# 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.

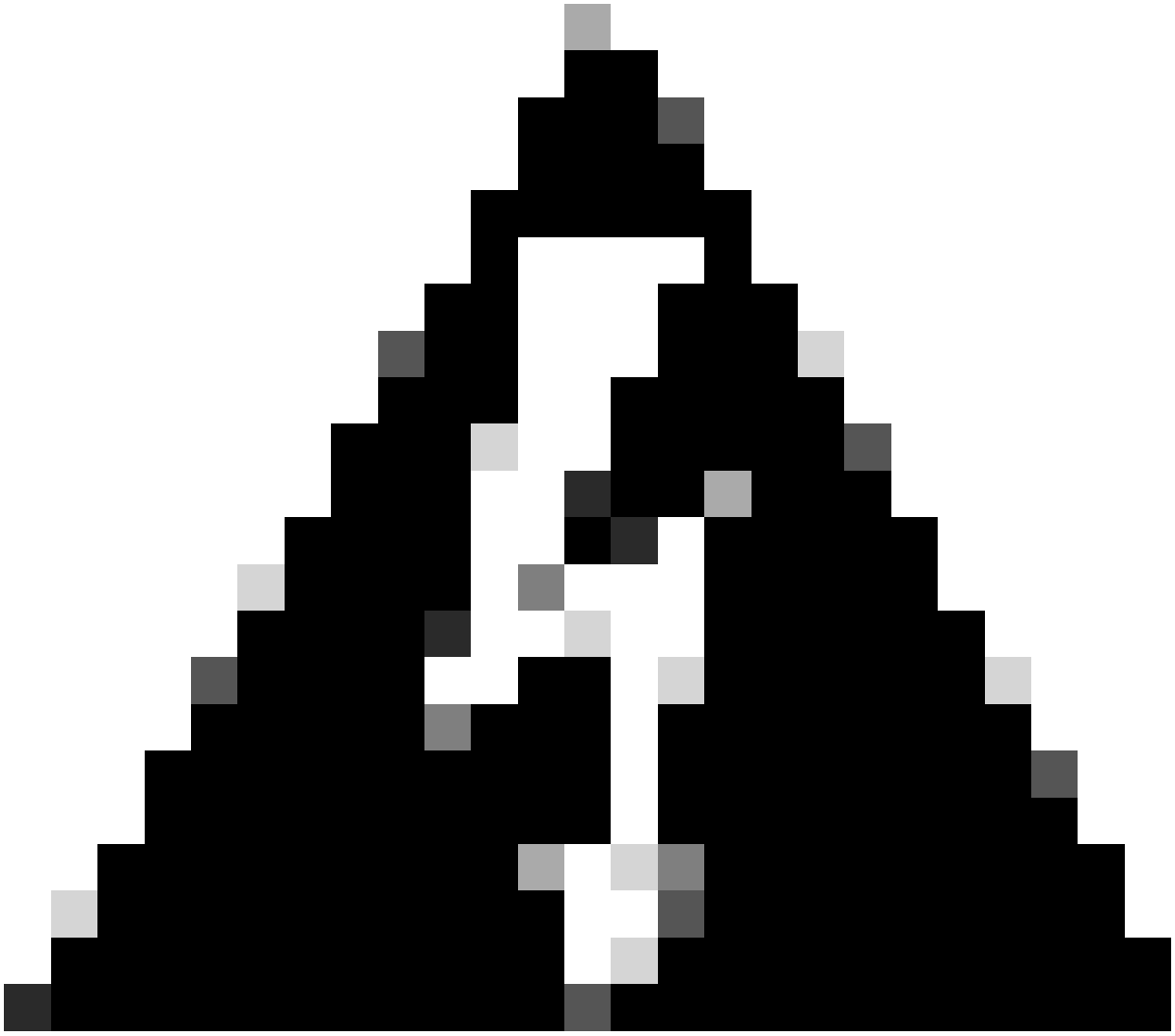
## Informações de Apoio

- 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.

