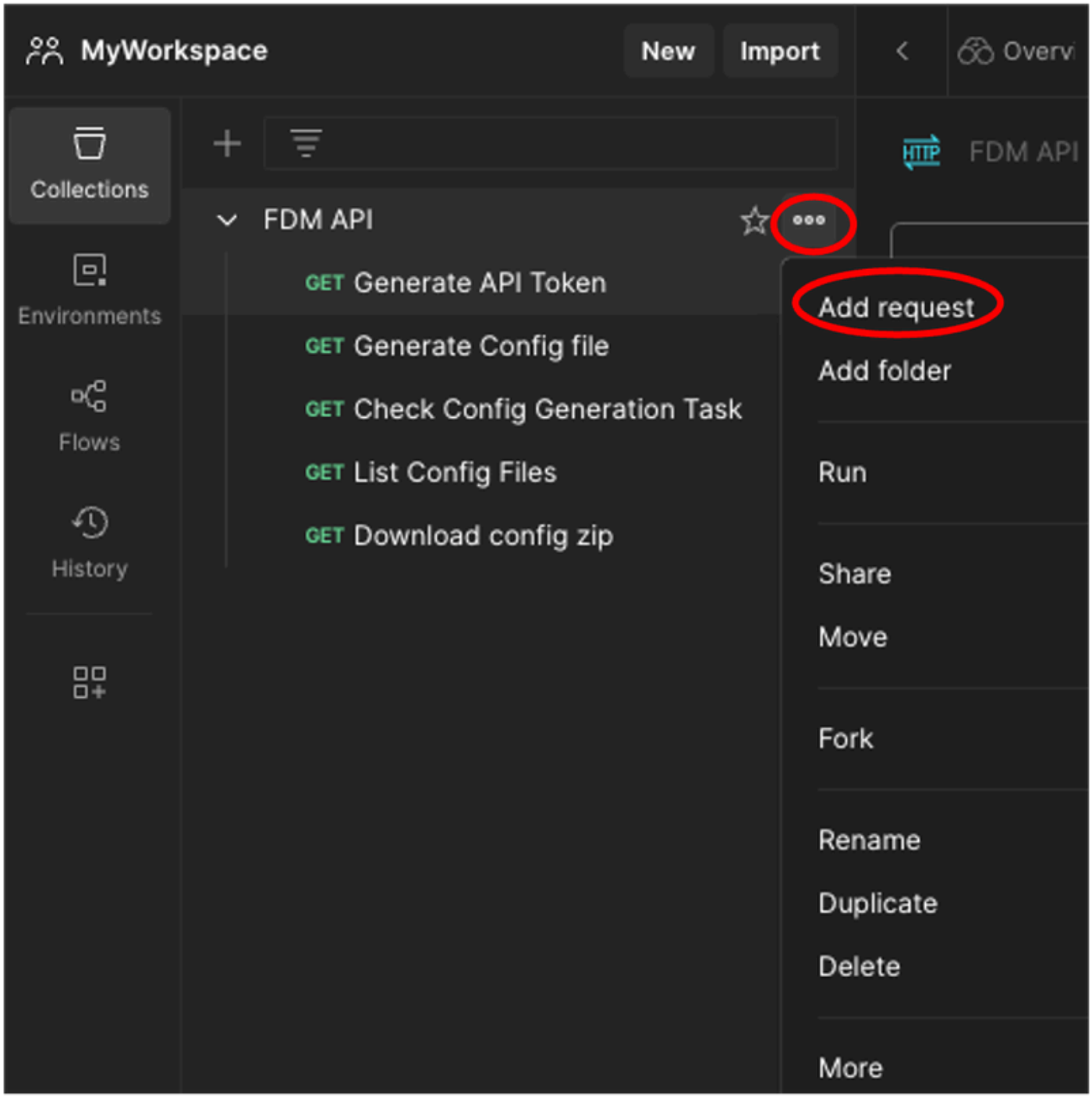


Advertencia: Al seleccionar este modo, sólo se permite migrar la política de control de acceso (ACP), la política de traducción de direcciones de red (NAT) y los objetos. En lo que respecta a los objetos, estos deben utilizarse en una regla ACP o NAT, para que se migren; de lo contrario, se ignoran.

Configuración

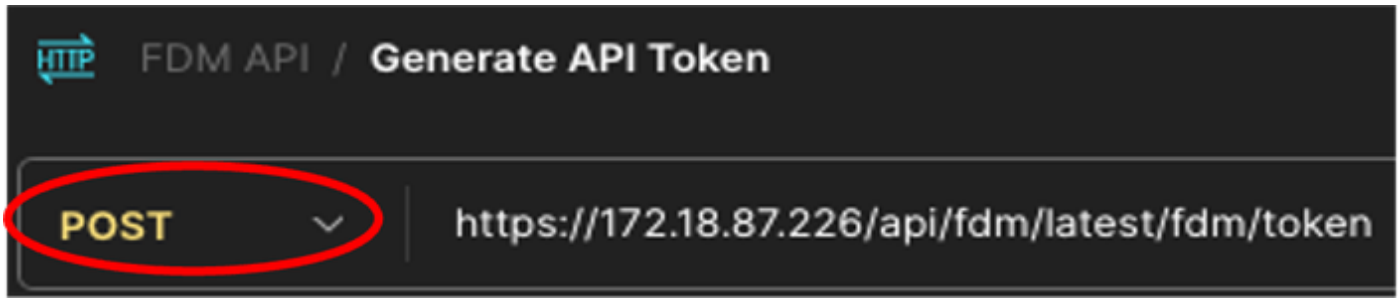
Solicitudes de API - Postman

1. En Postman, cree una nueva colección (en este escenario se utiliza la API de FDM).
2. Haga clic en los 3 puntos y después haga clic en Agregar solicitud.



Postman - Creación de colecciones y solicitud de adición

3. Llame a esta nueva solicitud: Generar token de API. Se va a crear como una solicitud GET, pero en el momento en que ejecute esta, POST debe seleccionarse en el menú desplegable. En el cuadro de texto situado junto a POST, introduzca la siguiente línea https://<FDM IP ADD>/api/fdm/latest/fdm/token



Postman - Solicitud de token

4. En la pestaña Cuerpo, seleccione la opción raw e introduzca las credenciales para acceder al dispositivo FTD (FDM) con este formato.

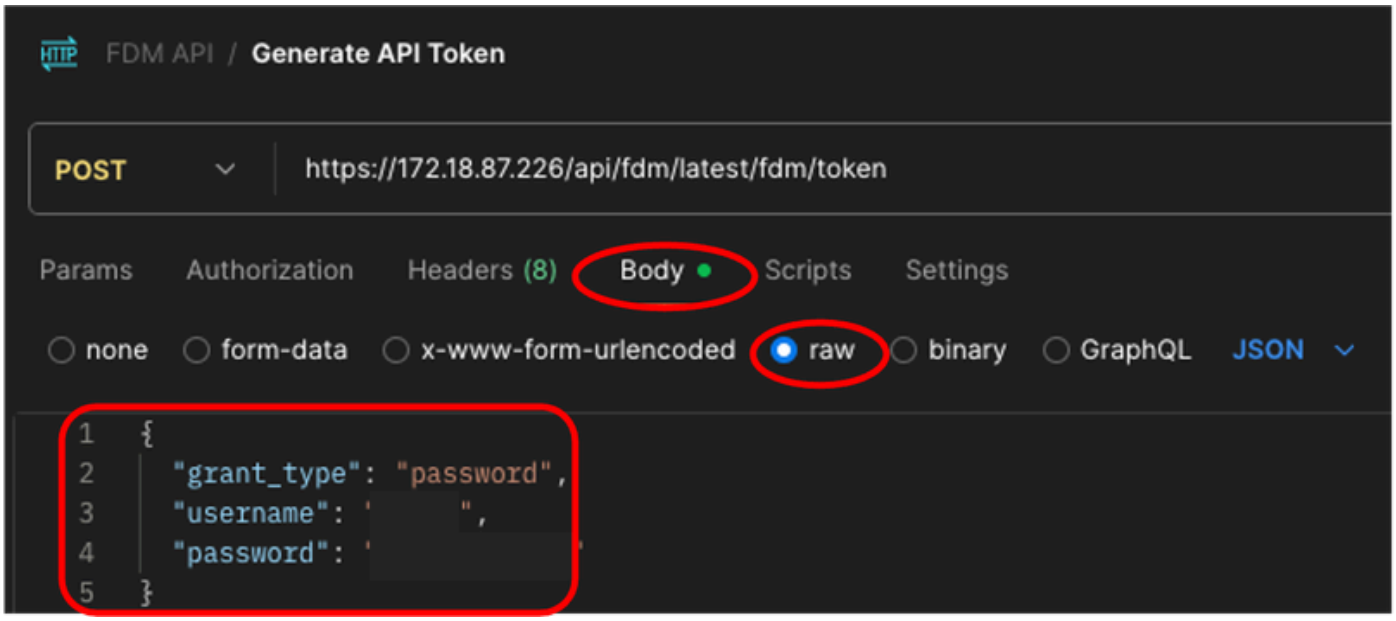
{

"grant_type": "contraseña",

"username": "username",

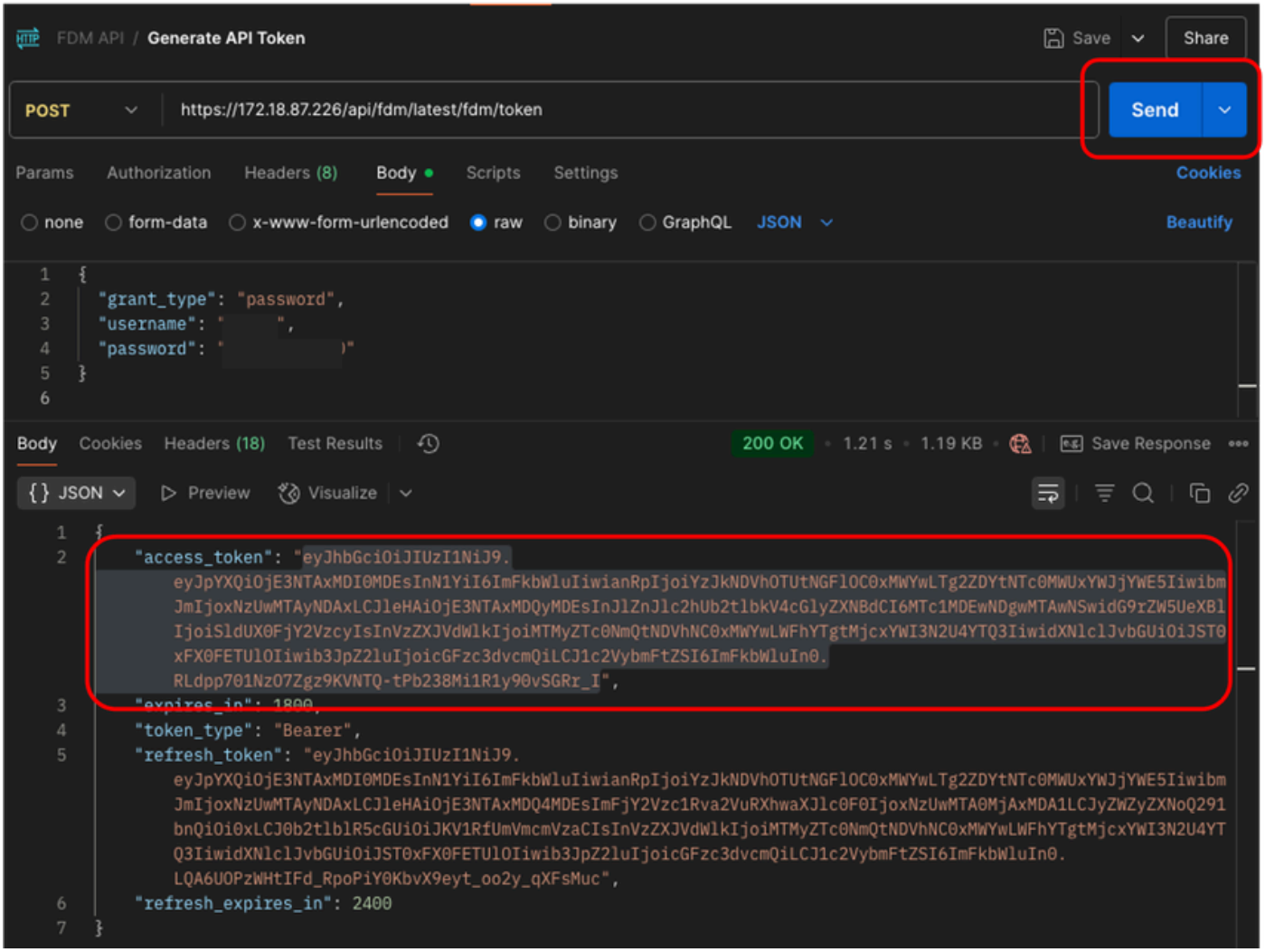
"contraseña": ”contraseña"

