

Migrar FDM para FMC por meio do FMT usando o arquivo Configuration.zip

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Considerações](#)

[Configuração](#)

[Solicitações de API - Postman](#)

[Ferramenta de migração de firewall](#)

[Verificação do FMC](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como gerar o arquivo de configuração.zip de um Gerenciador de dispositivos de firewall seguro (FDM) a ser migrado para um FMC usando o FMT.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defesa contra ameaças (FTD) do firewall da Cisco
- Cisco Firewall Management Center (FMC)
- Ferramenta de migração de firewall (FMT)
- Plataforma de API Postman

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software.

FTD 7.4.2

CVP 7.4.2

FMT 7.7.0.1

Postman 11.50.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

- O FDM agora pode ser migrado para o FMC de diferentes maneiras. Neste documento, o cenário que será explorado é a geração do arquivo .zip de configuração usando solicitações de API e o carregamento posterior desse arquivo para o FMT para migrar a configuração para o FMC.
- As etapas mostradas neste documento começam a usar o Postman diretamente, portanto, é recomendável que você já tenha o Postman instalado. O PC ou laptop que você vai usar deve ter acesso ao FDM e ao FMC, e o FMT também deve estar instalado e em execução.

Considerações

- Este documento se concentra na geração do arquivo .zip de configuração mais do que no uso FMT.
- A migração do FDM usando o arquivo de configuração .zip é para migrações não dinâmicas e não requer imediatamente um FTD de destino.

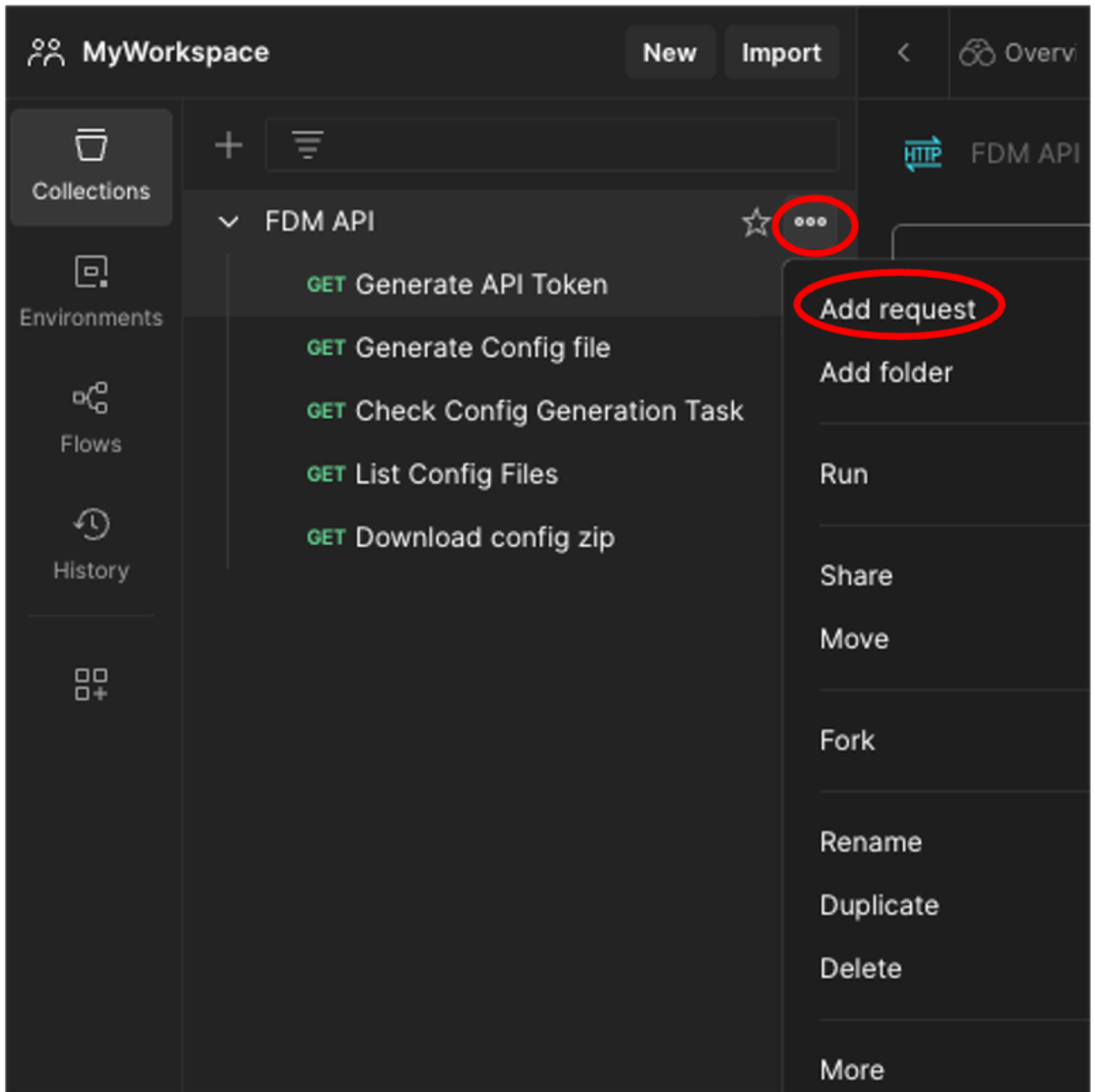


aviso: Escolher esse modo permite migrar somente ACP (Política de controle de acesso), NAT (Política de conversão de endereço de rede) e Objetos. No que diz respeito aos objetos, eles devem ser usados em uma regra ACP ou NAT, para serem migrados, caso contrário, eles serão ignorados.

Configuração

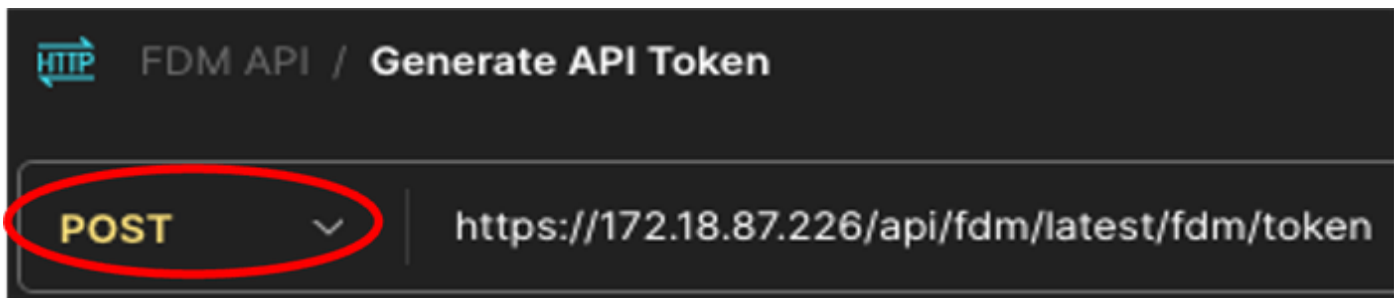
Solicitações de API - Postman

1. No Postman, crie uma nova coleção (neste cenário, a API do FDM é usada).
2. Clique nos 3 pontos e depois clique em Adicionar solicitação.



Postman - Criação de Coleção e Inclusão de Solicitação

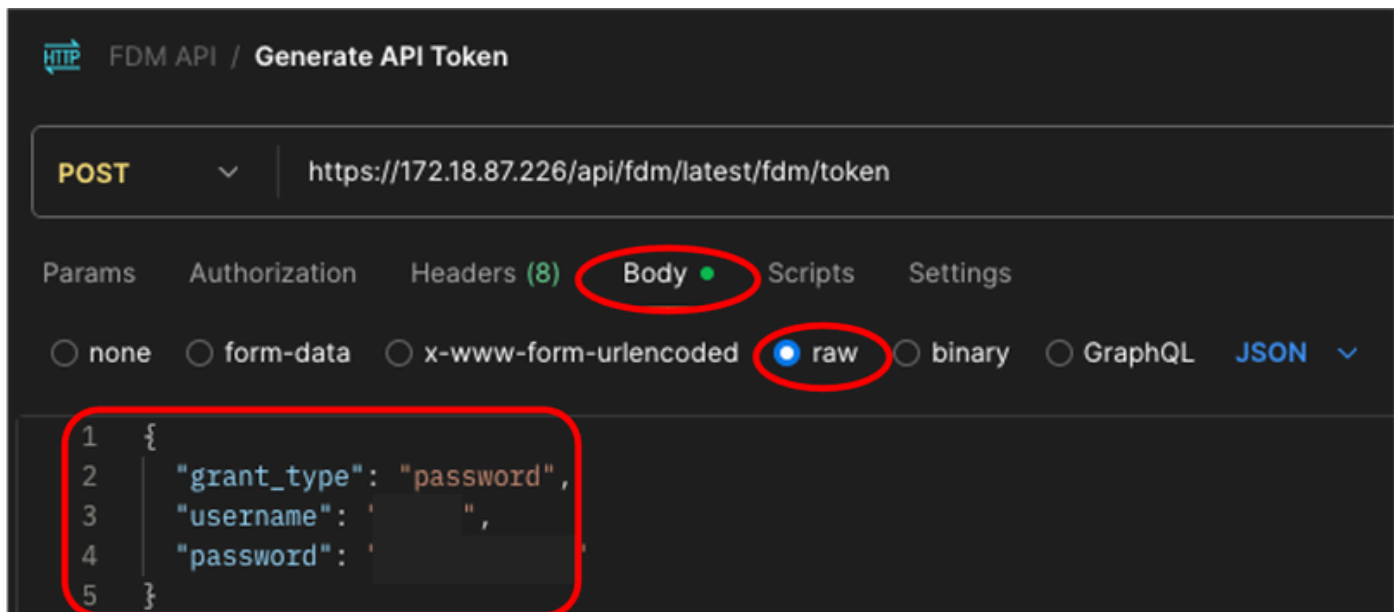
3. Chamar esta nova solicitação: Gerar token de API. Ele será criado como uma solicitação GET, mas no momento em que você estiver executando esta, POST deverá ser selecionado no menu suspenso. Na caixa de texto ao lado de POST, introduza a linha seguinte
`https://<FDM IP ADD>/api/fdm/latest/fdm/token`