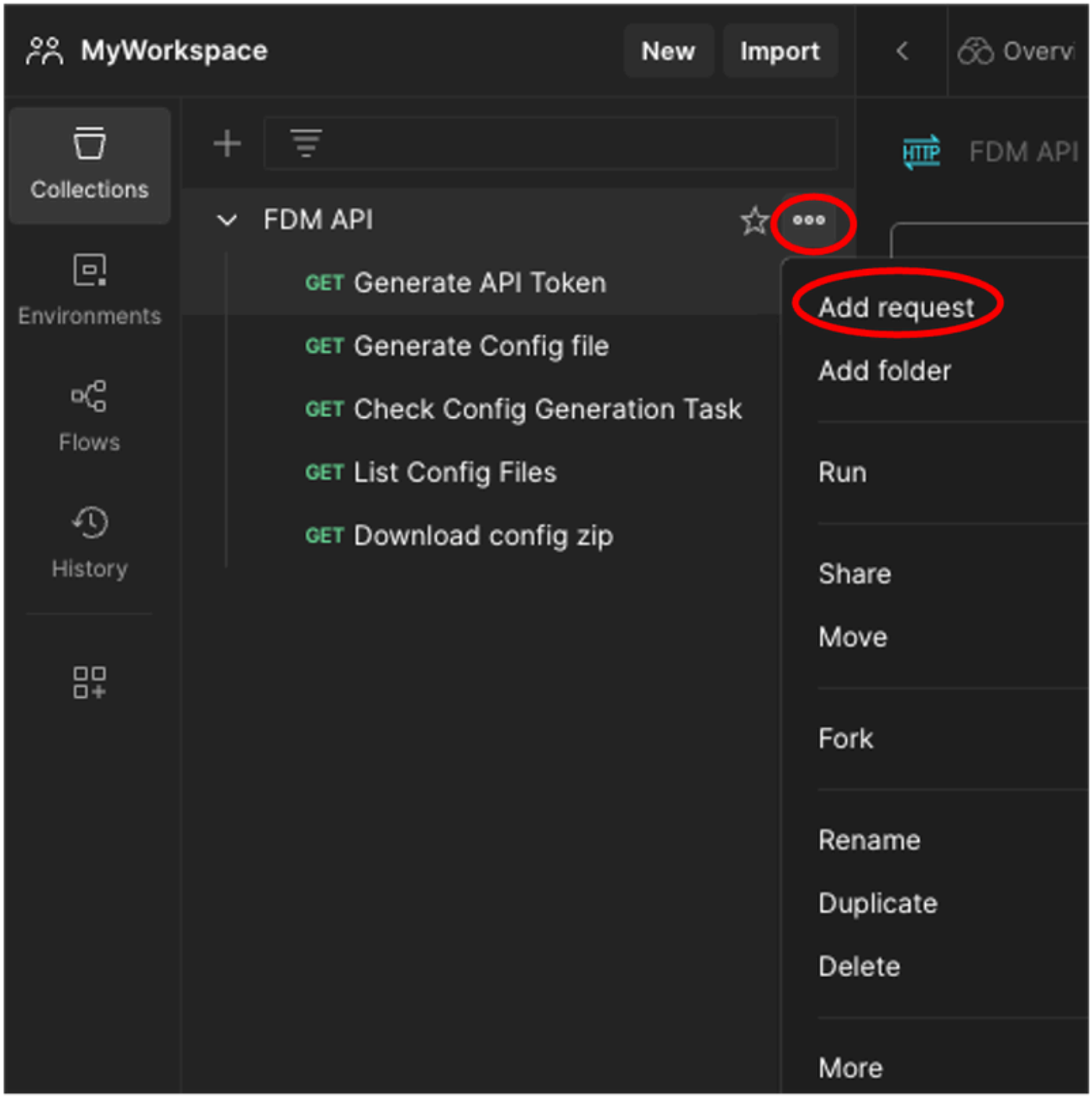


aviso: Escolher esse modo permite migrar somente ACP (Política de controle de acesso), NAT (Política de conversão de endereço de rede) e Objetos. No que diz respeito aos objetos, eles devem ser usados em uma regra ACP ou NAT, para serem migrados, caso contrário, eles serão ignorados.

# Configuração

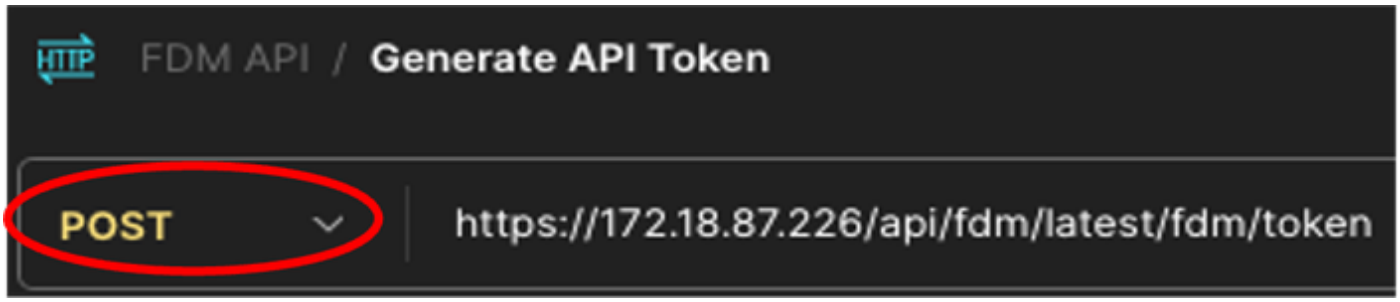
## Solicitações de API - Postman

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.