}



Postman - Cuerpo de solicitud de token

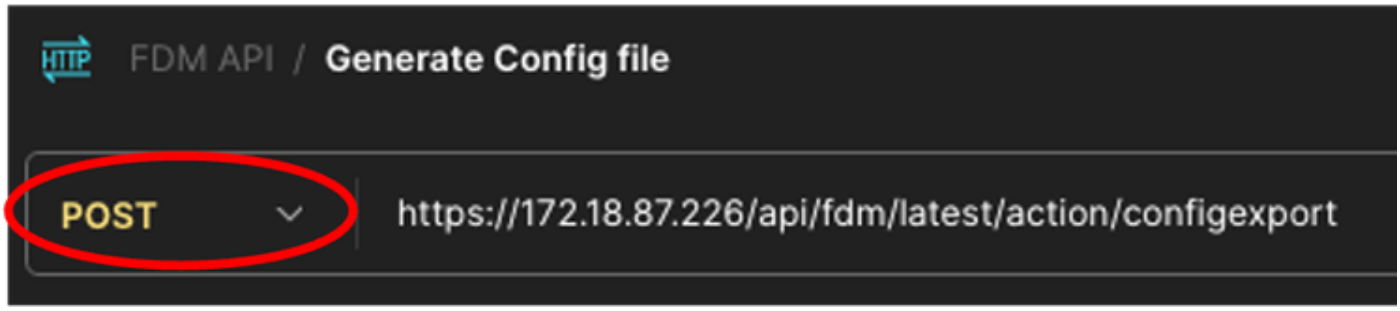
5. Finalmente, haga clic en Send para obtener su token de acceso. Si todo está bien, recibirá una respuesta de 200 OK. Haga una copia del token completo (entre comillas dobles) porque se va a utilizar en pasos posteriores.



Postman - Token Generado Correctamente

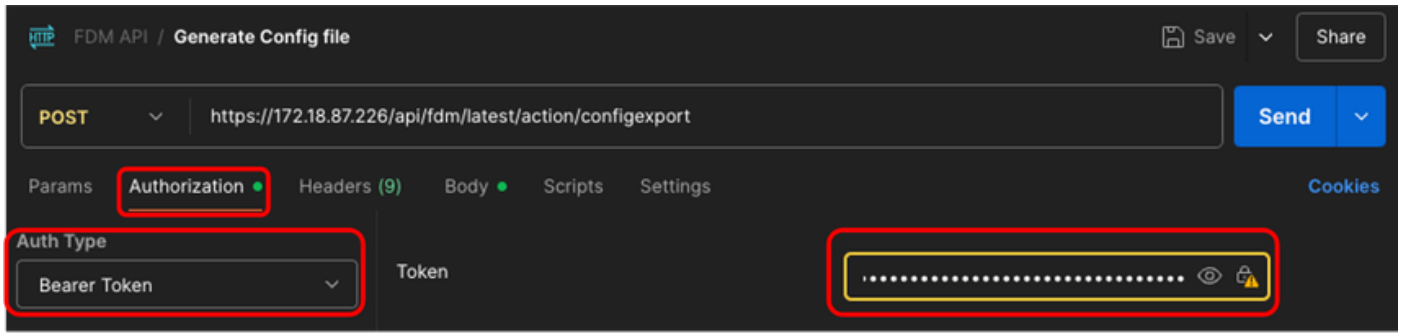
6. Repita el paso 2 para crear una nueva solicitud, POST se utilizará de nuevo.

7. Llame a esta nueva solicitud: Generar archivo de configuración. Se va a crear como una solicitud GET, pero en el momento en que ejecute esta, POST debe seleccionarse en el menú desplegable. En el cuadro de texto situado junto a POST, introduzca la siguiente línea https://<FDM IP ADD>/api/fdm/latest/action/configexport



Postman - Generar solicitud de archivo de configuración

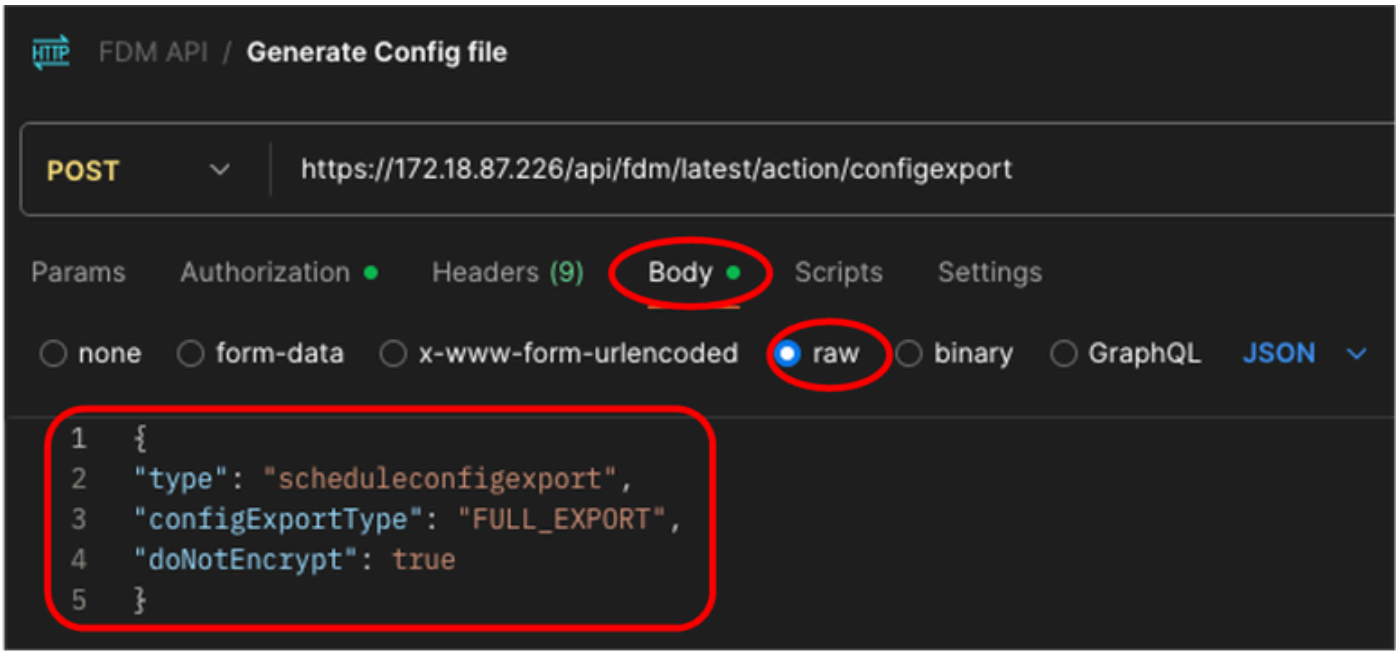
8. En la pestaña Authorization, seleccione Bearer Token as Auth Type en el menú desplegable, y en el cuadro de texto junto a Token pegue el token copiado en el paso 5.



Postman - Generar solicitud de archivo de configuración - Autorización

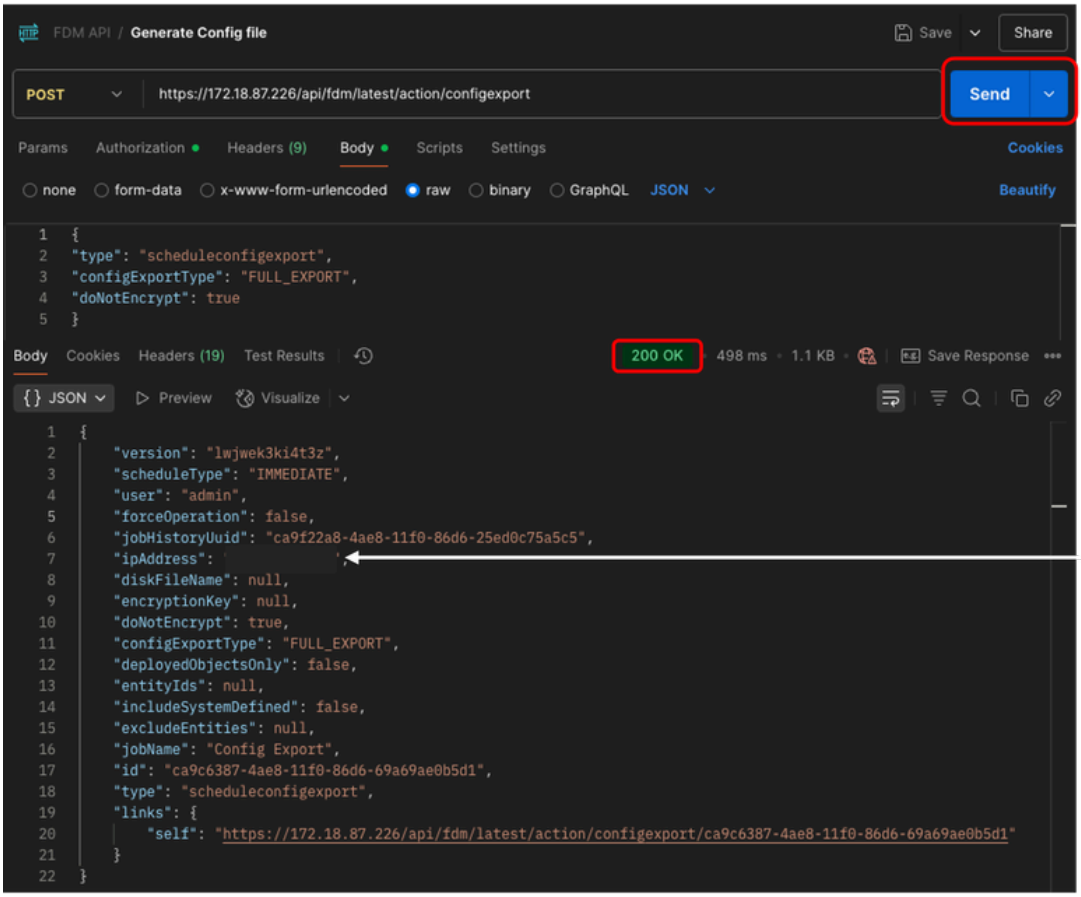
9. En la pestaña Cuerpo, seleccione la opción raw e introduzca esta información.

```
{
  "tipo": "scheduleconfigexport",
  "configExportType": "FULL_EXPORT",
  "doNotEncrypt": verdadero
}
```



Postman - Generar solicitud de archivo de configuración - Cuerpo

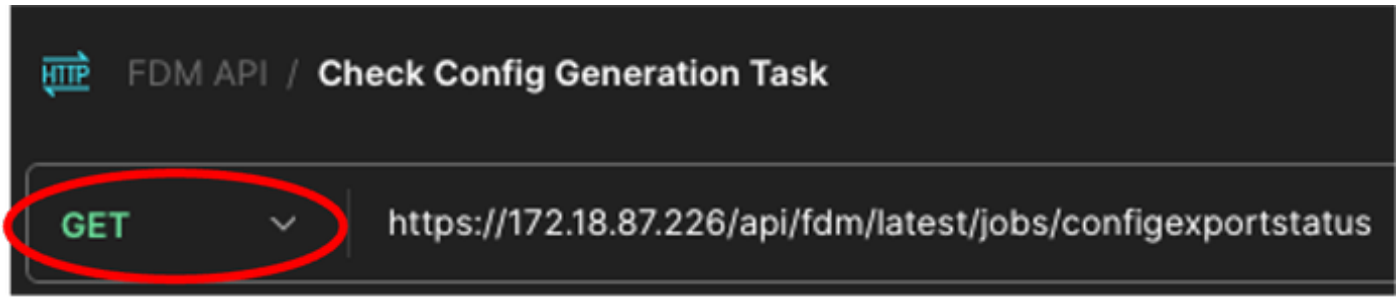
10. Por último, haga clic en Enviar. Si todo está bien, recibirá una respuesta de 200 OK.