Postman - Solicitação de token

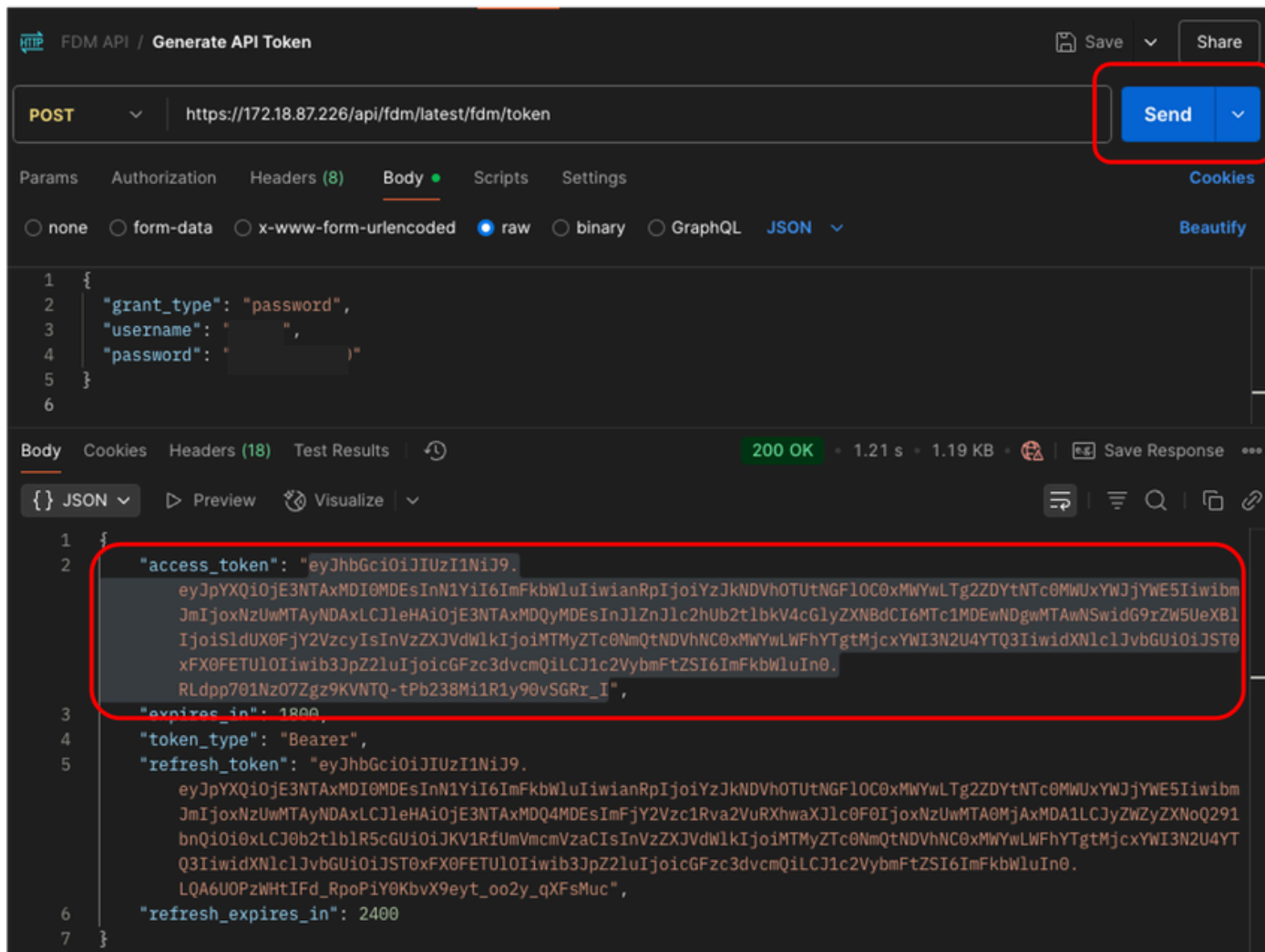
4. Na guia Corpo, selecione a opção raw e introduza as credenciais para acessar o dispositivo FTD (FDM) usando este formato.

```
{  
  "grant_type": "senha",  
  "nome de usuário": "nome de usuário",  
  "senha": "senha"  
}
```



Postman - Corpo da solicitação de token

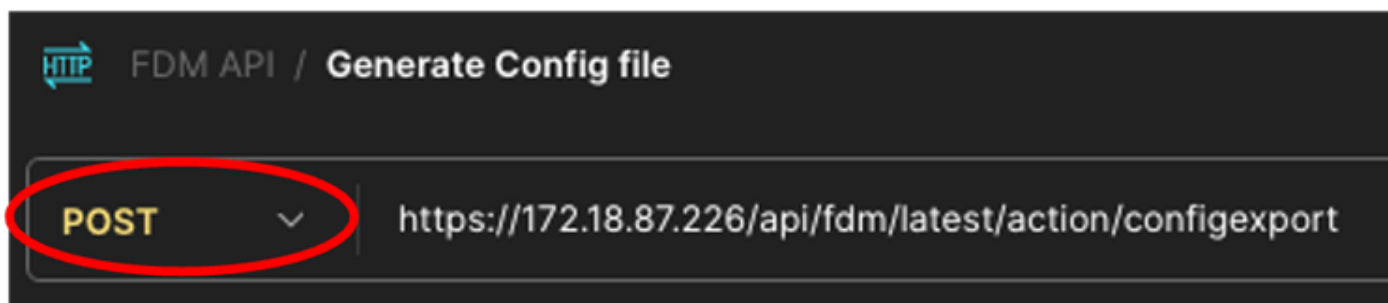
5. Finalmente, clique em Enviar para obter seu Token de Acesso. Se tudo estiver bem, você receberá uma resposta de 200 OK. Faça uma cópia do token inteiro (dentro das aspas duplas) porque ele será usado em etapas posteriores.



Postman - Token Gerado com Êxito

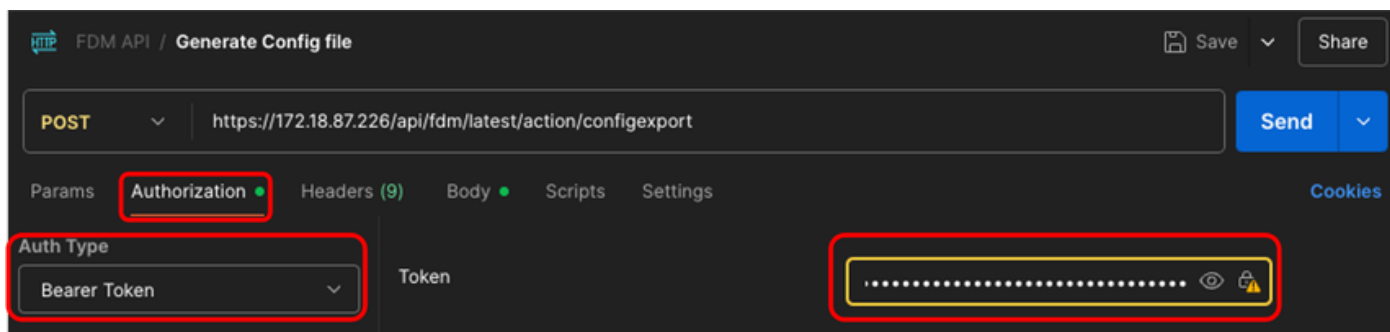
6. Repita a etapa 2, para criar uma nova solicitação, POST será usado novamente.

7. Chame esta nova solicitação: Gerar arquivo de configuração. Ele será criado como uma solicitação GET, mas no momento em que você estiver executando esta, POST deverá ser selecionado no menu suspenso. Na caixa de texto ao lado de POST, introduza a linha seguinte `https://<FDM IP ADD>/api/fdm/latest/action/configexport`



Postman - Gerar solicitação de arquivo de configuração

8. Na guia Autorização selecione Token do Portador como Tipo de Autenticação no menu suspenso, e na caixa de texto ao lado de Token cole o token copiado na etapa 5.