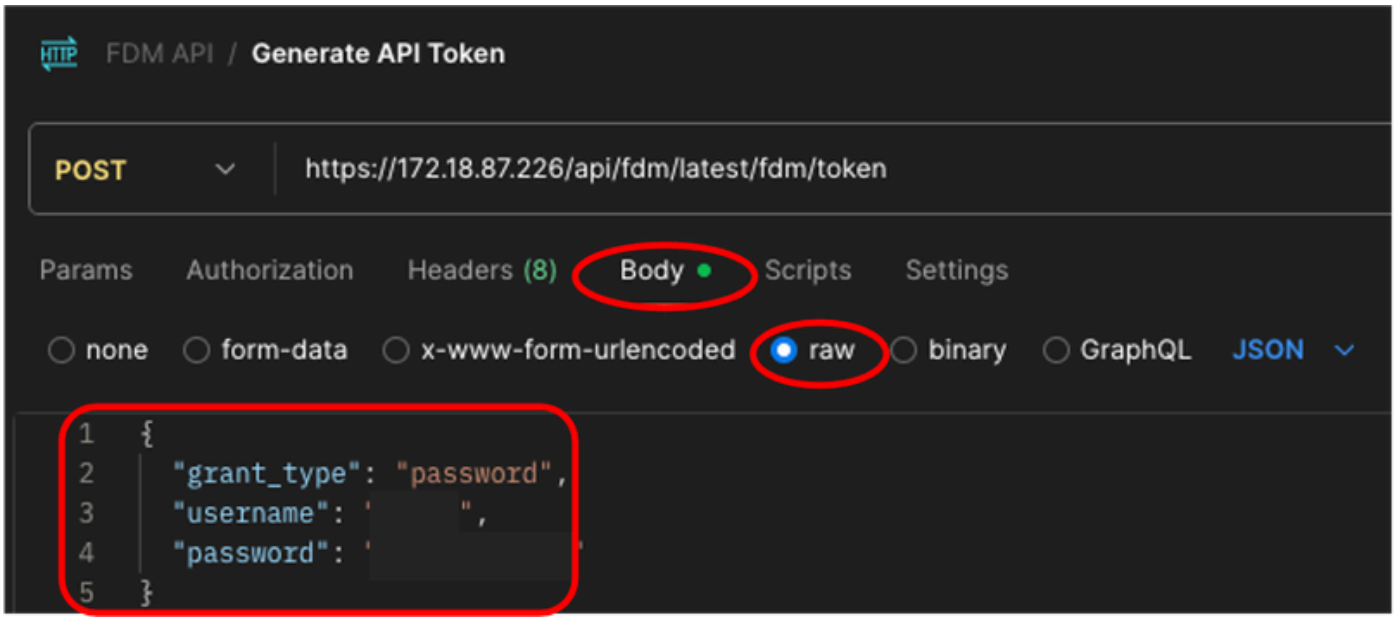
{

"grant_type": "senha",

"nome de usuário": "nome de usuário",

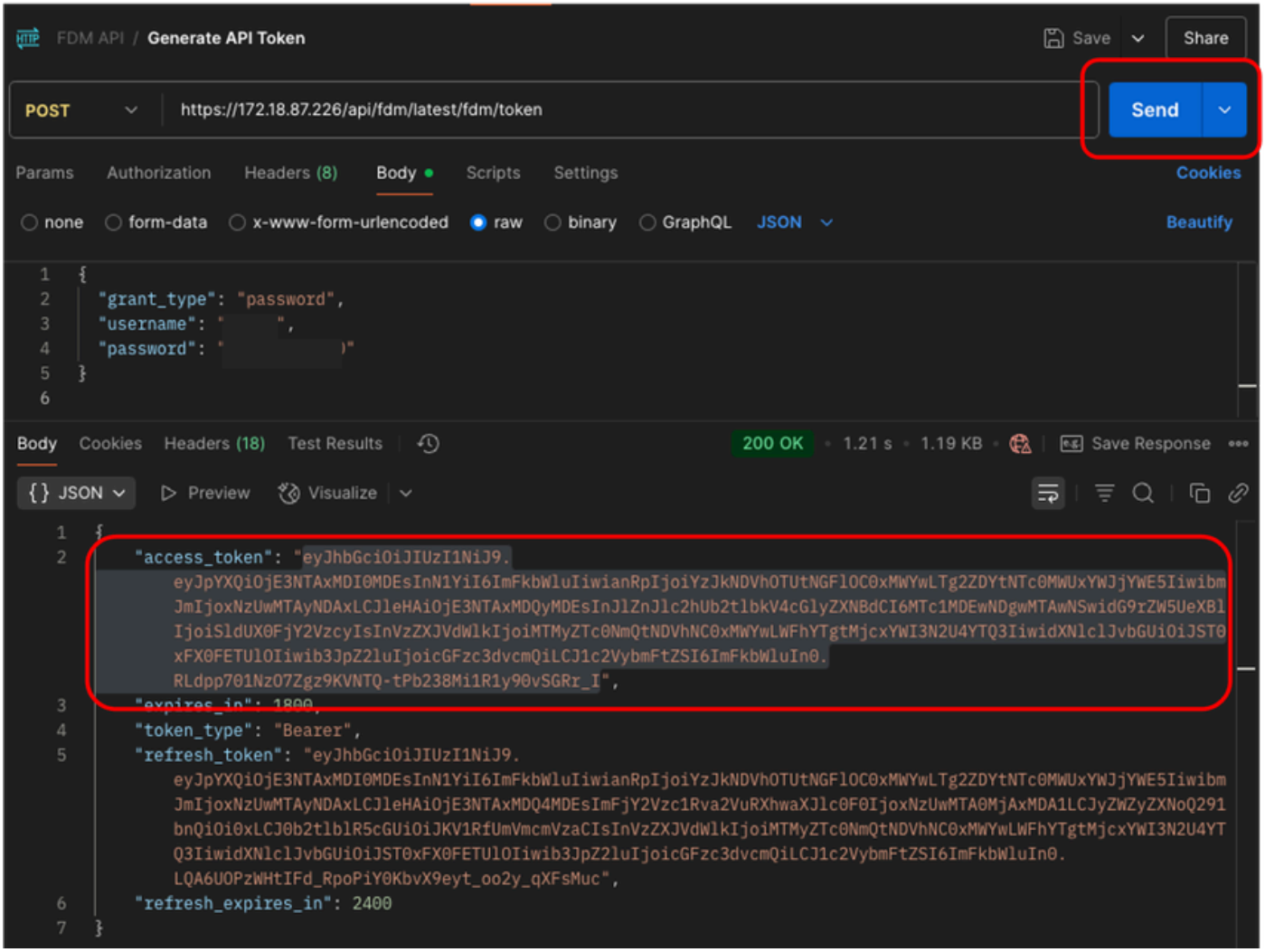
"senha": ”senha"