Postman - Generar solicitud de archivo de configuración - Salida

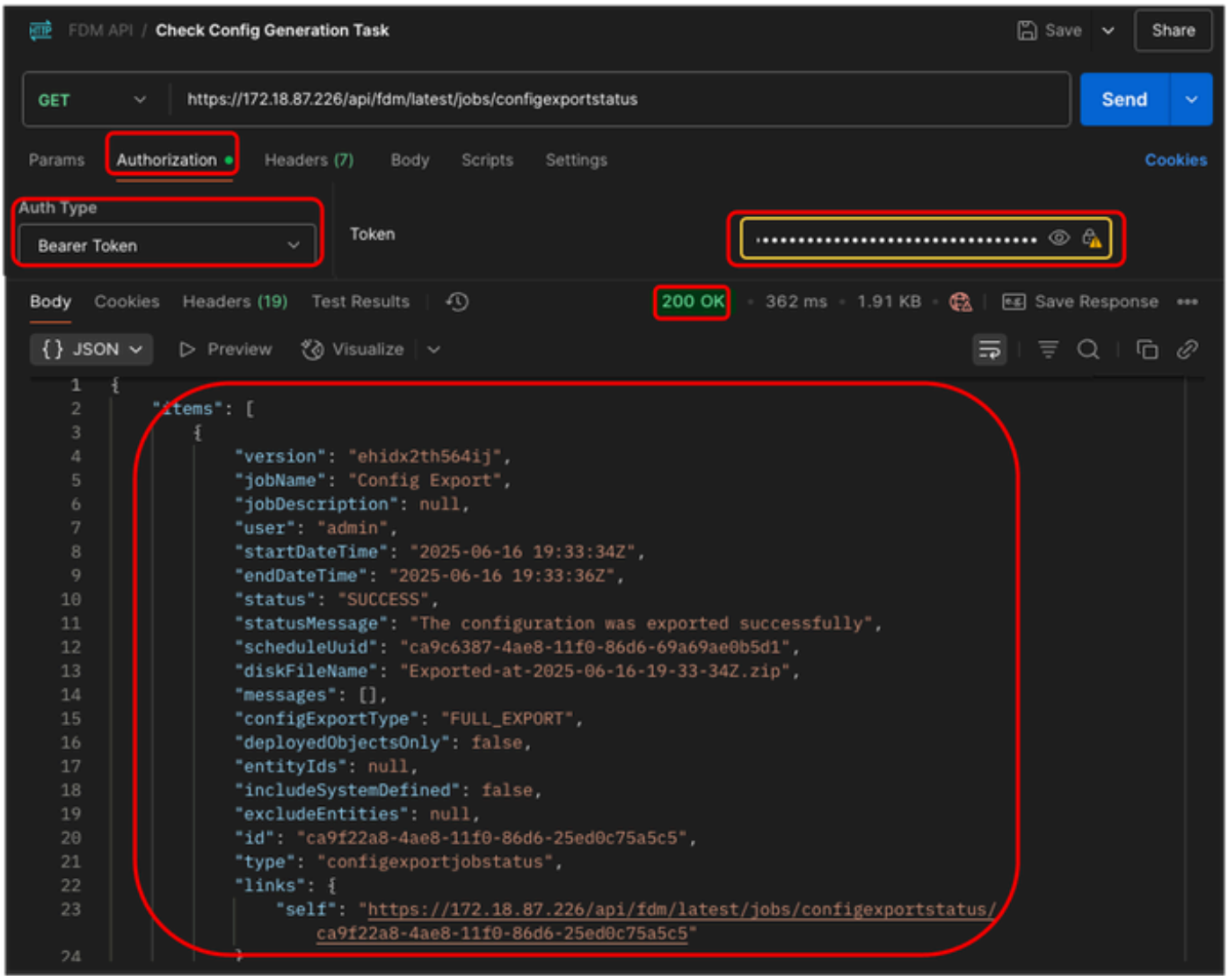
11. Repita el paso 2 para crear una nueva solicitud. GET se va a utilizar esta vez.

12. Llame a esta nueva solicitud: Marque Config Generation Task. Se va a crear como una solicitud GET. Además, la hora a la que está ejecutando este, GET debe seleccionarse en el menú desplegable. En el cuadro de texto situado junto a GET, introduzca la siguiente línea https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus



Postman - Comprobar solicitud de estado de exportación de configuración

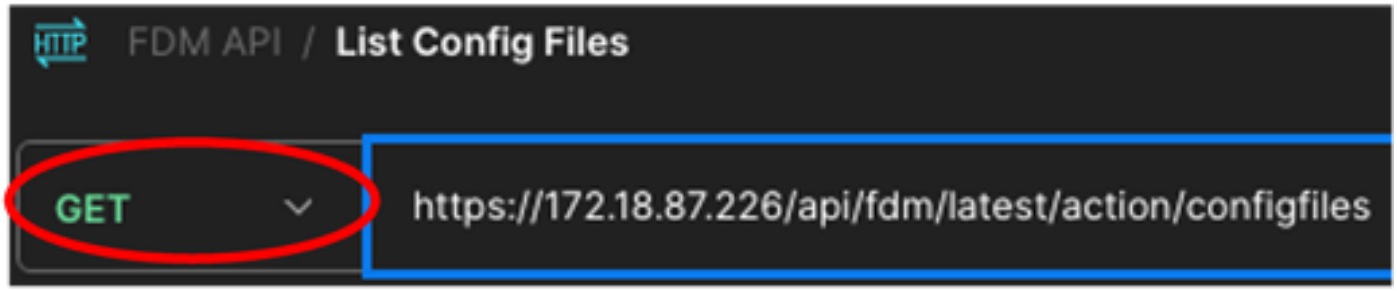
13. En la pestaña Authorization, seleccione Bearer Token as Auth Type en el menú desplegable, y en el cuadro de texto junto a Token pegue el token copiado en el paso 5. Finalmente, haga clic en Send. Si todo está bien, recibirá una respuesta de 200 OK y en el campo JSON se puede ver el estado de la tarea y otros detalles.



Postman - Solicitud de estado de exportación de configuración - Autorización y salida

14. Repita el paso 2 para crear una nueva solicitud; esta vez se utilizará GET.

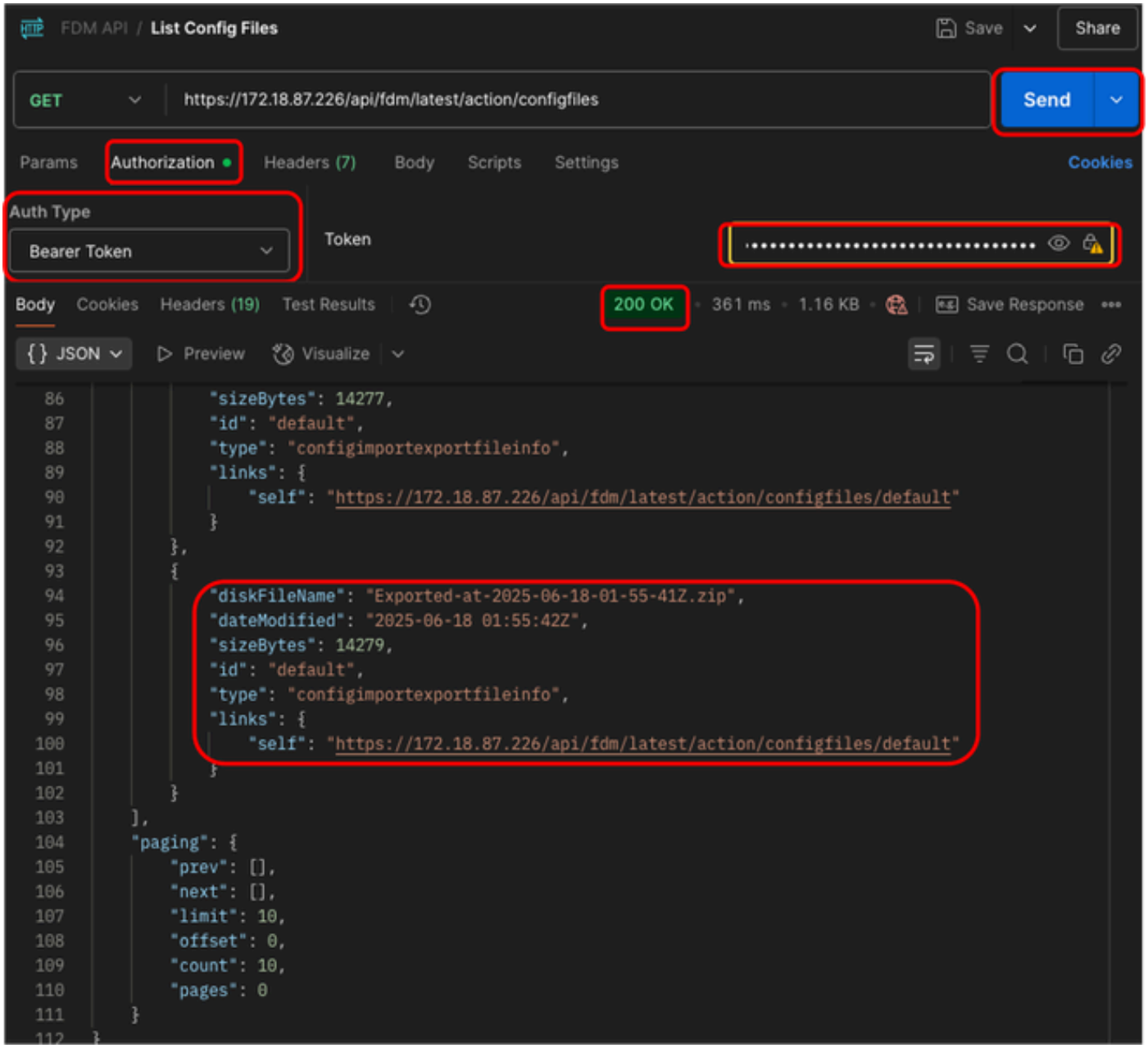
15. Llame a esta nueva solicitud: Enumera los archivos de configuración. Se va a crear como una solicitud GET; también en el momento en que ejecute esta solicitud, se debe seleccionar GET en el menú desplegable. En el cuadro de texto situado junto a GET, introduzca la siguiente línea https://<FDM IP ADD>/api/fdm/latest/action/configfiles



Postman - Solicitud de lista de archivos de configuración exportados

16. En la pestaña Authorization, seleccione Bearer Token as Auth Type en el menú desplegable, y en el cuadro de texto junto a Token pegue el token copiado en el paso 5. Finalmente, haga clic

en Send. Si todo está bien, recibirá una respuesta 200 OK y en el campo JSON, se mostrará la lista de los archivos exportados. El más reciente aparece en la parte inferior. Copie el último nombre de archivo (fecha más reciente en el nombre de archivo) porque se va a utilizar en el último paso.