Postman - Solicitação de geração de arquivo de configuração - Autorização

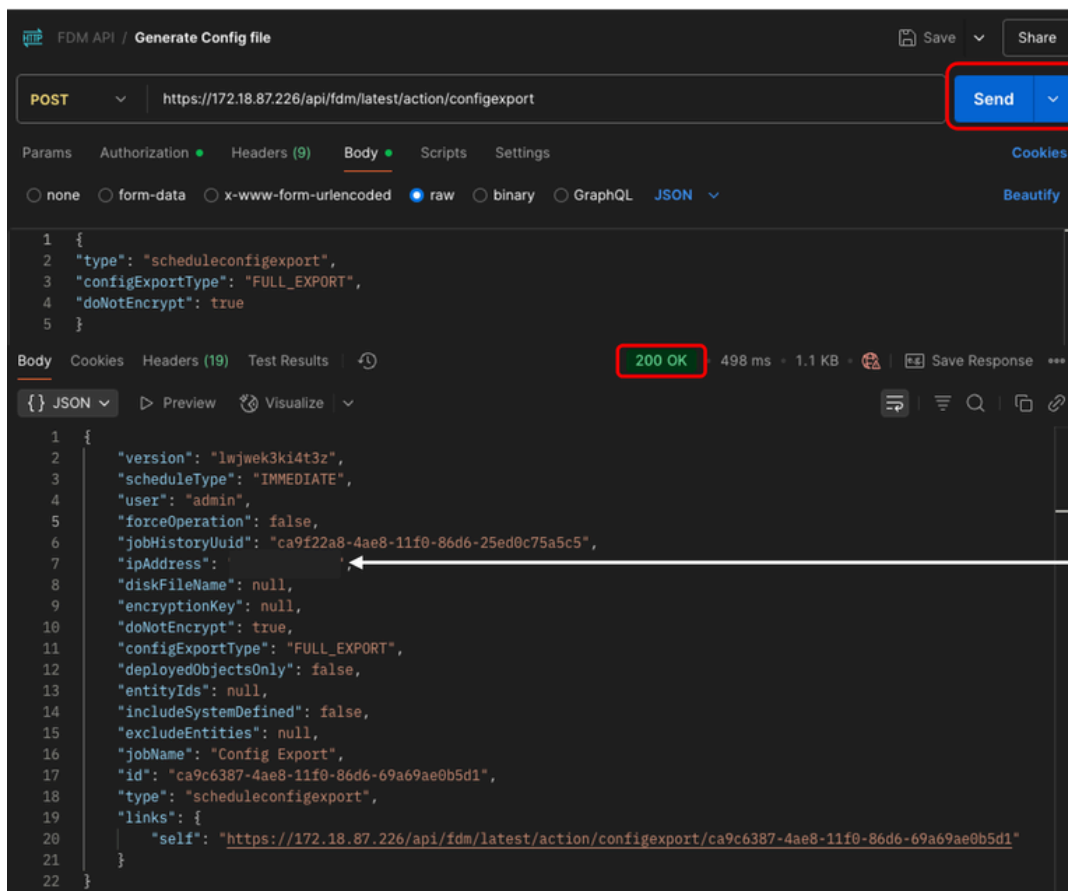
9. Na guia Corpo, selecione a opção bruto e introduza essas informações.

```
{  
  "Tipo": "agendarconfigexport",  
  "Tipo de Exportação de configuração": "FULL_EXPORT",  
  "não criptografar": verdadeiro  
}
```



Postman - Gerar solicitação de arquivo de configuração - Corpo

10. Finalmente, clique em Enviar. Se tudo estiver bem, você receberá uma resposta de 200 OK.

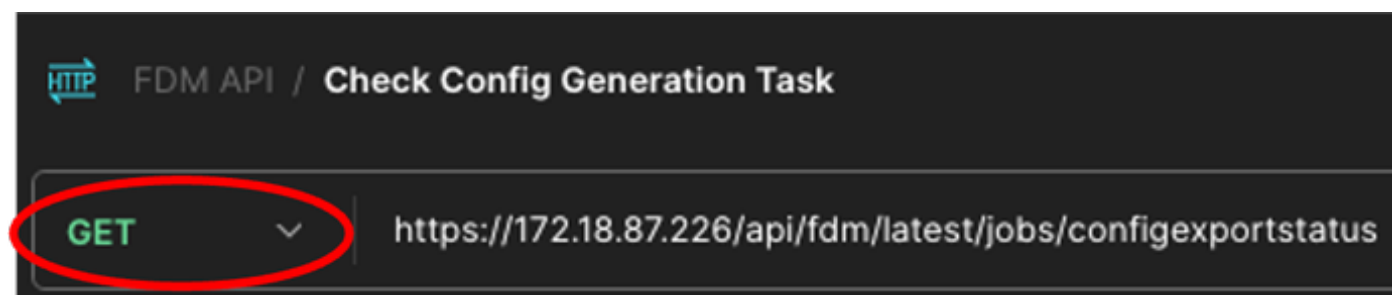


This IP address is the one that is connecting to the FTD through the requests.

Postman - Gerar solicitação de arquivo de configuração - Saída

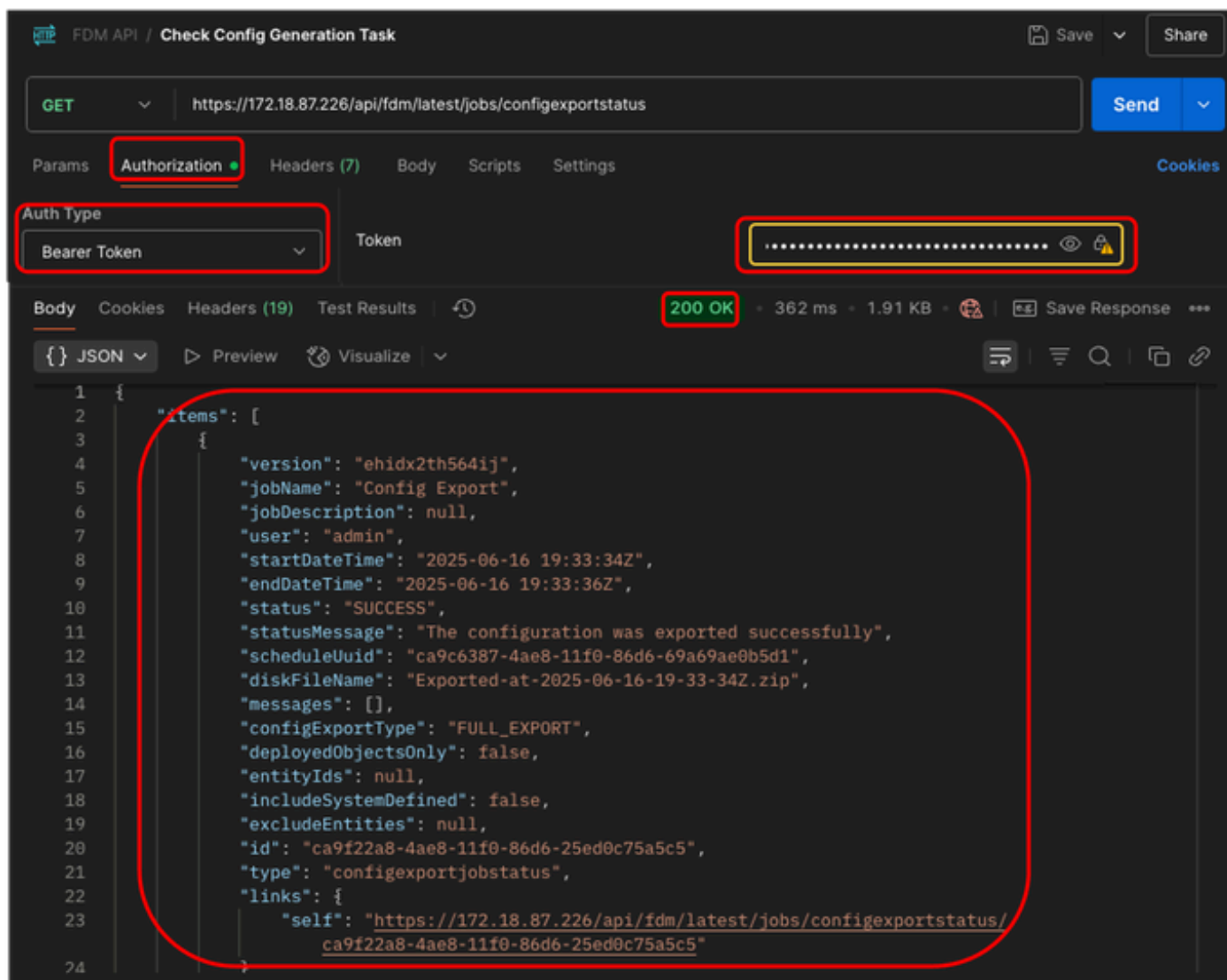
11. Repita a etapa 2 para criar uma nova solicitação. GET será usado desta vez.

12. Chame esta nova solicitação: Verificar Tarefa de Geração de Configuração. Ele será criado como uma solicitação GET. Além disso, no momento em que você estiver executando este, GET deve ser selecionado no menu suspenso. Na caixa de texto ao lado de GET, introduza a linha seguinte https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus



Postman - Verificar solicitação de status de exportação da configuração

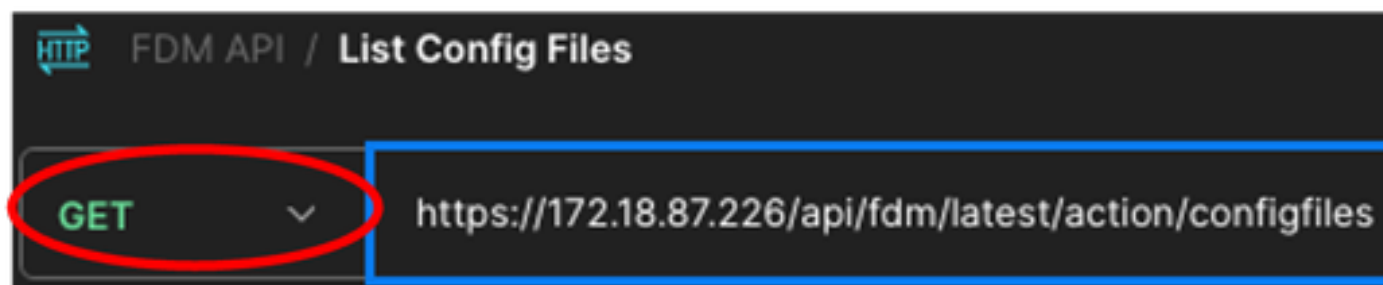
13. Na guia Autorização, selecione Token do Portador como Tipo de Autenticação no menu suspenso e, na caixa de texto ao lado de Token, cole o token copiado na etapa 5. Finalmente, clique em Enviar. Se tudo estiver bem, você receberá uma resposta 200 OK e, no campo JSON, o status da tarefa e outros detalhes poderão ser vistos.