}




Postman - Corpo da solicitação de token

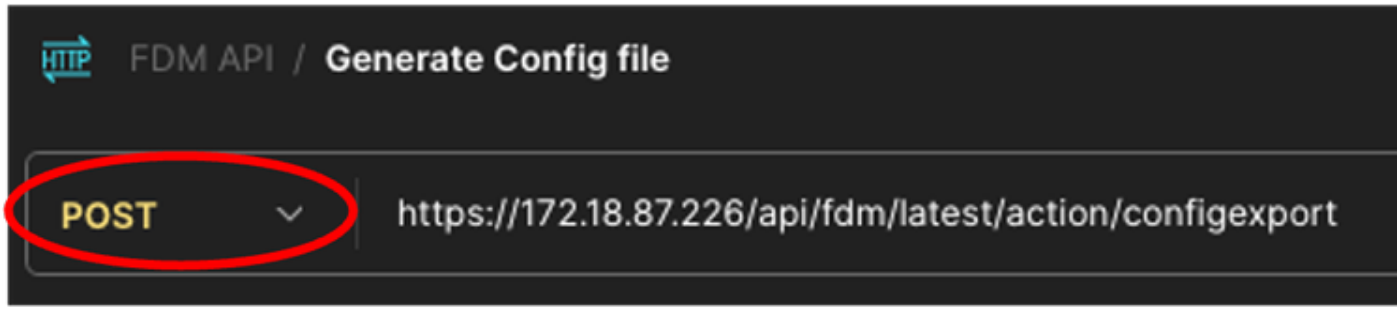
5. Finalmente, clique em Enviar para obter seu Token de Acesso. Se tudo estiver bem, você receberá uma resposta de 200 OK. Faça uma cópia do token inteiro (dentro das aspas duplas) porque ele será usado em etapas posteriores.




Postman - Token Gerado com Êxito

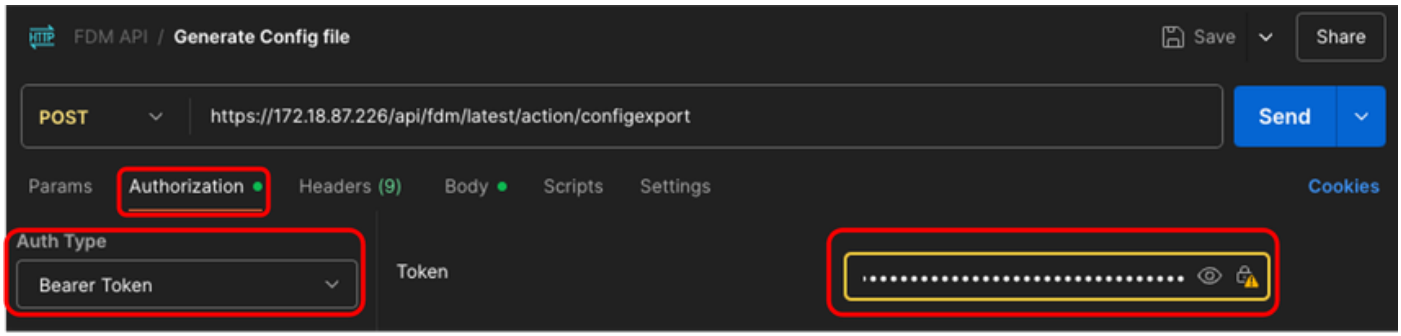
6. Repita a etapa 2, para criar uma nova solicitação, POST será usado novamente.

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.