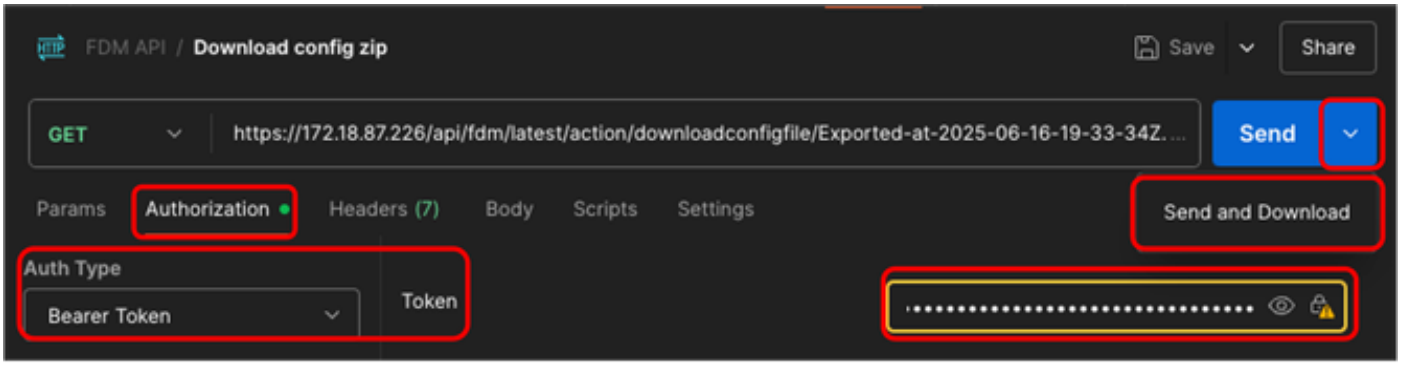
Postman - Solicitud de lista de archivos de configuración exportados - Autorización y salida

17. Repita el paso 2 para crear una nueva solicitud; esta vez se utilizará GET.

18. Llame a esta nueva solicitud: Descargar config zip. Se va a crear como una solicitud GET; también en el momento en que ejecute esta solicitud, se debe seleccionar GET en el menú desplegable. En el cuadro de texto situado junto a GET, introduzca la siguiente línea y pegue al final el nombre de archivo que copió en el paso 16. https://<FDM IP ADD>/api/fdm/latest/action/downloadconfigfile/<Exported_File_name.zip >

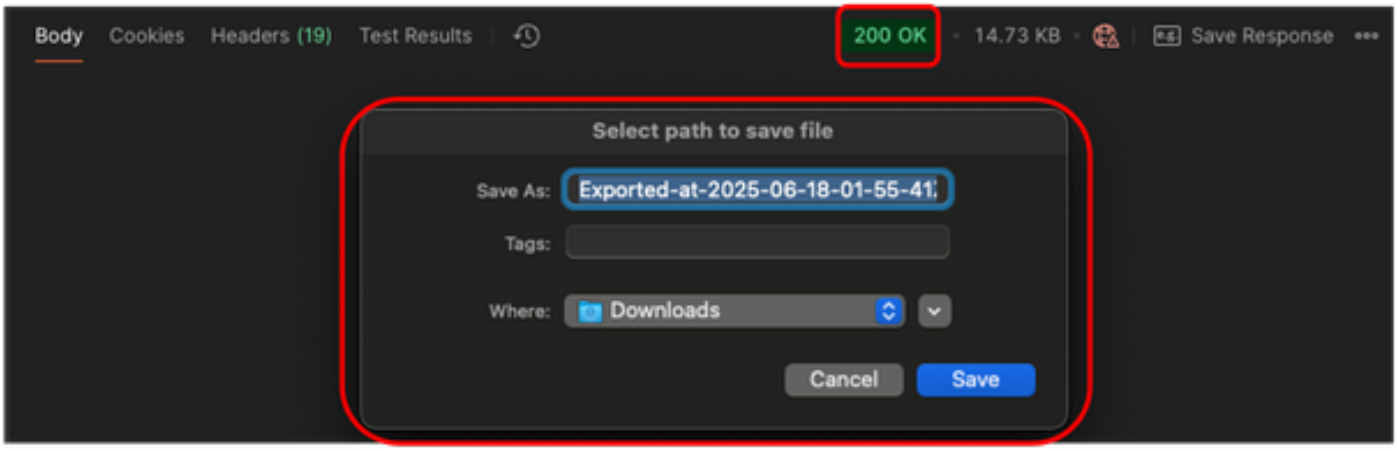
Postman - Descargar solicitud de archivo Config.zip

19. En la ficha Authorization, seleccione Bearer Token as Auth Type en el menú desplegable y, en el cuadro de texto situado junto a Token, pegue el token copiado en el paso 5. Por último, haga clic en la flecha hacia abajo junto a Send y seleccione Send and Download.



Postman - Descargar solicitud de archivo Config.zip - Autorización

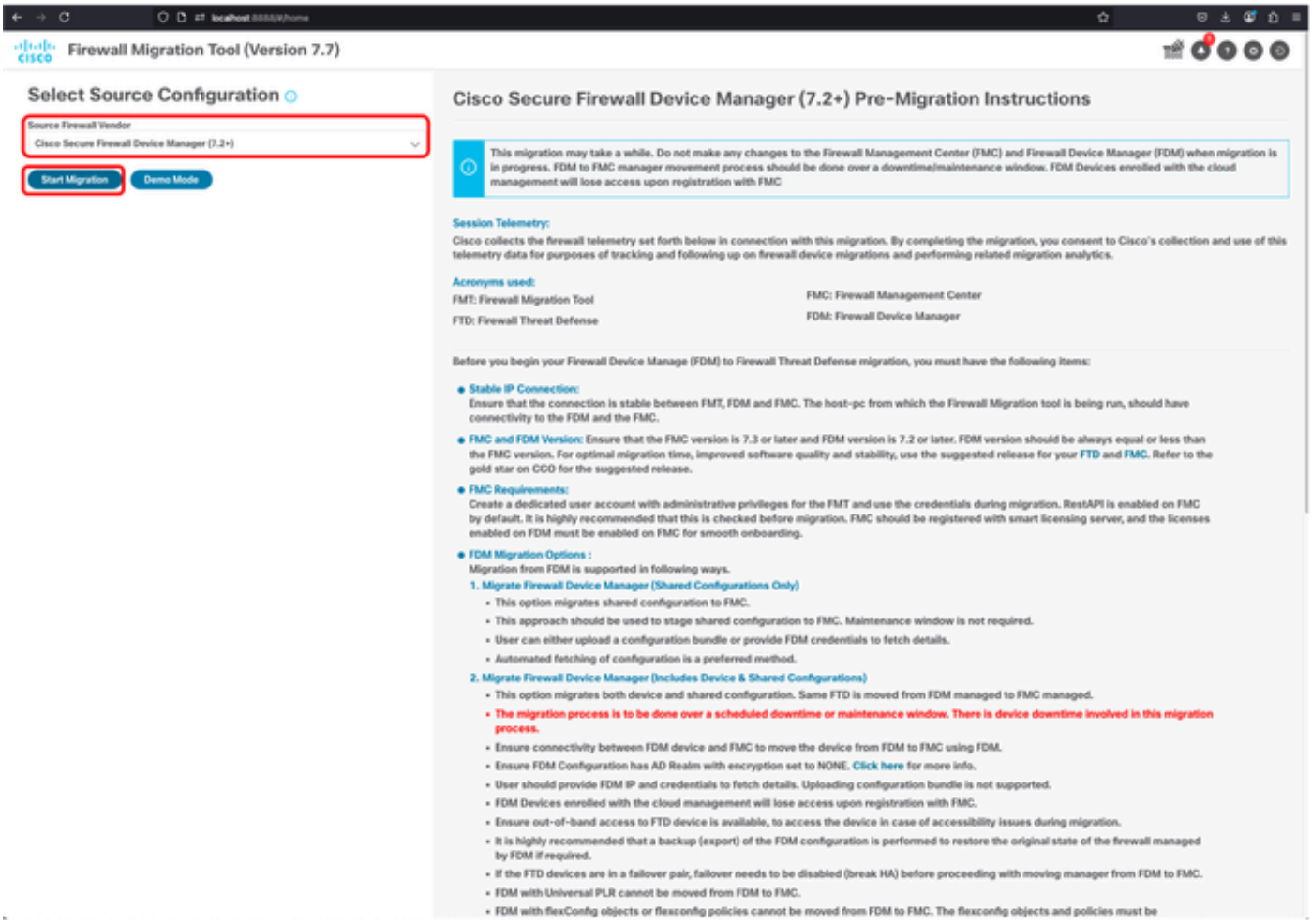
20. Si todo está bien, recibirá una respuesta de 200 OK y se mostrará una ventana emergente solicitando la carpeta de destino donde se guardará el archivo configuration.zip. Este archivo .zip se puede cargar ahora en la herramienta de migración del firewall.



Postman - Descargar solicitud de archivo Config.zip - Guardar

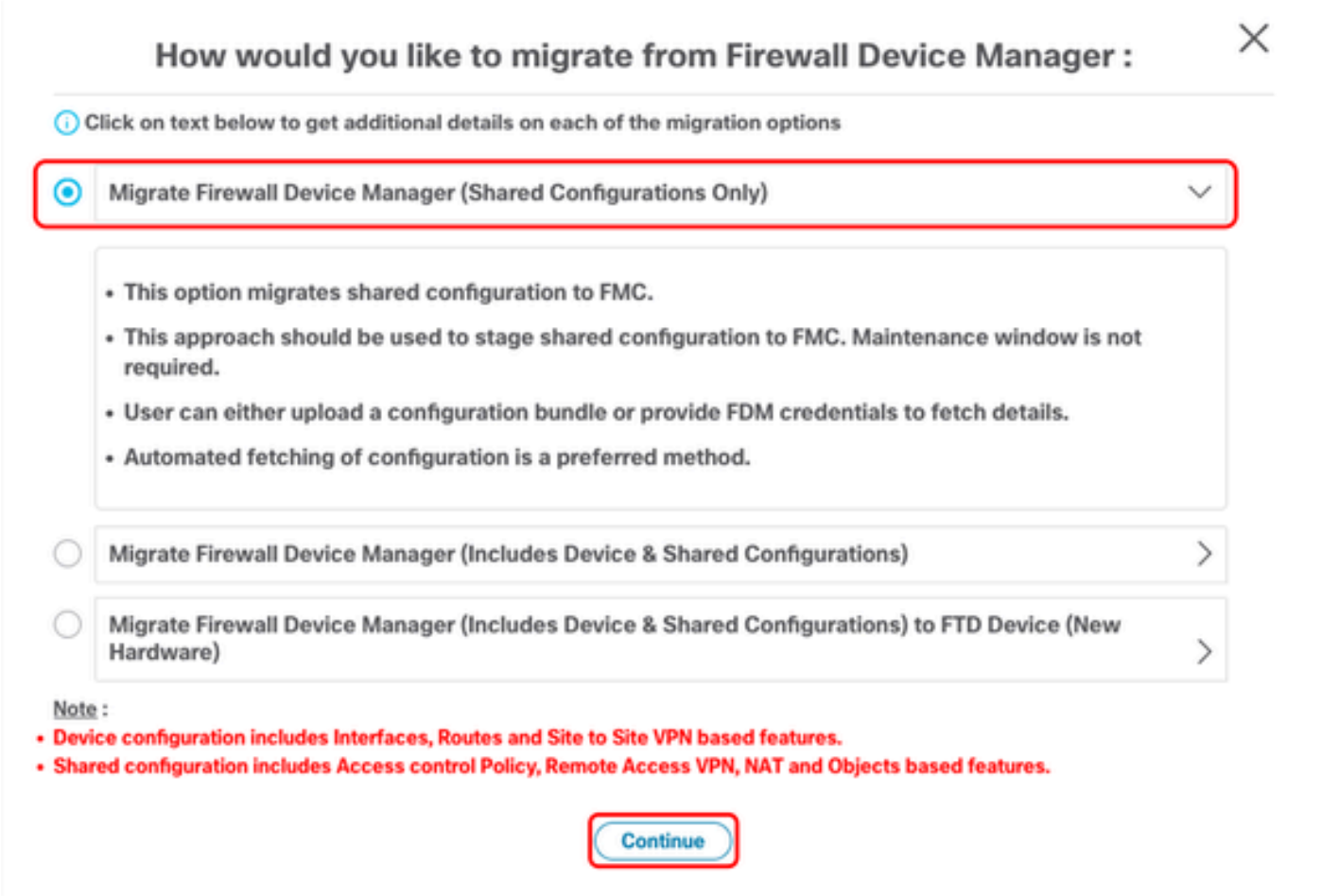
Herramienta de migración de firewall

21. Abra Firewall Migration Tool y, en el menú desplegable Select Source Configuration, seleccione Cisco Secure Firewall Device Manager (7.2+) y haga clic en Start Migration.