Postman - Solicitação de status de exportação de configuração - Autorização e saída

14. Repita a etapa 2, para criar uma nova solicitação, GET será usado desta vez.

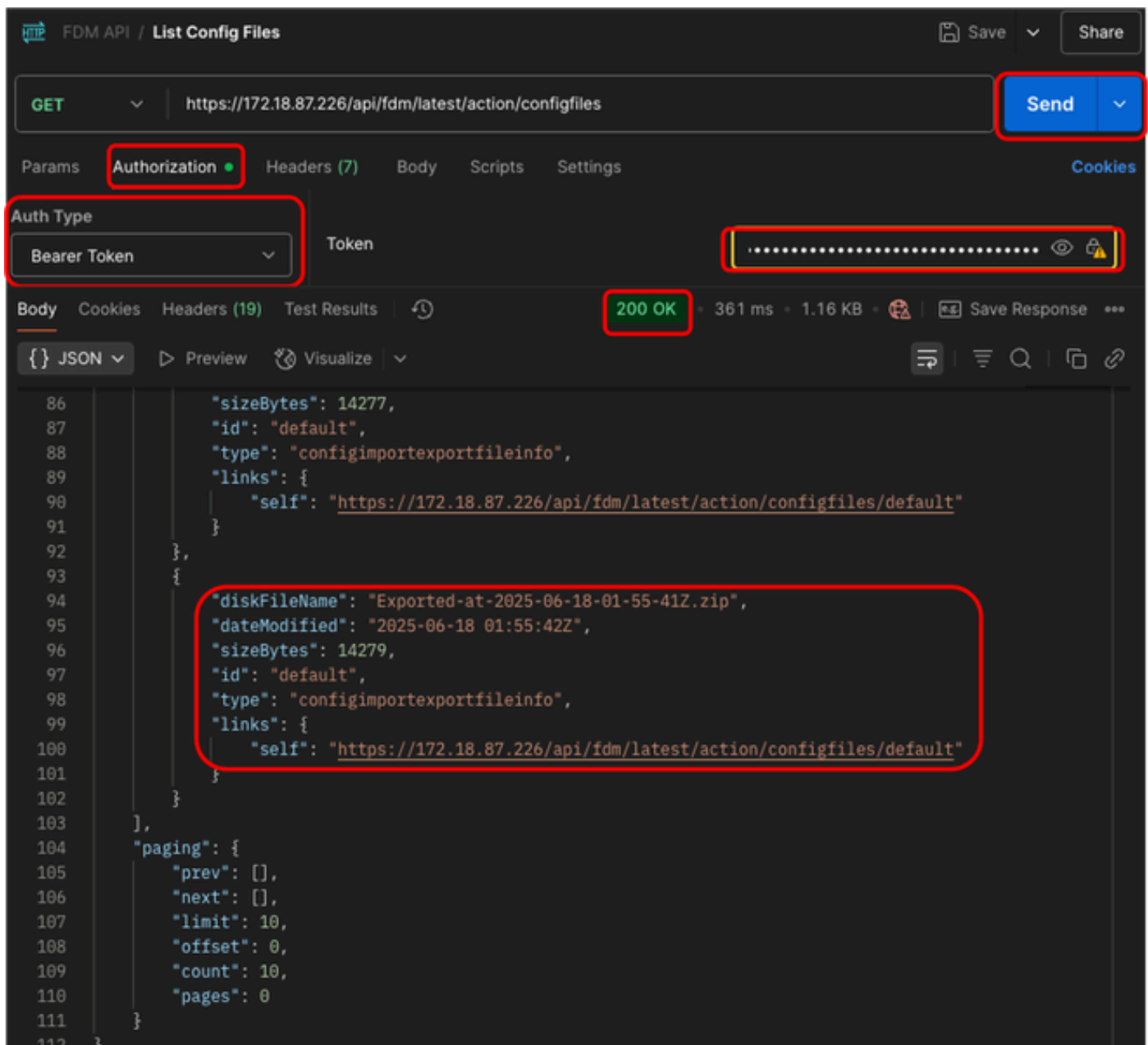
15. Chame essa nova solicitação: Listar arquivos de configuração. Ele será criado como uma solicitação GET, também no momento em que você estiver executando esta, GET deve ser selecionado no menu suspenso. Na caixa de texto ao lado de GET, introduza a linha seguinte `https://<FDM IP ADD>/api/fdm/latest/action/configfiles`



Postman - Solicitação de listagem de arquivos de configuração exportados

16. Na guia Autorização, selecione Token do Portador como Tipo de Autenticação no menu drop-down, e na caixa de texto ao lado de Token cole o token copiado na etapa 5. Finalmente, clique

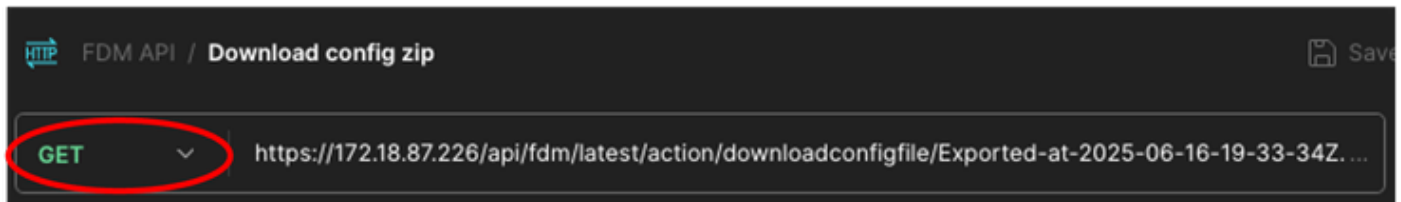
em Enviar. Se tudo estiver bem, você receberá uma resposta 200 OK e, no campo JSON, a lista dos arquivos exportados será mostrada. O mais recente está listado na parte inferior. Copie o nome do arquivo mais recente (data mais recente no nome do arquivo) porque ele será usado na última etapa.



Postman - Solicitação de listagem de arquivos de configuração exportados - Autorização e saída

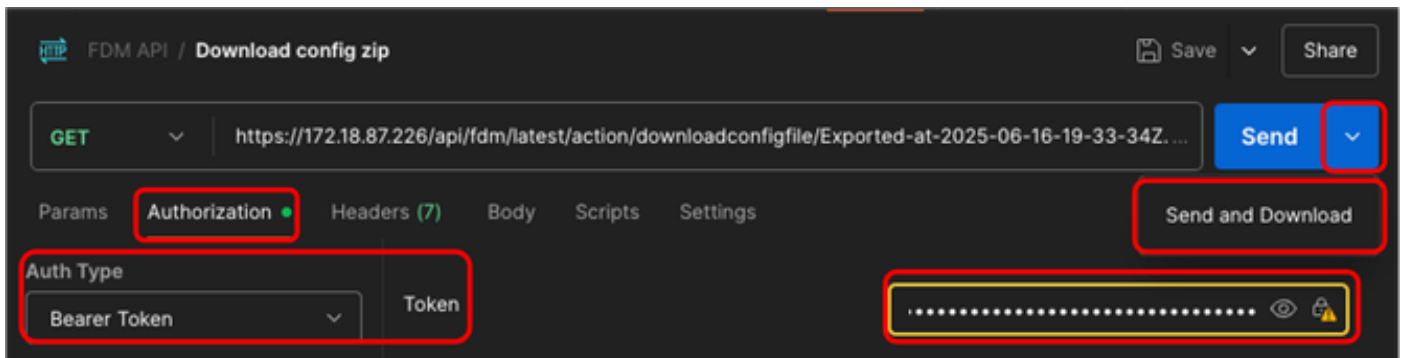
17. Repita a etapa 2, para criar uma nova solicitação, GET será usado desta vez.