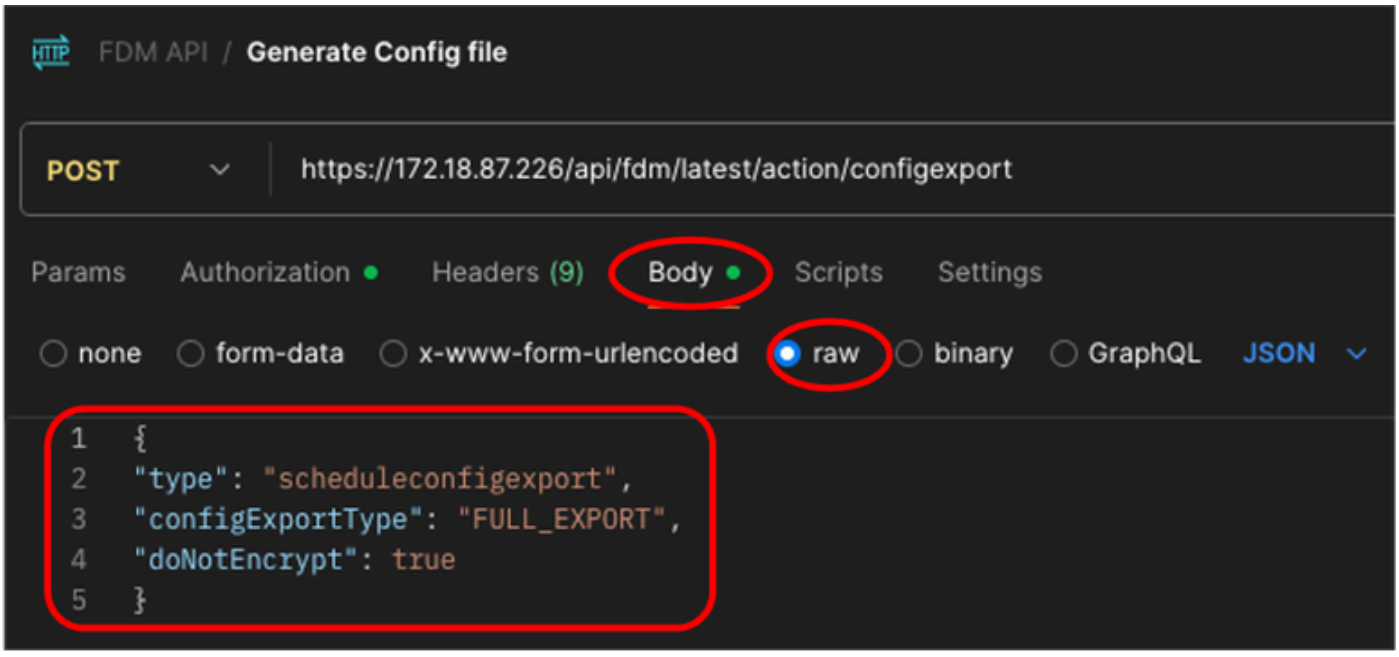
{

"Tipo": "agendarconfigexport",

"Tipo de Exportação de configuração": "FULL_EXPORT",

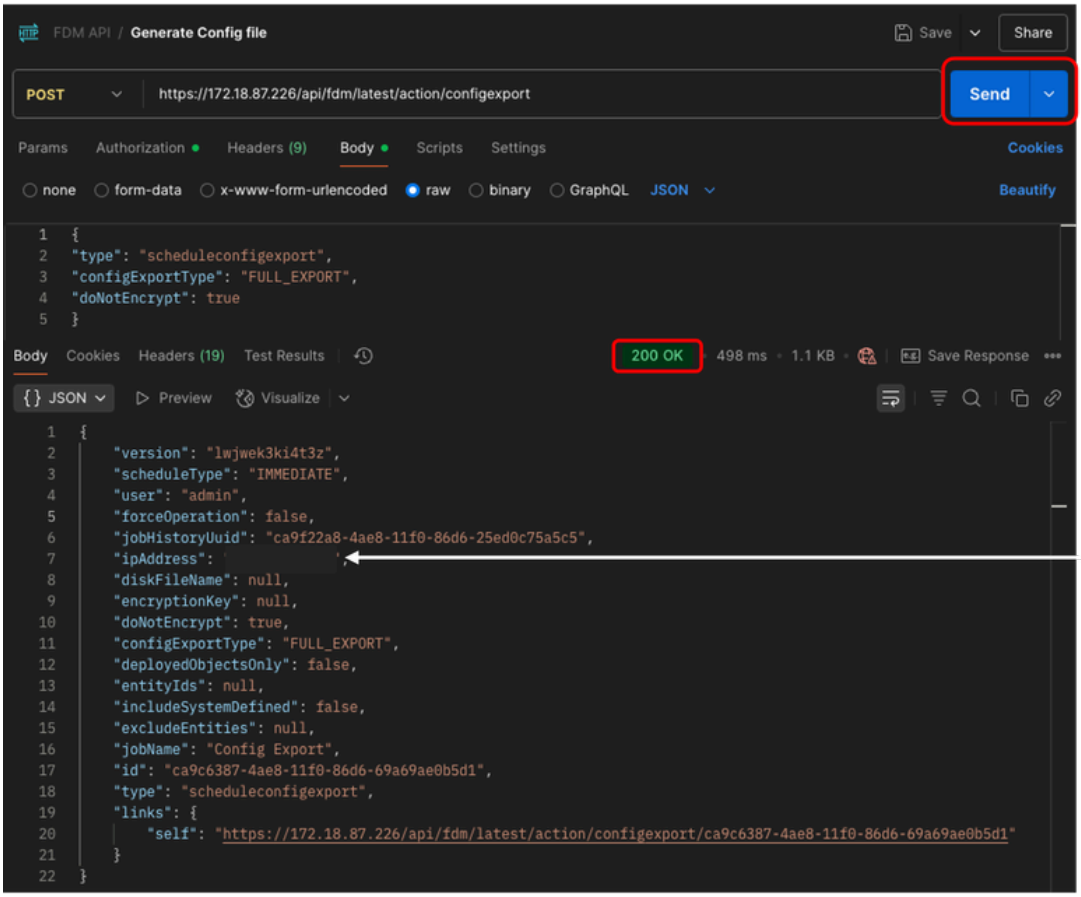
"não criptografar": verdadeiro

}




Postman - Gerar solicitação de arquivo de configuração - Corpo

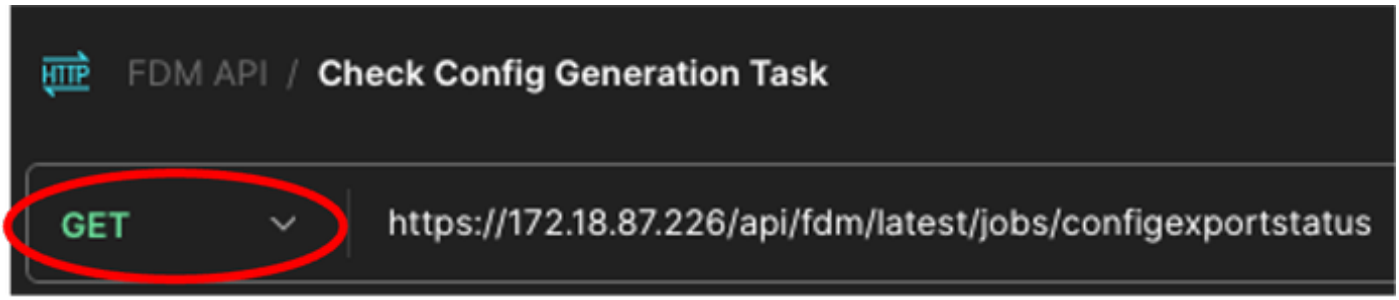
10. Finalmente, clique em Enviar. Se tudo estiver bem, você receberá uma resposta de 200 OK.