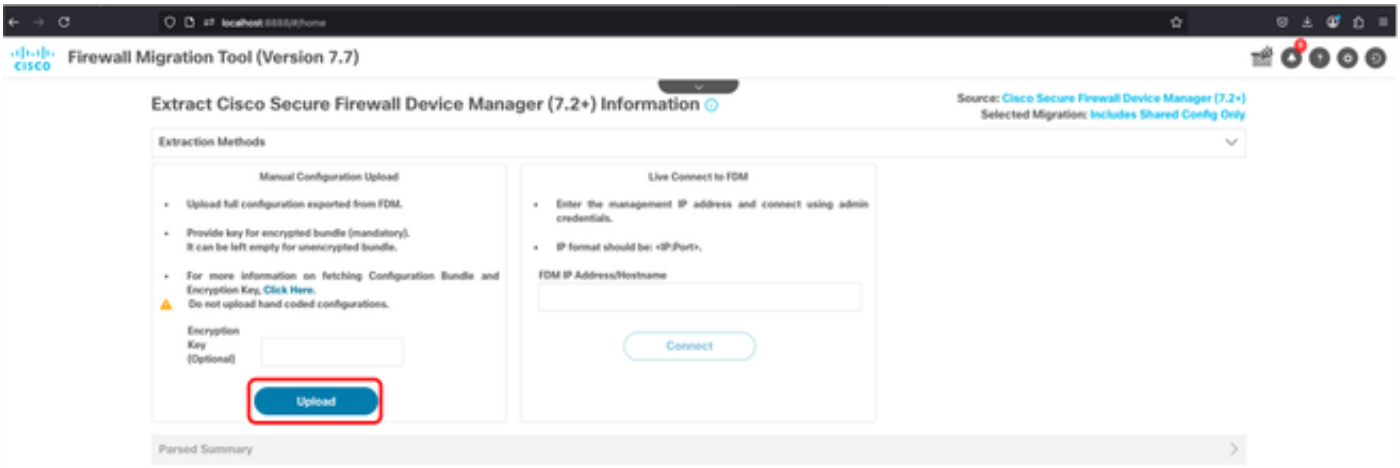
FMT - Selección de FDM

22. Marque primero el botón de opción Migrate Firewall Device Manager (Shared Configurations Only) y haga clic en Continue.



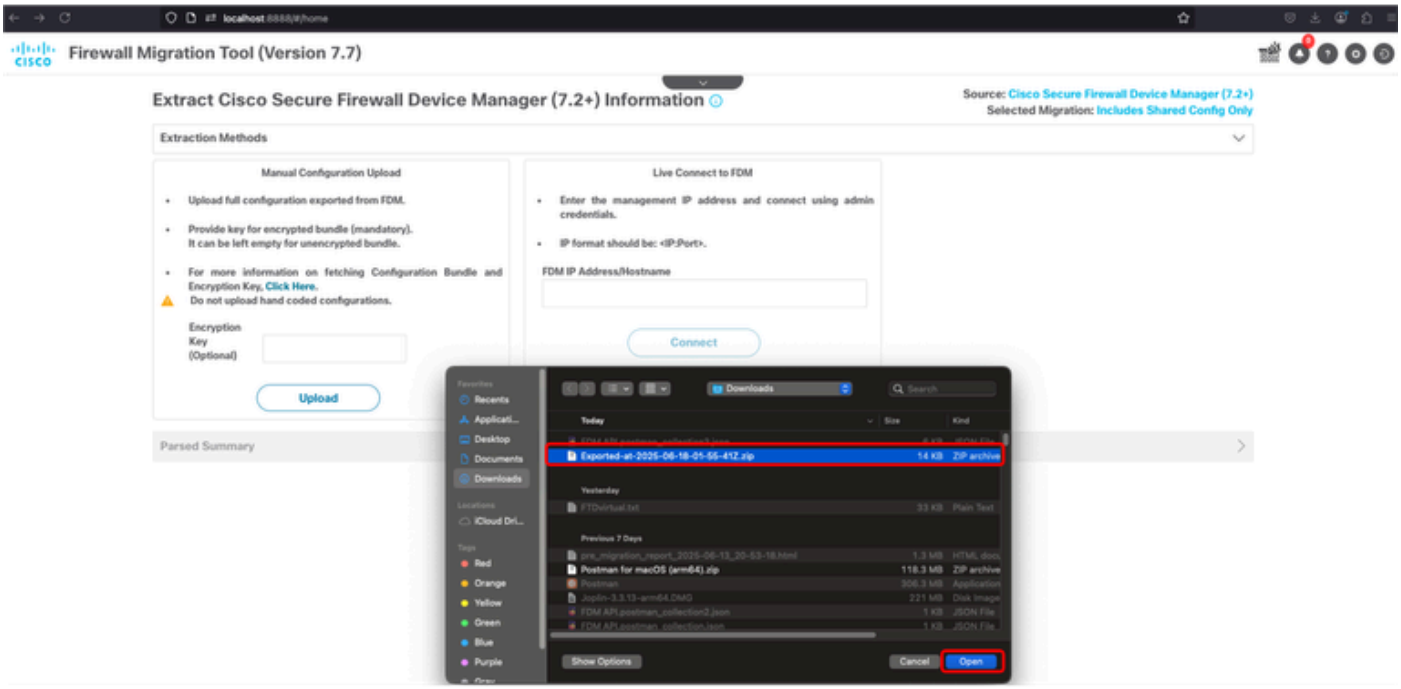
FMT - Sólo configuraciones compartidas de migración a FDM