18. Chame esta nova solicitação: Faça o download do zip de configuração. Ele será criado como uma solicitação GET, também no momento em que você estiver executando esta, GET deve ser selecionado no menu suspenso. Na caixa de texto ao lado de GET, introduza a linha seguinte, colando no final o nome do arquivo que você copiou na etapa 16. `https://<FDM IP ADD>/api/fdm/latest/action/downloadconfigfile/<Exported_File_name.zip >`



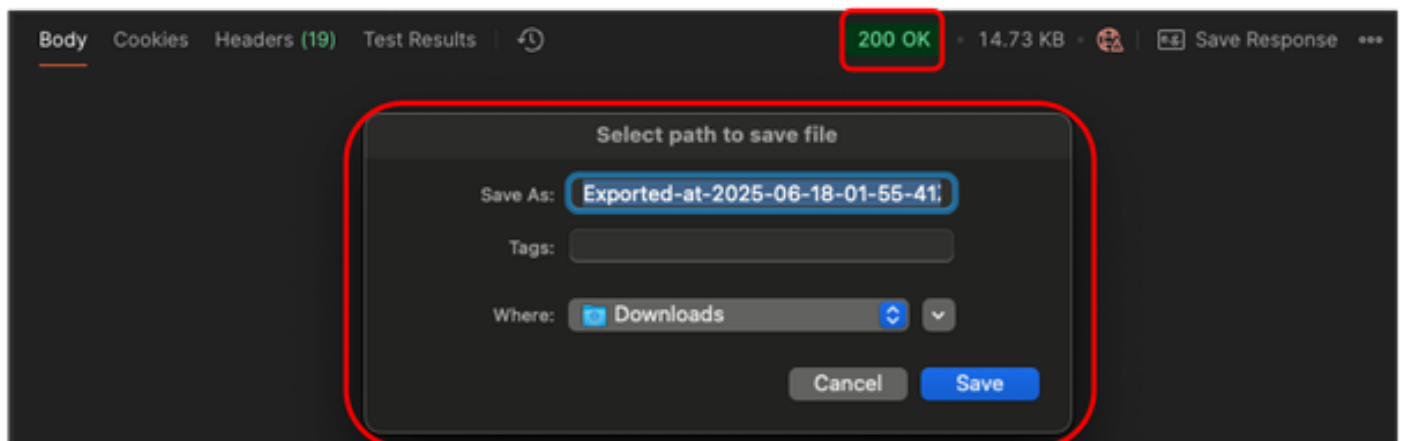
Postman - Fazer download da solicitação de arquivo Config.zip

19. Na guia Autorização, selecione Bearer Token como tipo de autenticação no menu suspenso e, na caixa de texto ao lado de Token, cole o token copiado na etapa 5. Finalmente, clique na seta para baixo ao lado de Send e escolha Send e Download.



Postman - Fazer download da solicitação de arquivo Config.zip - Autorização

20. Se tudo estiver bem, você receberá uma resposta 200 OK e uma janela pop-up será exibida solicitando a pasta de destino onde o arquivo configuration.zip será salvo. Esse arquivo .zip agora pode ser carregado na Ferramenta de Migração de Firewall.



Postman - Fazer download da solicitação de arquivo Config.zip - Salvar

Ferramenta de migração de firewall

21. Abra a Firewall Migration Tool e, no menu suspenso Selecionar configuração de origem, selecione Cisco Secure Firewall Device Manager (7.2+) e clique em Iniciar migração.

Select Source Configuration

Source Firewall Vendor
Cisco Secure Firewall Device Manager (7.2+)

Start Migration Demo Mode

Cisco Secure Firewall Device Manager (7.2+) Pre-Migration Instructions

This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) and Firewall Device Manager (FDM) when migration is in progress. FDM to FMC manager movement process should be done over a downtime/maintenance window. FDM Devices enrolled with the cloud management will lose access upon registration with FMC.

Session Telemetry:
Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:
FMT: Firewall Migration Tool
FTD: Firewall Threat Defense
FMC: Firewall Management Center
FDM: Firewall Device Manager

Before you begin your Firewall Device Manager (FDM) to Firewall Threat Defense migration, you must have the following items:

- **Stable IP Connection:**
Ensure that the connection is stable between FMT, FDM and FMC. The host-pc from which the Firewall Migration tool is being run, should have connectivity to the FDM and the FMC.
- **FMC and FDM Version:** Ensure that the FMC version is 7.3 or later and FDM version is 7.2 or later. FDM version should be always equal or less than the FMC version. For optimal migration time, improved software quality and stability, use the suggested release for your FTD and FMC. Refer to the gold star on CCO for the suggested release.
- **FMC Requirements:**
Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration. RestAPI is enabled on FMC by default. It is highly recommended that this is checked before migration. FMC should be registered with smart licensing server, and the licenses enabled on FDM must be enabled on FMC for smooth onboarding.
- **FDM Migration Options :**
Migration from FDM is supported in following ways.
 1. **Migrate Firewall Device Manager (Shared Configurations Only)**
 - This option migrates shared configuration to FMC.
 - This approach should be used to stage shared configuration to FMC. Maintenance window is not required.
 - User can either upload a configuration bundle or provide FDM credentials to fetch details.
 - Automated fetching of configuration is a preferred method.
 2. **Migrate Firewall Device Manager (Includes Device & Shared Configurations)**
 - This option migrates both device and shared configuration. Same FTD is moved from FDM managed to FMC managed.
 - **The migration process is to be done over a scheduled downtime or maintenance window. There is device downtime involved in this migration process.**
 - Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM.
 - Ensure FDM Configuration has AD Realm with encryption set to NONE. [Click here](#) for more info.
 - User should provide FDM IP and credentials to fetch details. Uploading configuration bundle is not supported.
 - FDM Devices enrolled with the cloud management will lose access upon registration with FMC.
 - Ensure out-of-band access to FTD device is available, to access the device in case of accessibility issues during migration.
 - It is highly recommended that a backup (export) of the FDM configuration is performed to restore the original state of the firewall managed by FDM if required.
 - If the FTD devices are in a failover pair, failover needs to be disabled (break HA) before proceeding with moving manager from FDM to FMC.
 - FDM with Universal PLR cannot be moved from FDM to FMC.
 - FDM with flexConfig objects or flexconfig policies cannot be moved from FDM to FMC. The flexconfig objects and policies must be

FMT - Seleção do FDM

22. Marque o primeiro Botão de Opção, Migrar Gerenciador de Dispositivos de Firewall (Somente Configurações Compartilhadas) e clique em Continuar.

How would you like to migrate from Firewall Device Manager :



Click on text below to get additional details on each of the migration options

☒ Migrate Firewall Device Manager (Shared Configurations Only)

- This option migrates shared configuration to FMC.
- This approach should be used to stage shared configuration to FMC. Maintenance window is not required.
- User can either upload a configuration bundle or provide FDM credentials to fetch details.
- Automated fetching of configuration is a preferred method.

☐ Migrate Firewall Device Manager (Includes Device & Shared Configurations)

☐ Migrate Firewall Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)

Note :

- Device configuration includes Interfaces, Routes and Site to Site VPN based features.
- Shared configuration includes Access control Policy, Remote Access VPN, NAT and Objects based features.

Continue

FMT - Somente Configurações Compartilhadas de Migração do FDM

23. No painel esquerdo (Carregamento de configuração manual) clique em Carregar.

Firewall Migration Tool (Version 7.7)

Extract Cisco Secure Firewall Device Manager (7.2+) Information

Source: Cisco Secure Firewall Device Manager (7.2+) Selected Migration: Includes Shared Config Only

Extraction Methods

Manual Configuration Upload

- Upload full configuration exported from FDM.
- Provide key for encrypted bundle (mandatory). It can be left empty for unencrypted bundle.
- For more information on fetching Configuration Bundle and Encryption Key, [Click Here](#). Do not upload hand coded configurations.

Encryption Key (Optional)

Upload

Live Connect to FDM

- Enter the management IP address and connect using admin credentials.
- IP format should be: <IP>:<Port>.