Postman - Gerar solicitação de arquivo de configuração - Saída

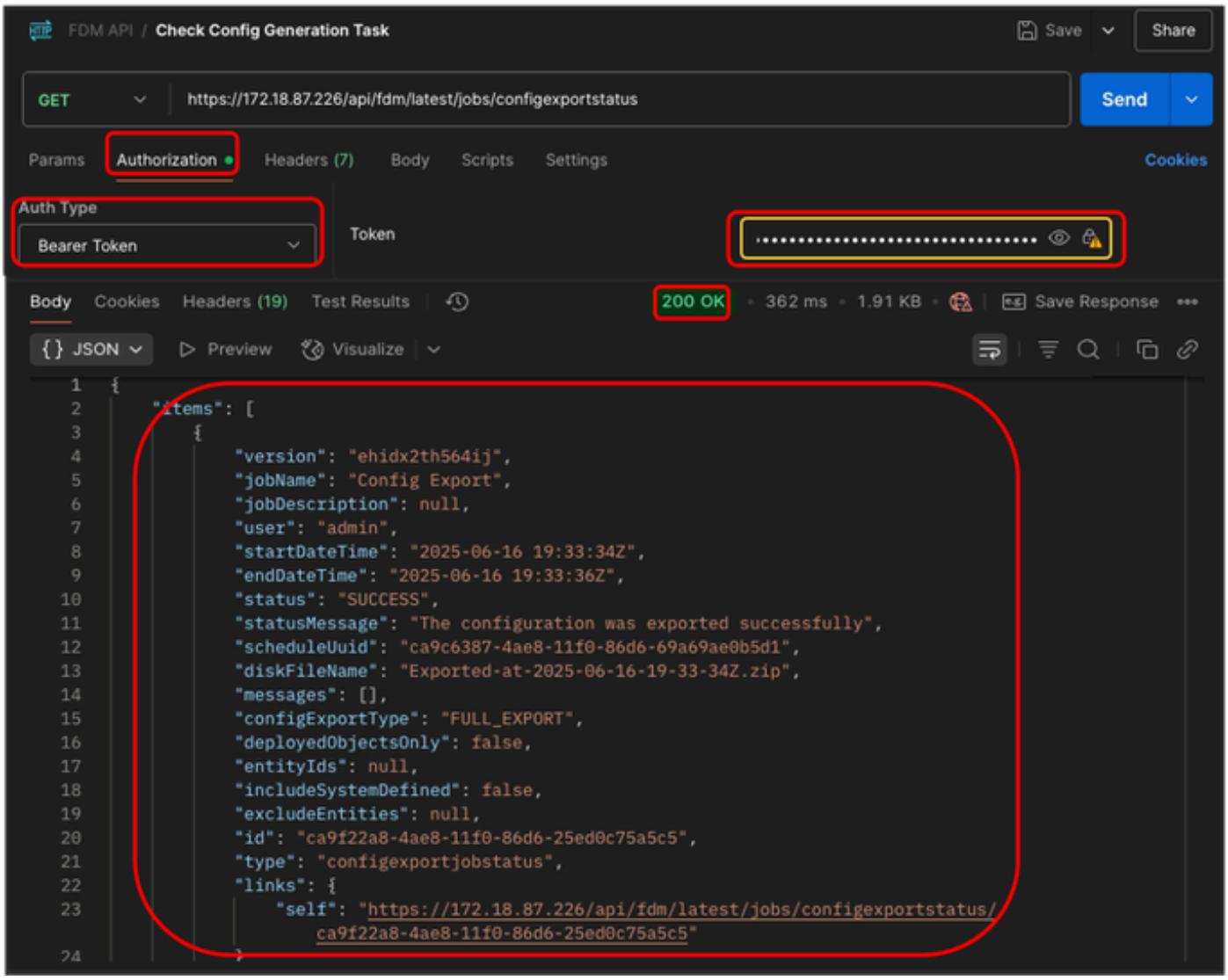
11. Repita a etapa 2 para criar uma nova solicitação. GET será usado desta vez.

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

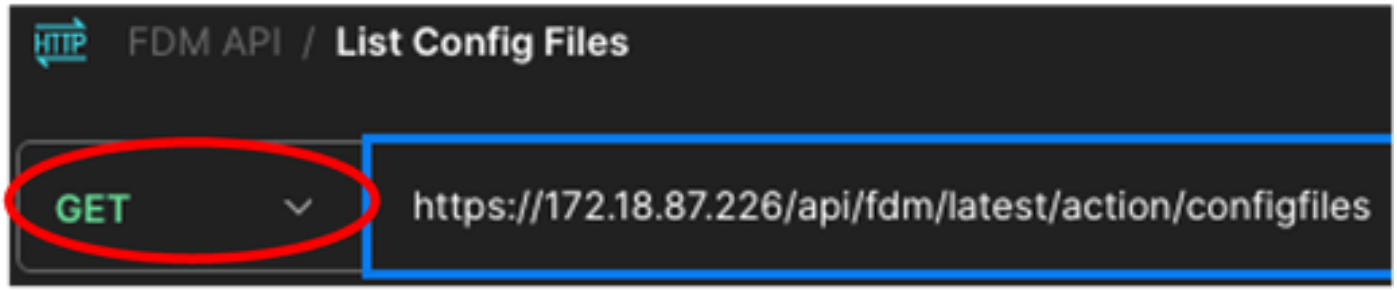
13. Na guia Autorização, selecione Token do Portador como Tipo de Autenticação no menu suspenso e, na caixa de texto ao lado de Token, cole o token copiado na etapa 5. Finalmente, clique em Enviar. Se tudo estiver bem, você receberá uma resposta 200 OK e, no campo JSON, o status da tarefa e outros detalhes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