23. En el panel izquierdo (Carga de configuración manual), haga clic en Cargar.



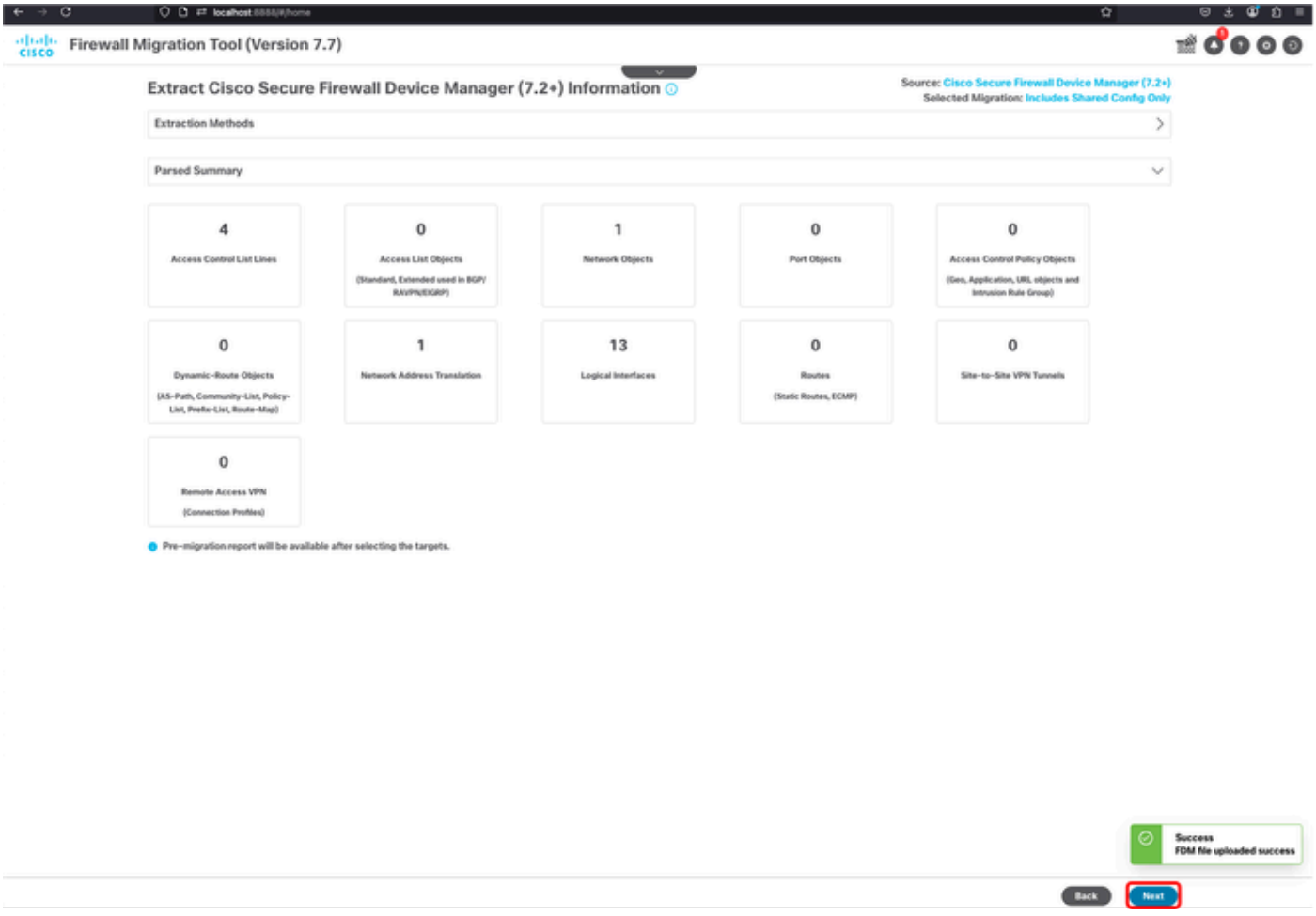
FMT - Cargar archivo Config.zip

24. Seleccione el archivo zip config exportado en la carpeta que guardó anteriormente y haga clic en Abrir.



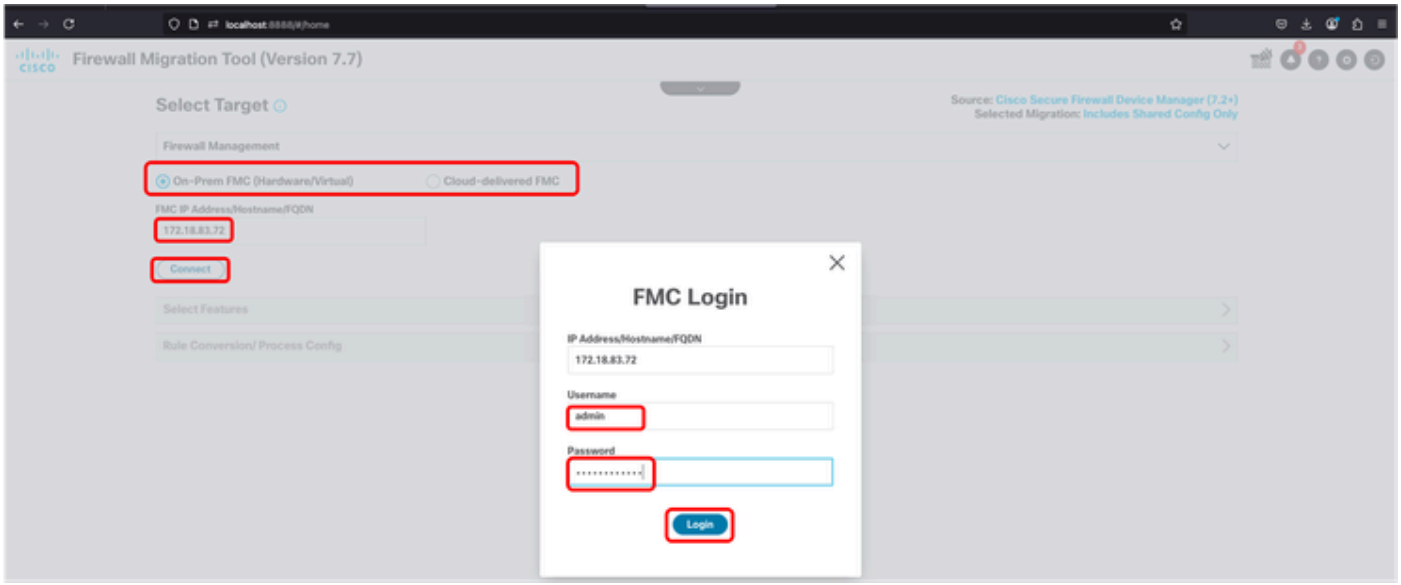
FMT - Selección de archivo Config.zip

25. Si todo va como se espera, se muestra el Resumen analizado. Además, en la esquina inferior derecha se puede ver una ventana emergente que informa de que el archivo de FDM se ha cargado correctamente. Haga clic en Next (Siguiente).



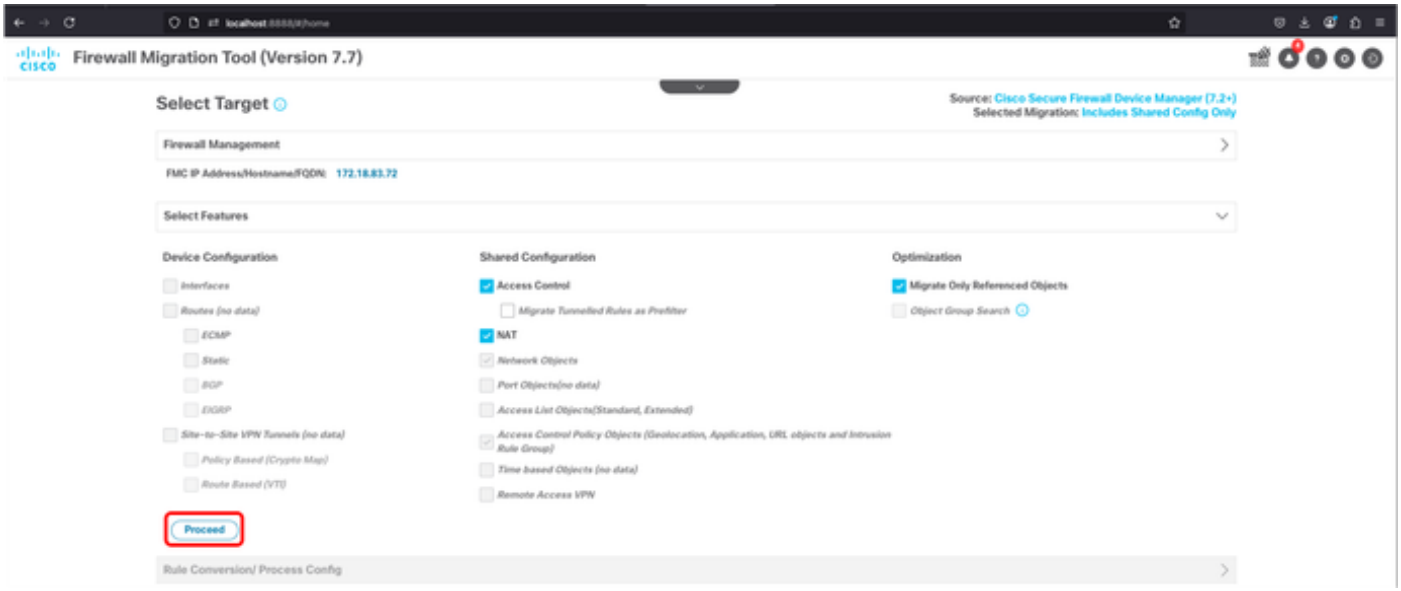
FMT - Resumen de análisis

26. Marque la opción que mejor se adapte a su entorno (FMC en las instalaciones o Cd-FMC). En esta situación, se utiliza un FMC en las instalaciones. Escriba la dirección IP del CSP y haga clic en Conectar. Aparece una nueva ventana emergente en la que se solicitan las credenciales de FMC. Después de introducir esta información, haga clic en Iniciar sesión.



FMT: inicio de sesión en FMC Target

27. La siguiente pantalla muestra el CSP de destino y las funciones que se van a migrar. Haga clic en Proceed.

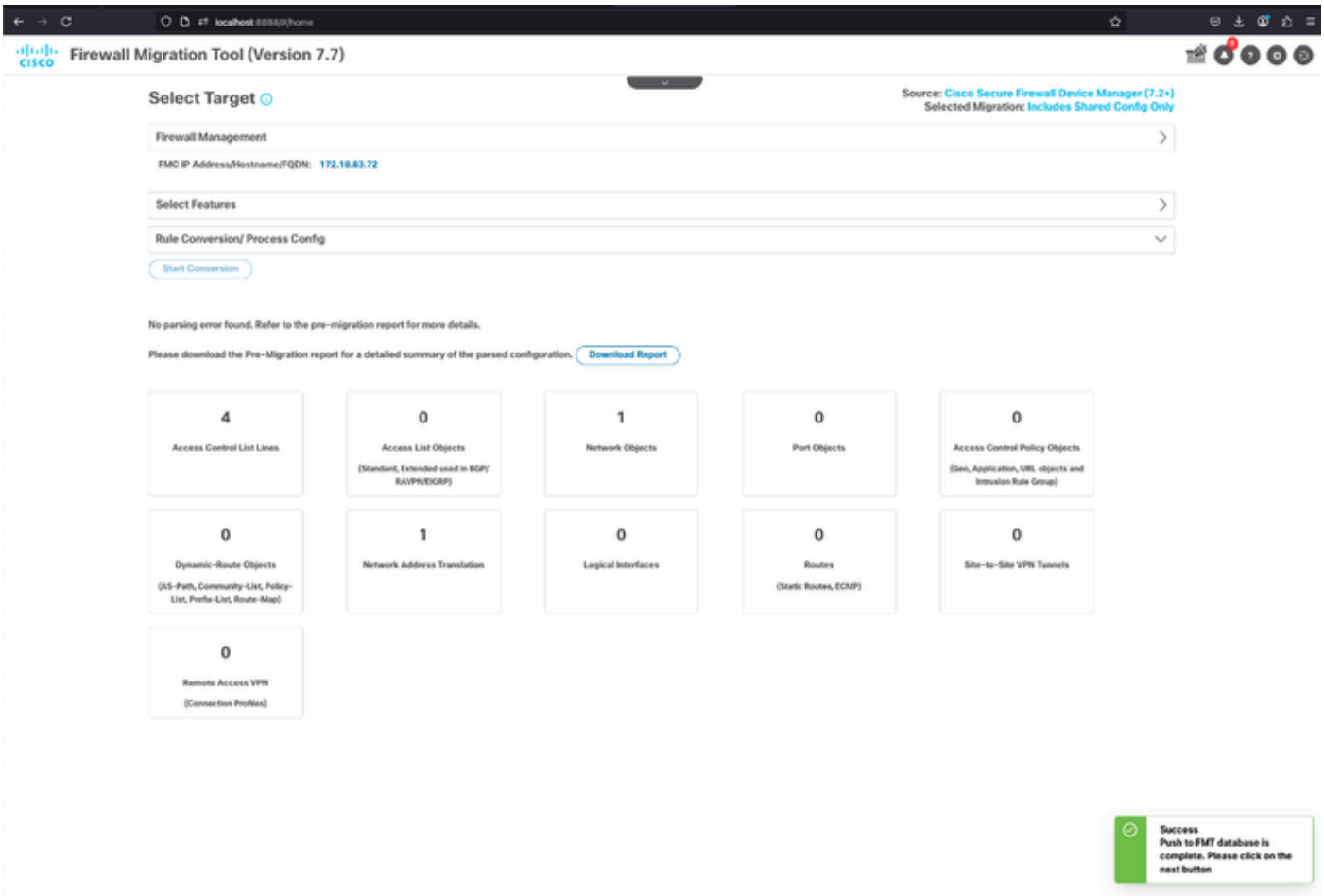


FMT - Objetivo de FMC - Selección de características

28. Una vez confirmado el objetivo de FMC, haga clic en el botón Start Conversion.

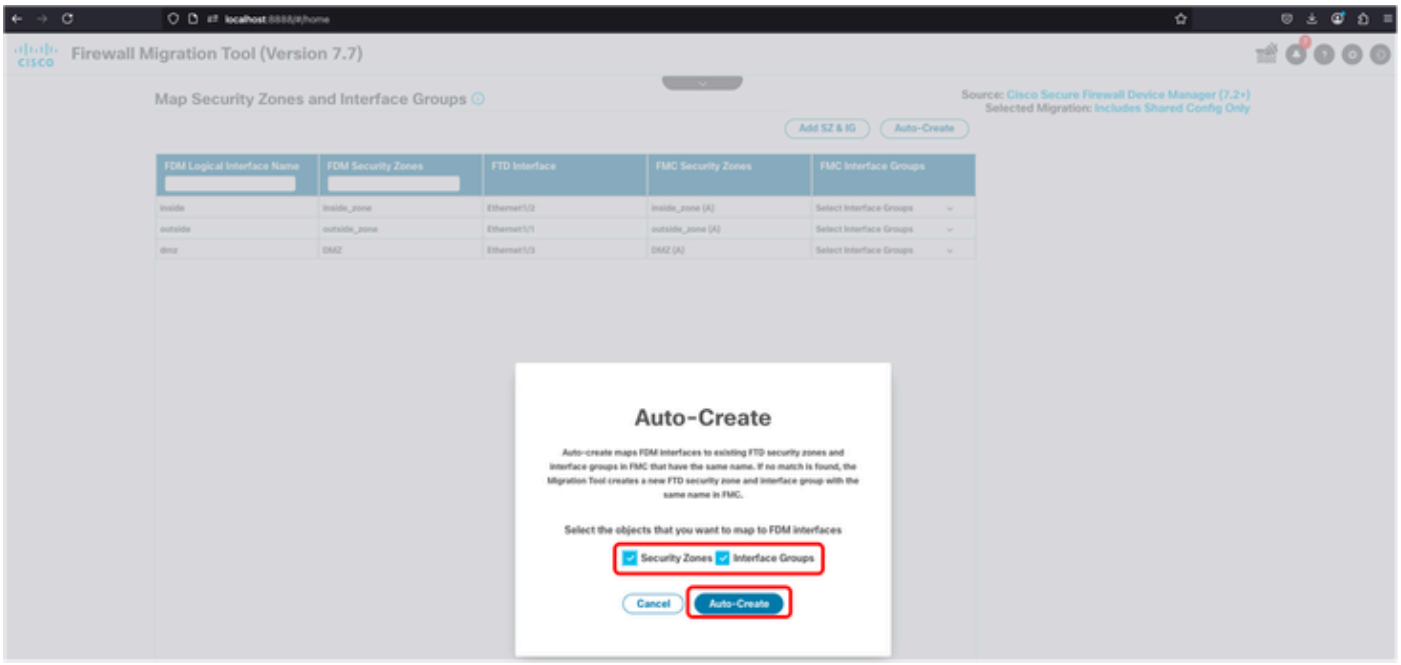
FMT: iniciando conversión de configuración

29. Si todo va como se espera, se muestra una ventana emergente en la esquina inferior derecha que informa de que la transferencia a la base de datos de FMT está completa. Haga clic en Next (Siguiente).