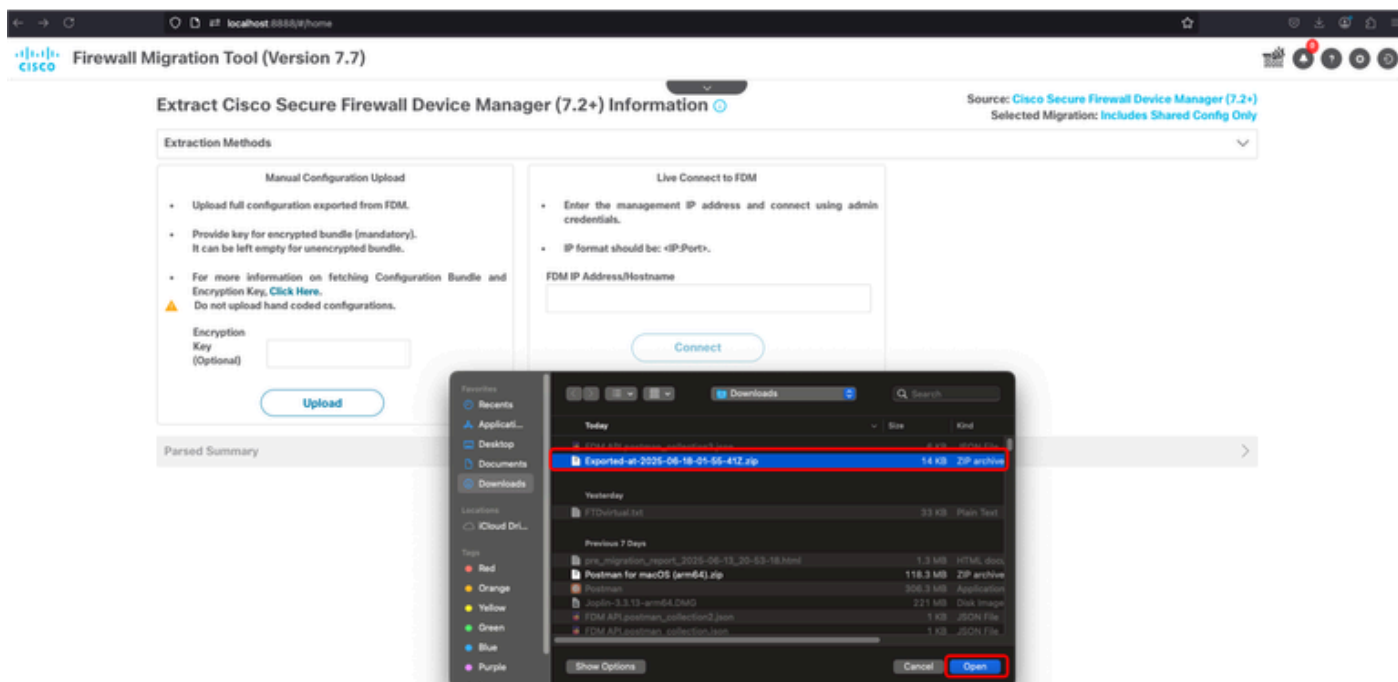
FDM IP Address/Hostname

Connect

Parsed Summary

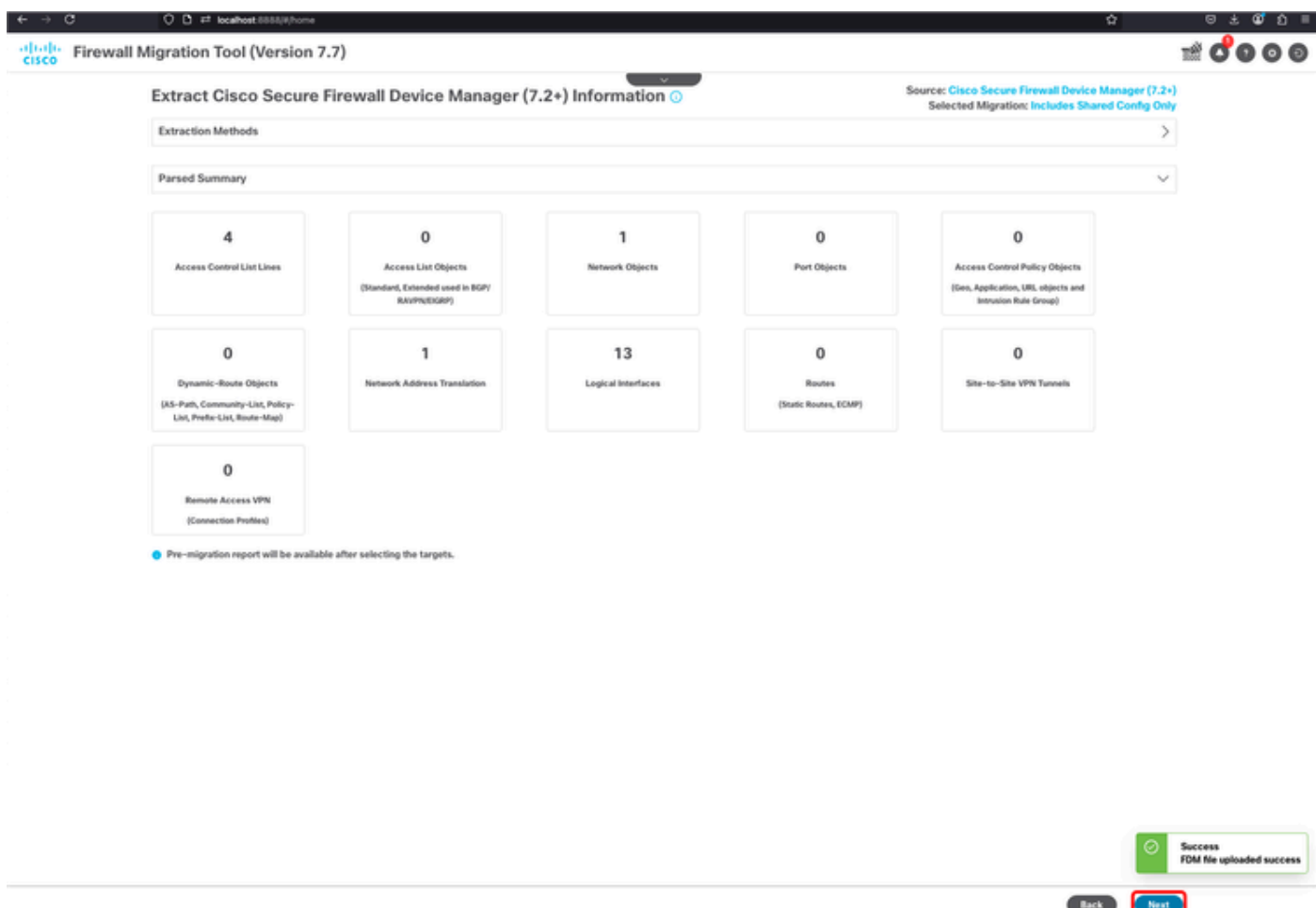
FMT - Carregar arquivo Config.zip

24. Selecione o arquivo zip config exportado na pasta salva anteriormente e clique em Abrir.



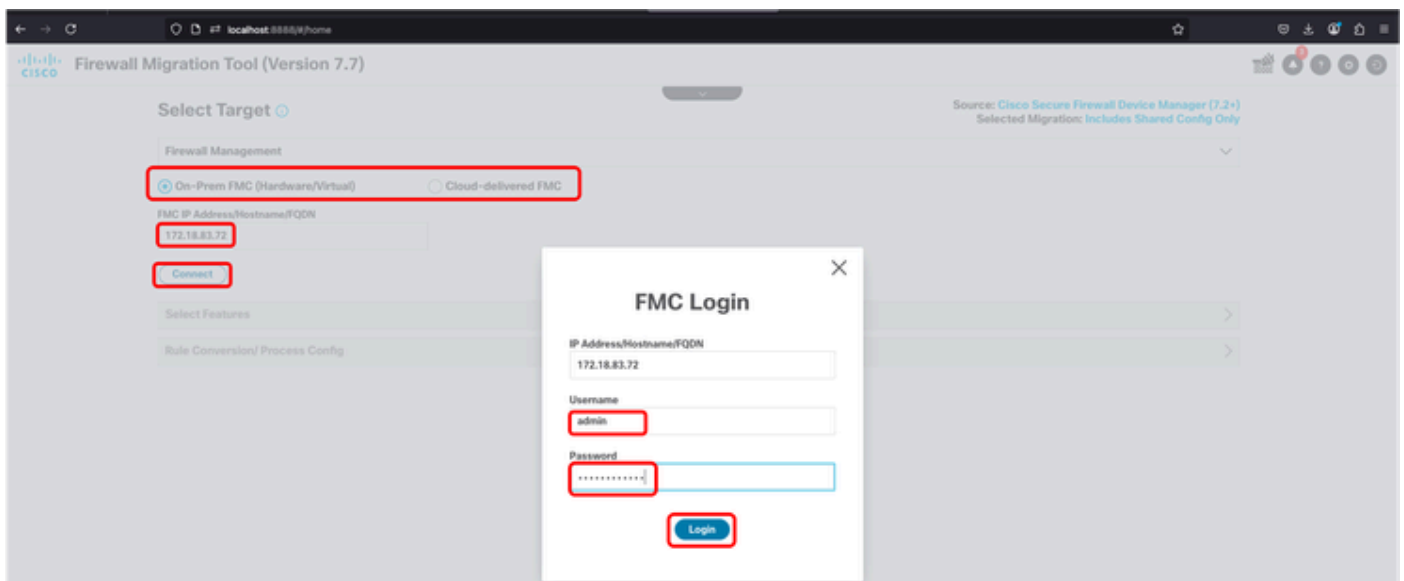
FMT - Seleção de arquivo Config.zip

25. Se tudo correr conforme o esperado, o Resumo Analisado será exibido. Além disso, no canto inferior direito, um pop-up pode ser visto informando que o arquivo do FDM foi carregado com êxito. Clique em Next.



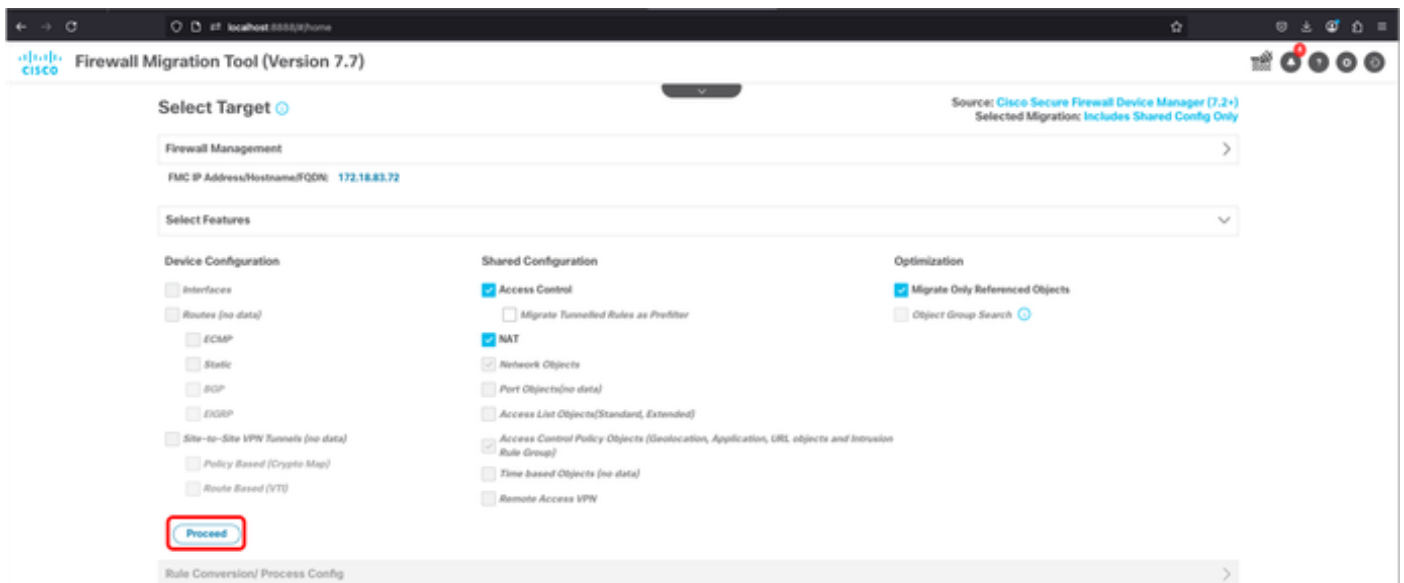
FMT - Resumo de Análise

26. Marque a opção mais adequada ao seu ambiente (FMC no local ou Cd-FMC). Neste cenário, é usado um FMC no local. Digite o endereço IP do FMC e clique em Connect. Uma nova janela pop-up será exibida e solicitará as credenciais do FMC. Depois de inserir essas informações, clique em Login.