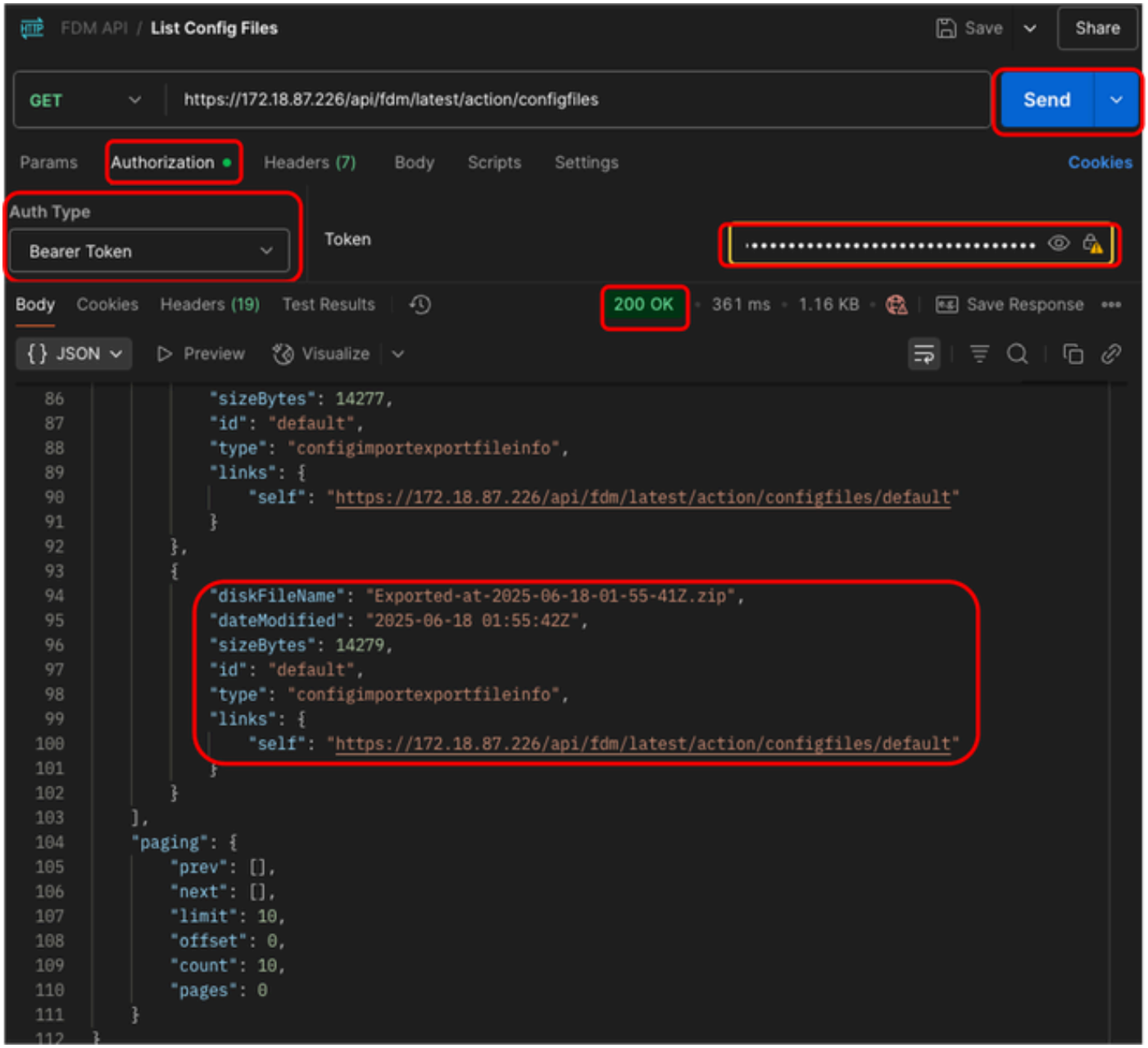
15. Chame essa nova solicitação: Listar arquivos de configuração. Ele será criado como uma solicitação GET, também no momento em que você estiver executando esta, GET deve ser selecionado no menu suspenso. Na caixa de texto ao lado de GET, introduza a linha seguinte https://<FDM IP ADD>/api/fdm/latest/action/configfiles




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.



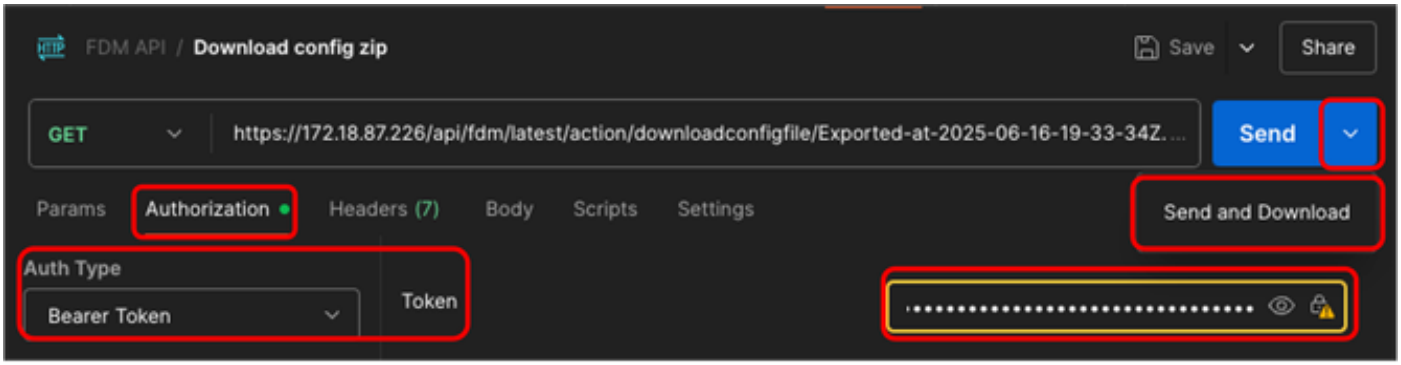

Postman - Solicitação de listagem de arquivos de configuração exportados - Autorização e saída