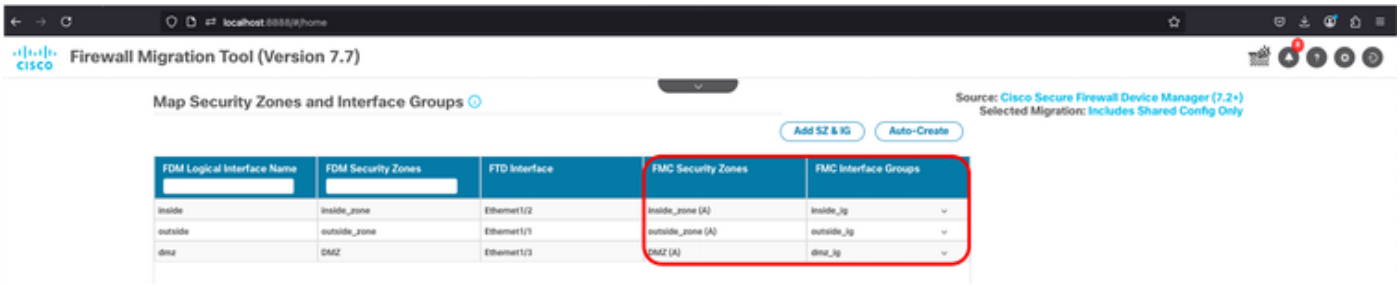
FMT: inserción de base de datos completada correctamente

30. En la siguiente pantalla, debe crear o seleccionar manualmente las zonas de seguridad y los grupos de interfaces. En este escenario, se utiliza la creación automática.



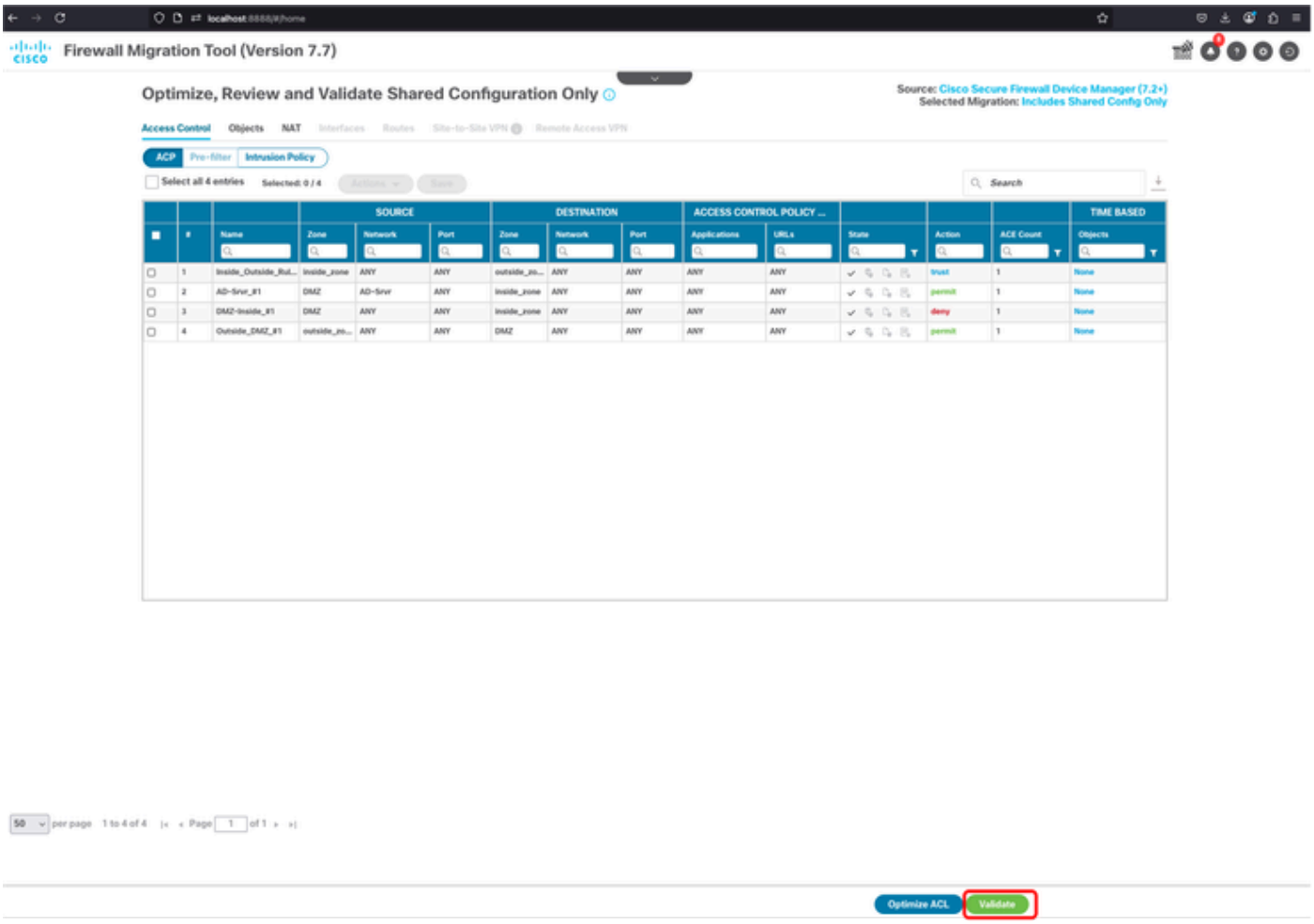
FMT - Creación automática de zonas de seguridad y grupos de interfaces

31. Una vez terminado, el cuadro muestra en la cuarta y quinta columnas la zona de seguridad y el grupo de interfaces, respectivamente.



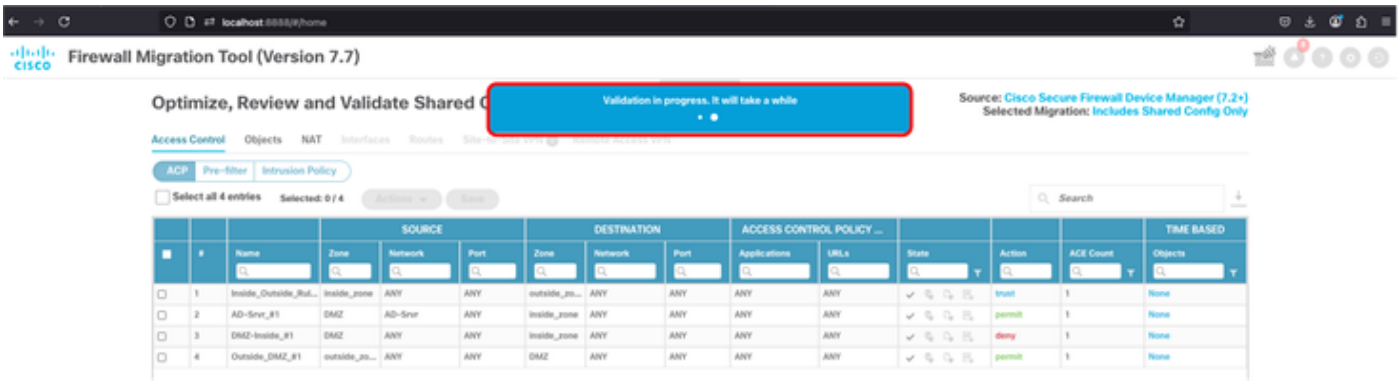
FMT - Zonas de seguridad y grupos de interfaz creados correctamente

32. En la siguiente pantalla, puede optimizar ACL o simplemente validar ACP, Objetos y NAT. Una vez hecho, haga clic en el botón Validar.