FMT - Logon de destino do FMC

27. A próxima tela mostra o FMC de destino e os recursos que serão migrados. Clique em Continuar.



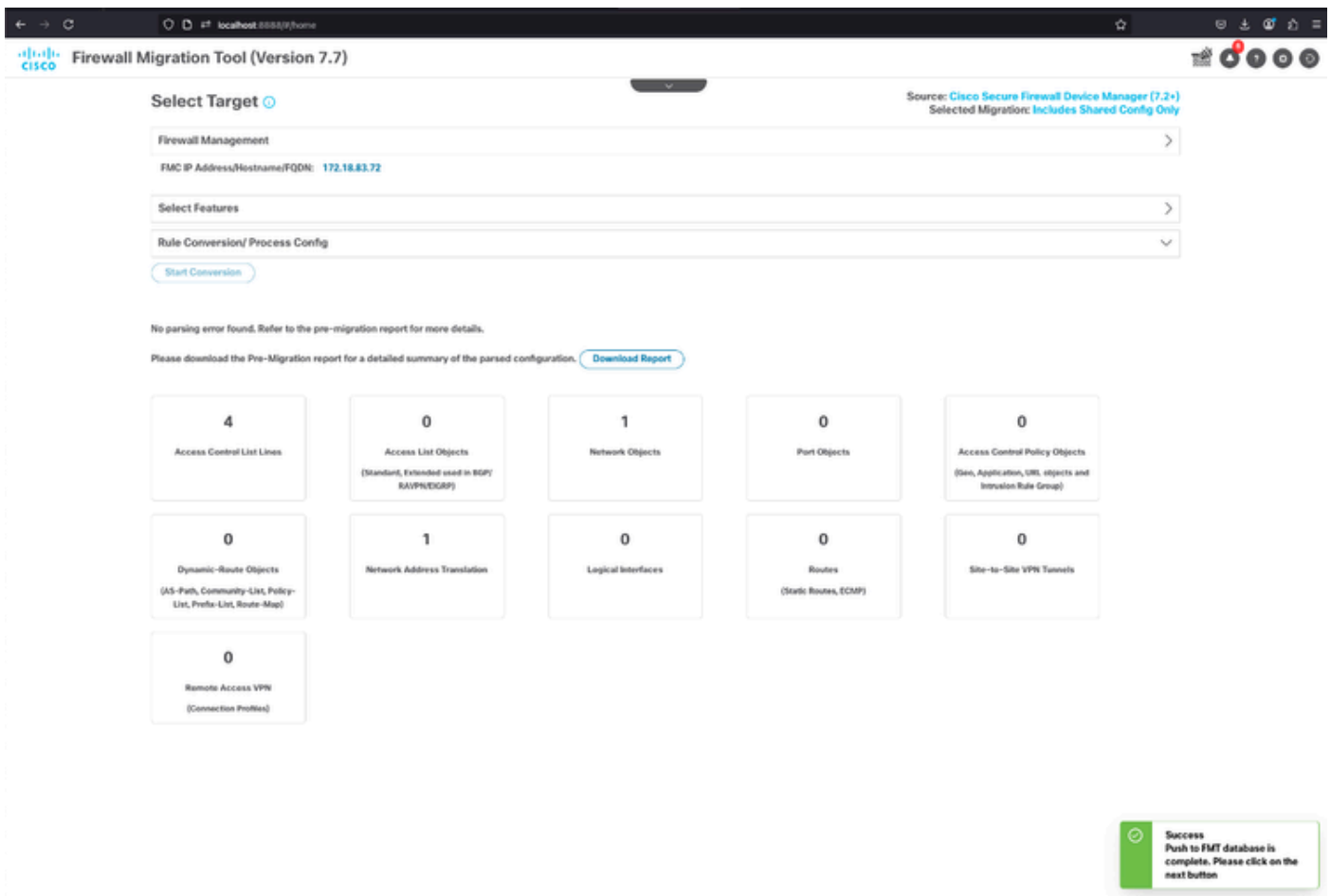
FMT - Destino FMC - Seleção de recursos

28. Depois de confirmado o objetivo do FMC, clique no botão Start Conversion.



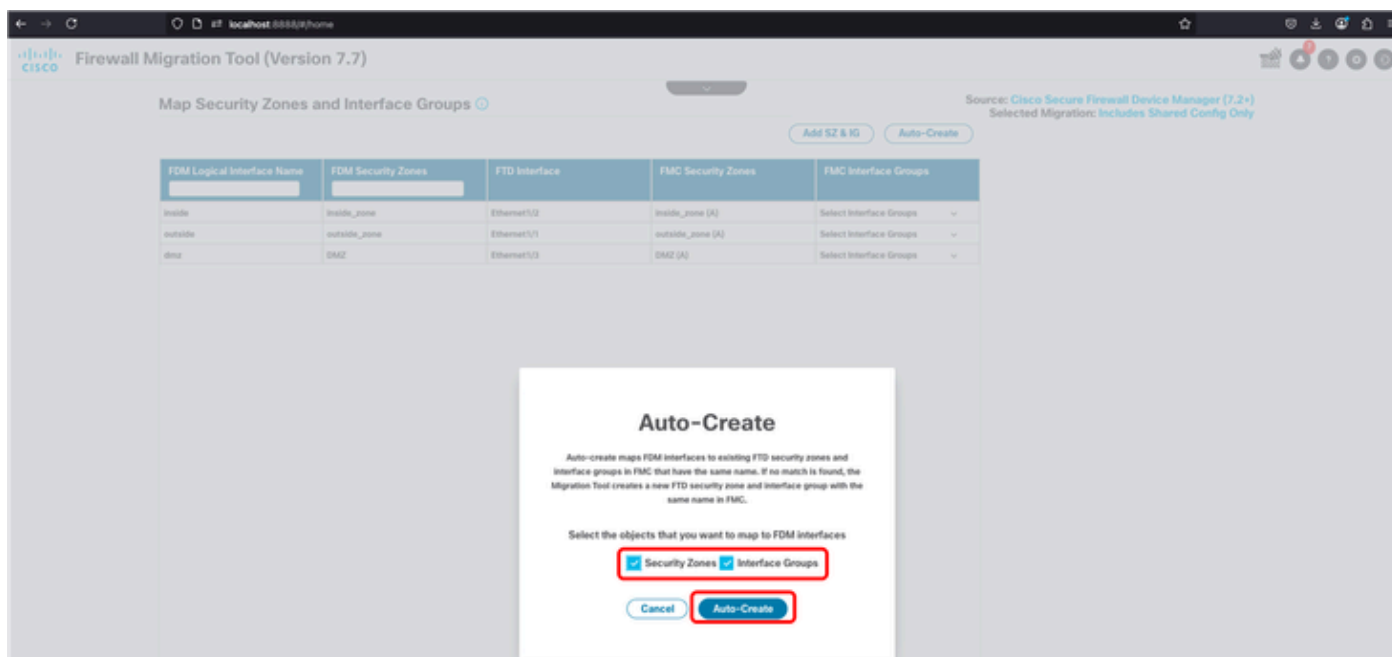
FMT - Iniciando a conversão da configuração

29. Se tudo correr como esperado, uma janela pop-up será exibida no canto inferior direito informando que o envio para o banco de dados FMT foi concluído. Clique em Next.



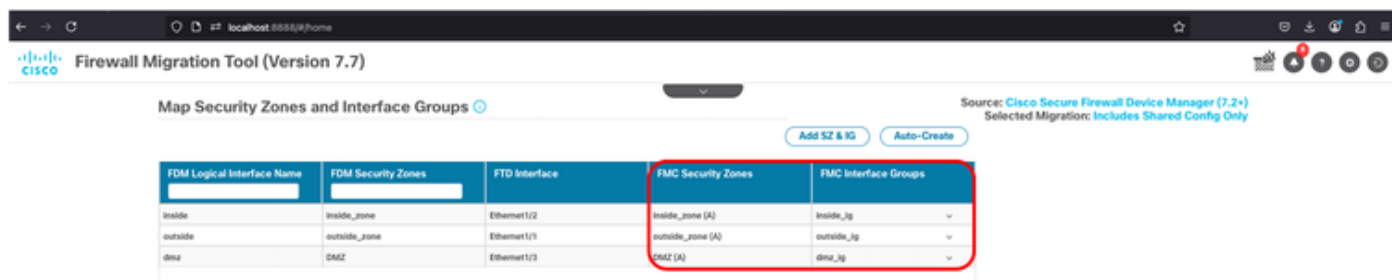
FMT - Envio de Banco de Dados Concluído com Êxito

30. Na próxima tela, você deve criar manualmente ou escolher criar automaticamente as zonas de segurança e os grupos de interface. Neste cenário, a criação automática é usada.