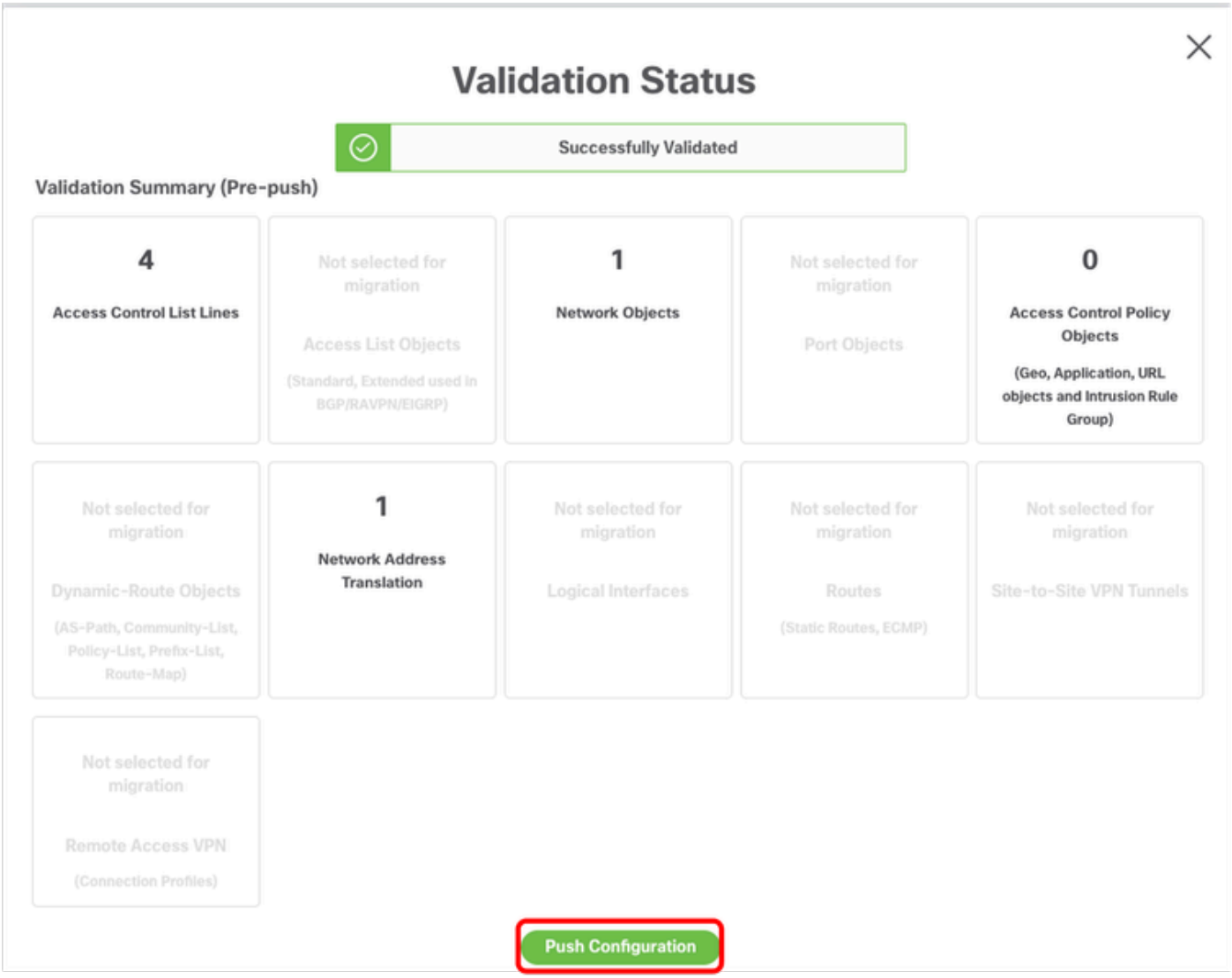
FMT - Optimizar ACL - Validar migración

33. La validación tardará un par de minutos en completarse.



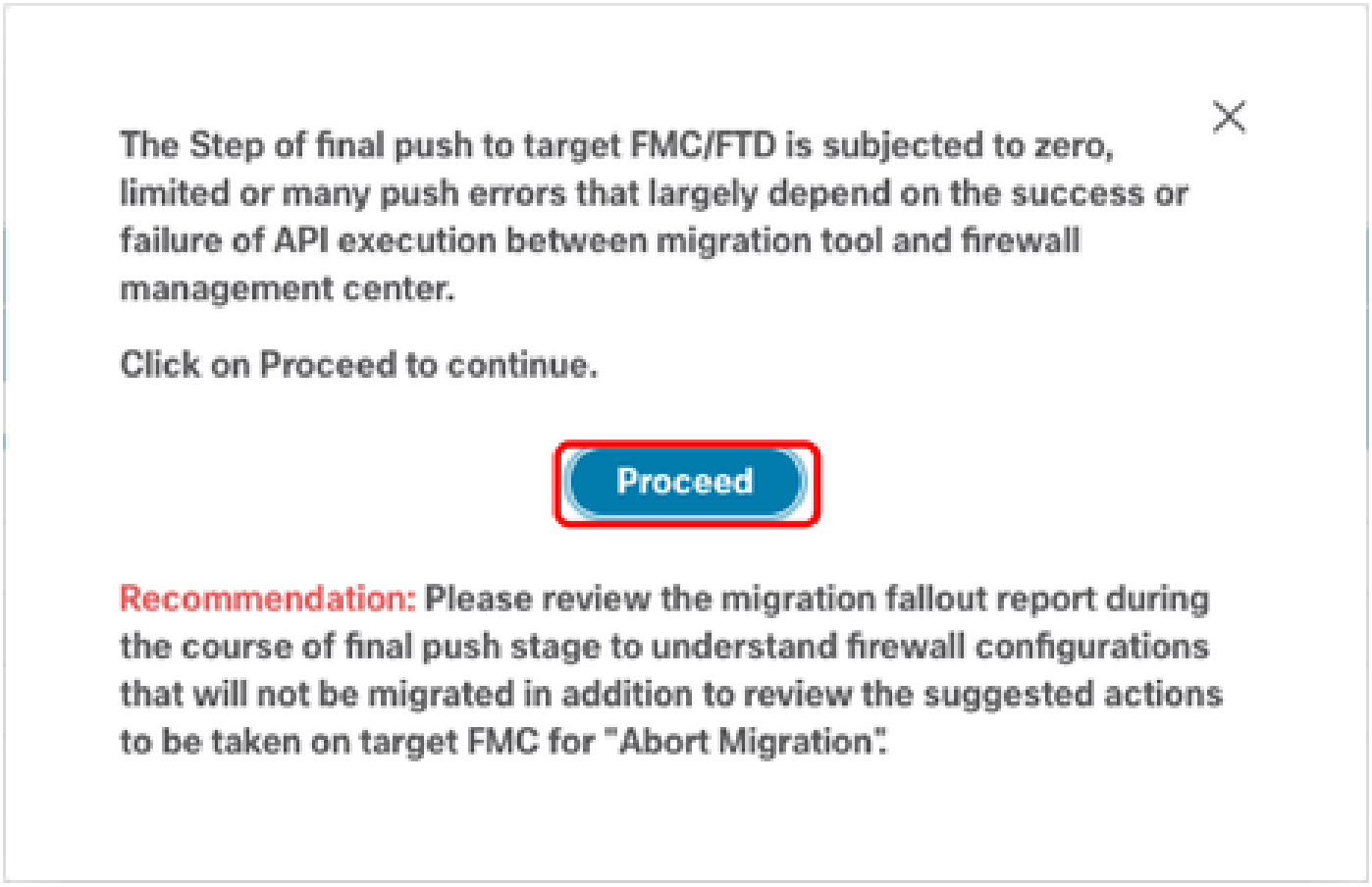
FMT - Validación en curso

34. Una vez hecho esto, FMT le permite saber que la configuración se ha validado correctamente y el siguiente paso es hacer clic en el botón Push Configuration.



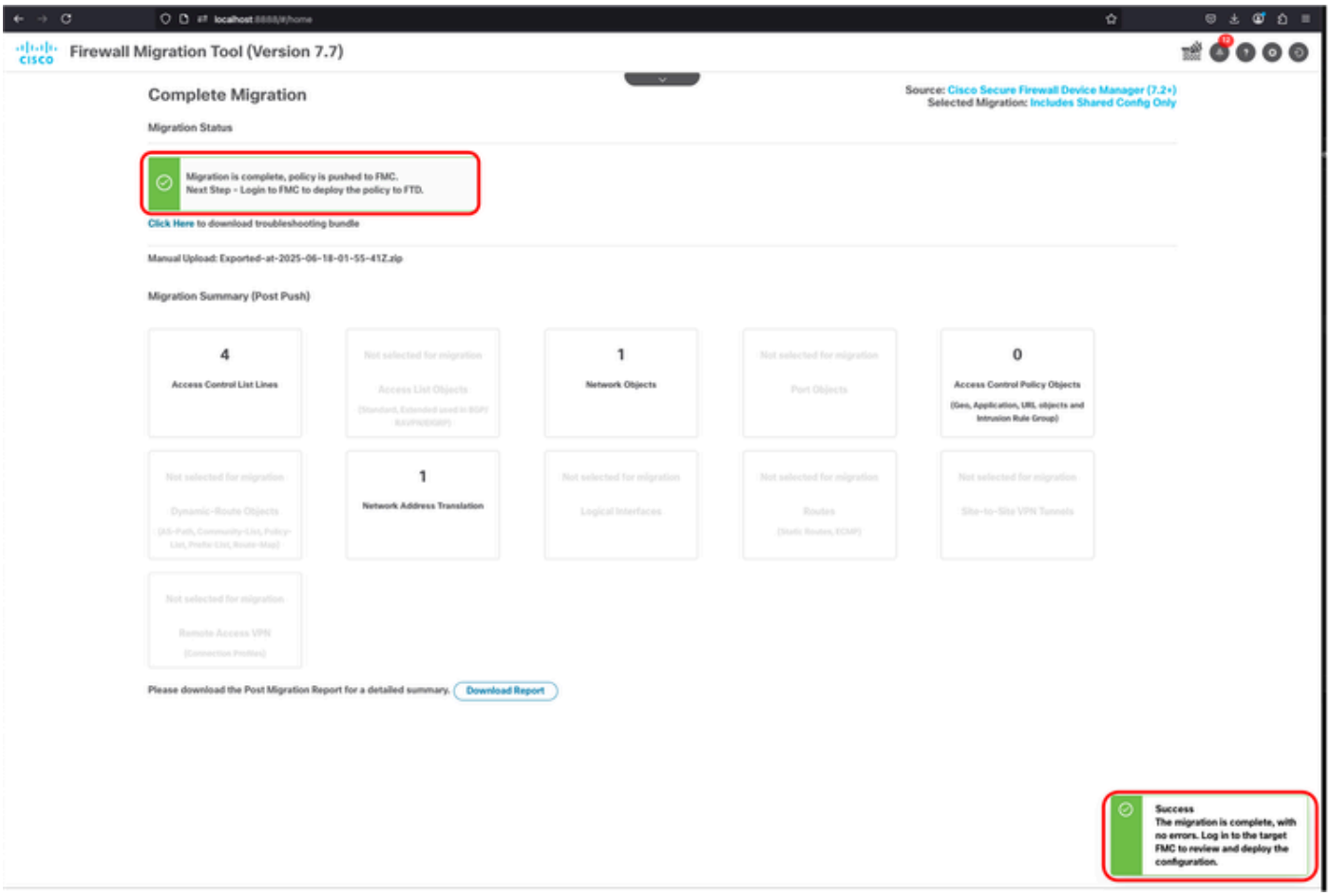
FMT - Validación realizada correctamente - Envío de la configuración a FMC

35. Por último, haga clic en el botón Proceed.



FMT: continuar con la inserción de configuración

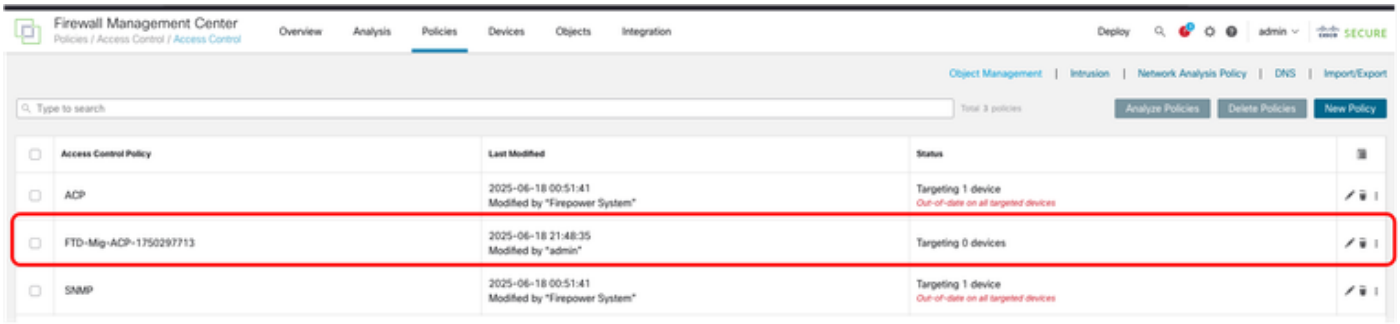
36. Si todo va como se espera, se muestra la notificación de migración correcta. FMT le solicita que inicie sesión en FMC e implemente la política migrada en FTD.



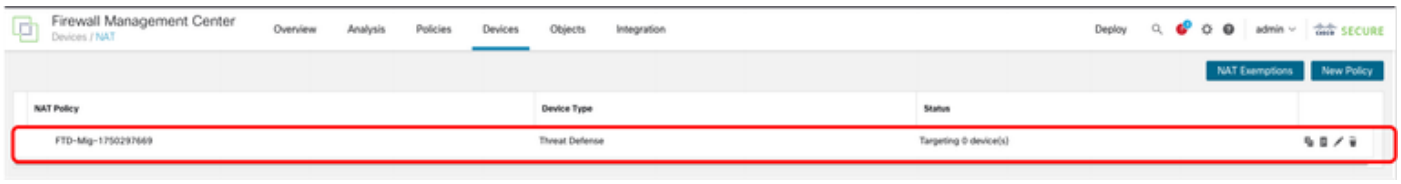
FMT: notificación de migración correcta

Verificación de FMC

37. Después de iniciar sesión en FMC, las políticas ACP y NAT se muestran como FTD-Mig. Ahora puede continuar con la implementación del nuevo FTD.



FMC - ACP migrado



FMC - Política NAT migrada

Información Relacionada

- FMT: Guía de migración de FDM a FMC
- Notas de la versión de FMT

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).