FMT - Criação Automática de Zonas de Segurança e Grupos de Interface

31. Depois de preenchida, a tabela mostra na 4ª e 5ª colunas, a Zona de segurança e o Grupo de interface, respectivamente.



FMT - Zonas de segurança e grupos de interface criados com êxito

32. Na próxima tela, você pode otimizar a ACL ou apenas validar o ACP, Objetos e NAT. Depois de concluído, clique no botão Validar.

Firewall Migration Tool (Version 7.7)

Optimize, Review and Validate Shared Configuration Only

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Shared Config Only

Access Control Objects NAT Interfaces Routers Site-to-Site VPN Remote Access VPN

ACP Pre-filter Intrusion Policy

Select all 4 entries Selected: 0 / 4 Actions Save

Search

#	Name	SOURCE			DESTINATION			ACCESS CONTROL POLICY ...		State	Action	ACE Count	TIME BASED
		Zone	Network	Port	Zone	Network	Port	Applications	URLs				
1	Inside_Outside_Rul...	inside_zone	ANY	ANY	outside_in...	ANY	ANY	ANY	ANY	✓	trust	1	None
2	AD-Srvr_R1	DMZ	AD-Srvr	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	permit	1	None
3	DMZ-Inside_R1	DMZ	ANY	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	deny	1	None
4	Outside_DMZ_R1	outside_in...	ANY	ANY	DMZ	ANY	ANY	ANY	ANY	✓	permit	1	None

50 per page 1 to 4 of 4 Page 1 of 1

Optimize ACL Validate

FMT - Otimizar ACL - Validar Migração

33. A validação demora alguns minutos para ser concluída.

Firewall Migration Tool (Version 7.7)

Optimize, Review and Validate Shared C

Validation in progress. It will take a while

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Shared Config Only

Access Control Objects NAT Interfaces Routers Site-to-Site VPN Remote Access VPN

ACP Pre-filter Intrusion Policy

Select all 4 entries Selected: 0 / 4 Actions Save

Search

#	Name	SOURCE			DESTINATION			ACCESS CONTROL POLICY ...		State	Action	ACE Count	TIME BASED
		Zone	Network	Port	Zone	Network	Port	Applications	URLs				
1	Inside_Outside_Rul...	inside_zone	ANY	ANY	outside_in...	ANY	ANY	ANY	ANY	✓	trust	1	None
2	AD-Srvr_R1	DMZ	AD-Srvr	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	permit	1	None
3	DMZ-Inside_R1	DMZ	ANY	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	deny	1	None
4	Outside_DMZ_R1	outside_in...	ANY	ANY	DMZ	ANY	ANY	ANY	ANY	✓	permit	1	None

FMT - Validação em Andamento

34. Depois de concluído, o FMT permite que você saiba que a configuração foi validada com êxito e a próxima etapa é clicar no botão Configuração Push.

×

Validation Status

✓

Successfully Validated

Validation Summary (Pre-push)

4 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	0 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)	1 Network Address Translation	Not selected for migration Logical Interfaces	Not selected for migration Routes (Static Routes, ECMP)	Not selected for migration Site-to-Site VPN Tunnels
Not selected for migration Remote Access VPN (Connection Profiles)				

Push Configuration

FMT - Validação Bem-sucedida - Enviar Configuração para FMC

35. Finalmente, clique no botão Prosseguir.

The Step of final push to target FMC/FTD is subjected to zero, limited or many push errors that largely depend on the success or failure of API execution between migration tool and firewall management center.



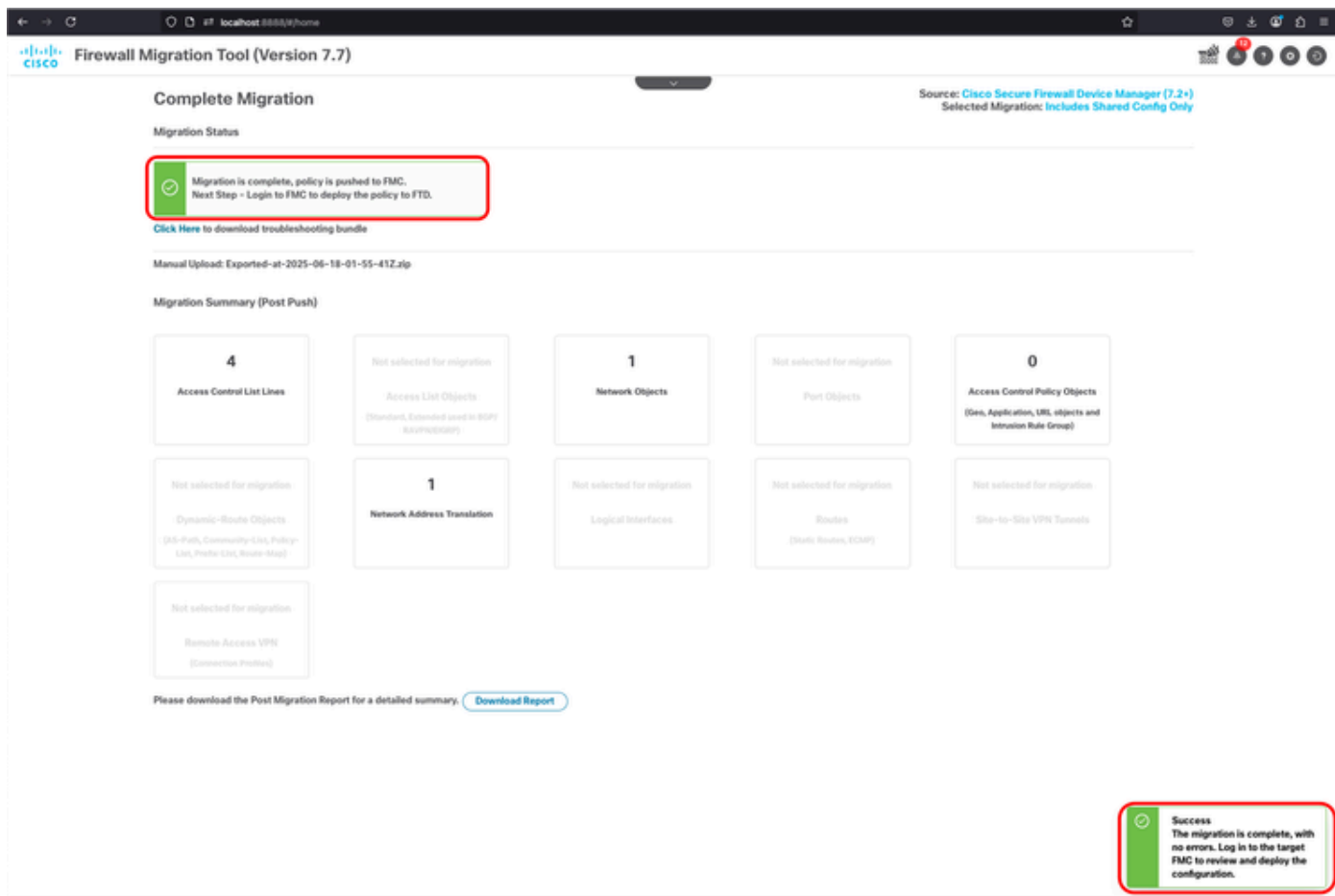
Click on Proceed to continue.

Proceed

Recommendation: Please review the migration fallout report during the course of final push stage to understand firewall configurations that will not be migrated in addition to review the suggested actions to be taken on target FMC for "Abort Migration".

FMT - Prosseguir com envio de configuração

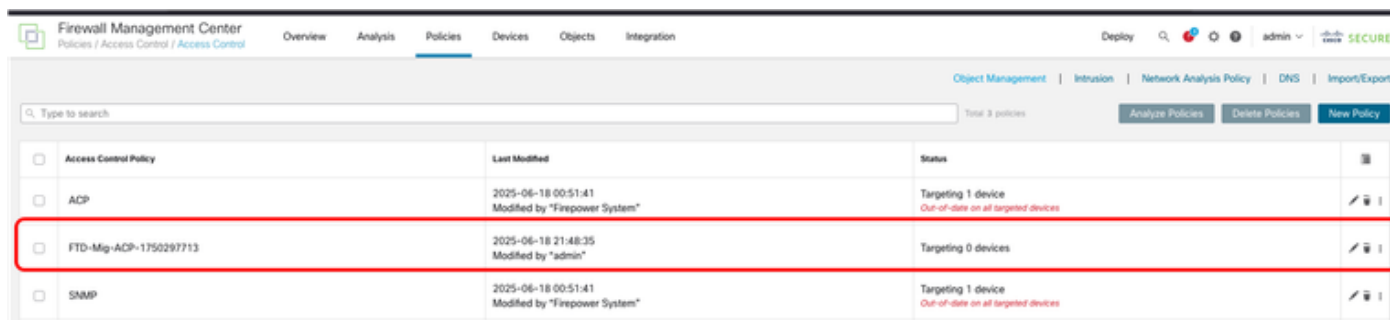
36. Se tudo correr conforme esperado, será exibida a notificação de Migração bem-sucedida. O FMT solicita que você faça login no FMC e implante a política migrada no FTD.



FMT - Notificação de Migração Bem-sucedida

Verificação do FMC

37. Após o login no FMC, as políticas de ACP e NAT são mostradas como FTD-Mig. Agora, você pode prosseguir com a implantação para o novo FTD.



FMC - ACP Migrado



FMC - Política NAT migrada

Informações Relacionadas

- [FMT - Guia de Migração do FDM para o FMC](#)
- [Notas de versão do FMT](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.