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 >

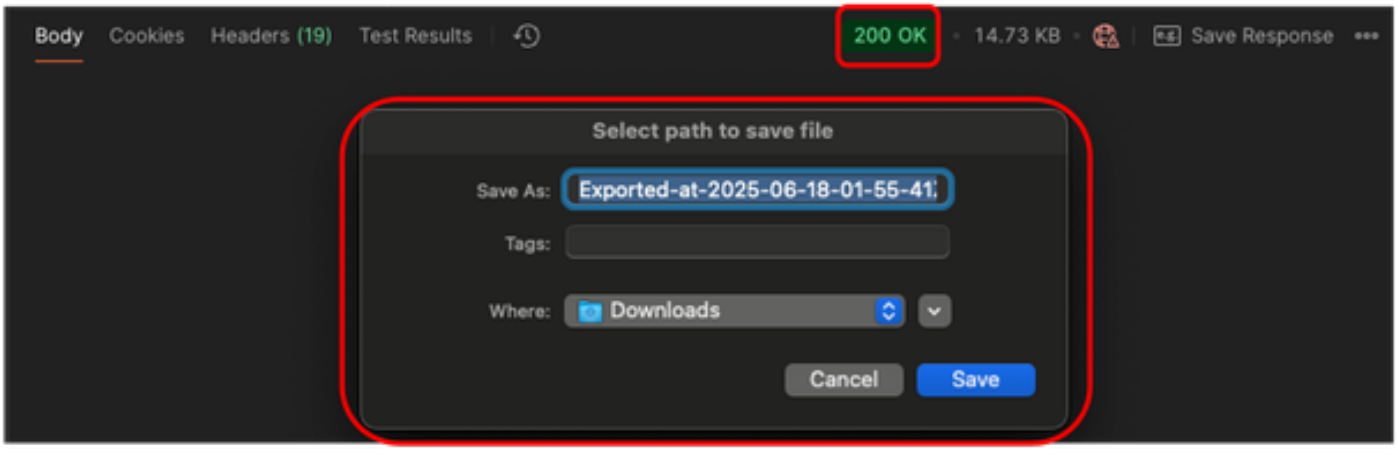

Postman - Fazer download da solicitação de arquivo Config.zip

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

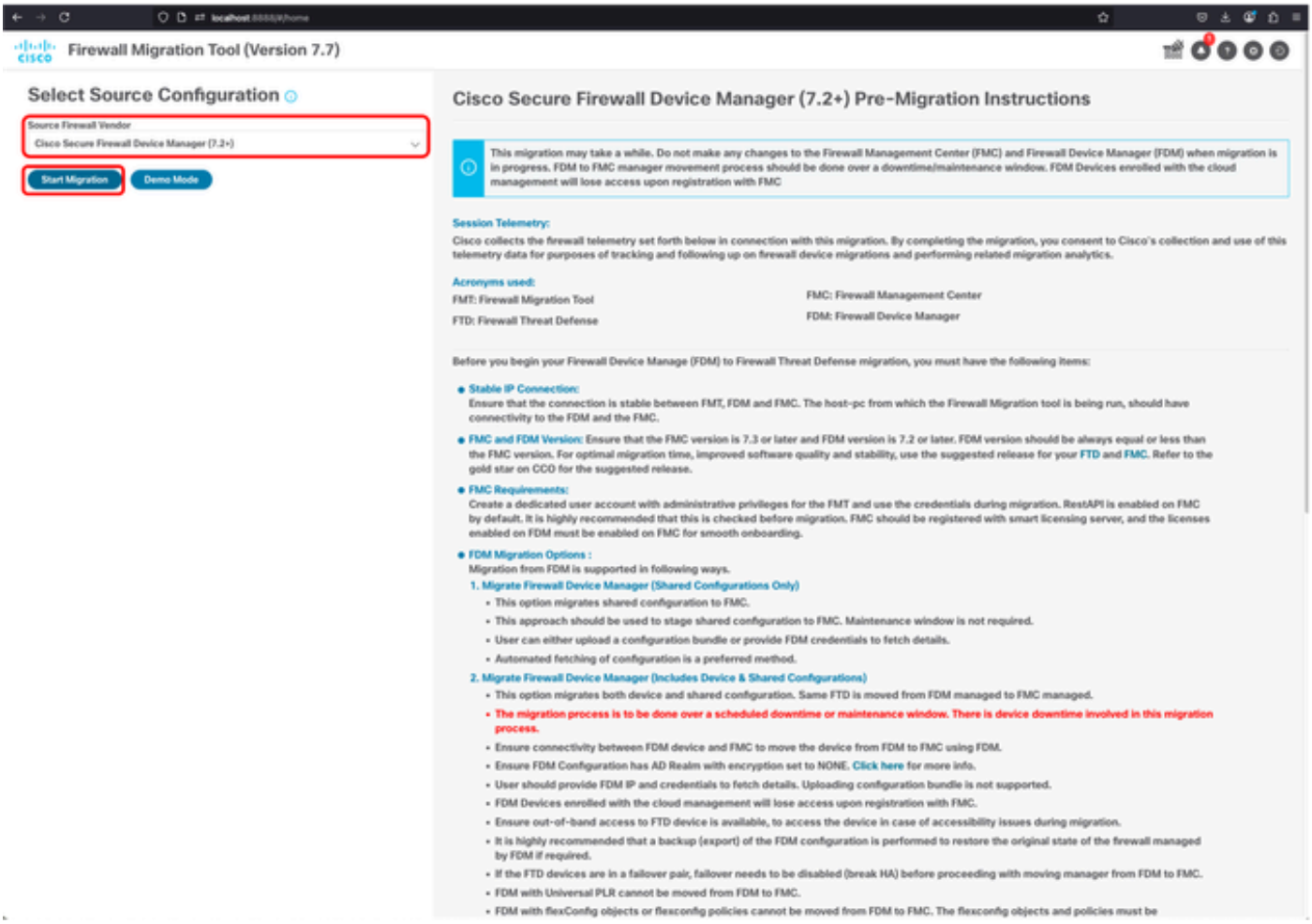
20. Se tudo estiver bem, você receberá uma resposta 200 OK e uma janela pop-up será exibida solicitando a pasta de destino onde o arquivo configuration.zip será salvo. Esse arquivo .zip agora pode ser carregado na Ferramenta de Migração de Firewall.




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

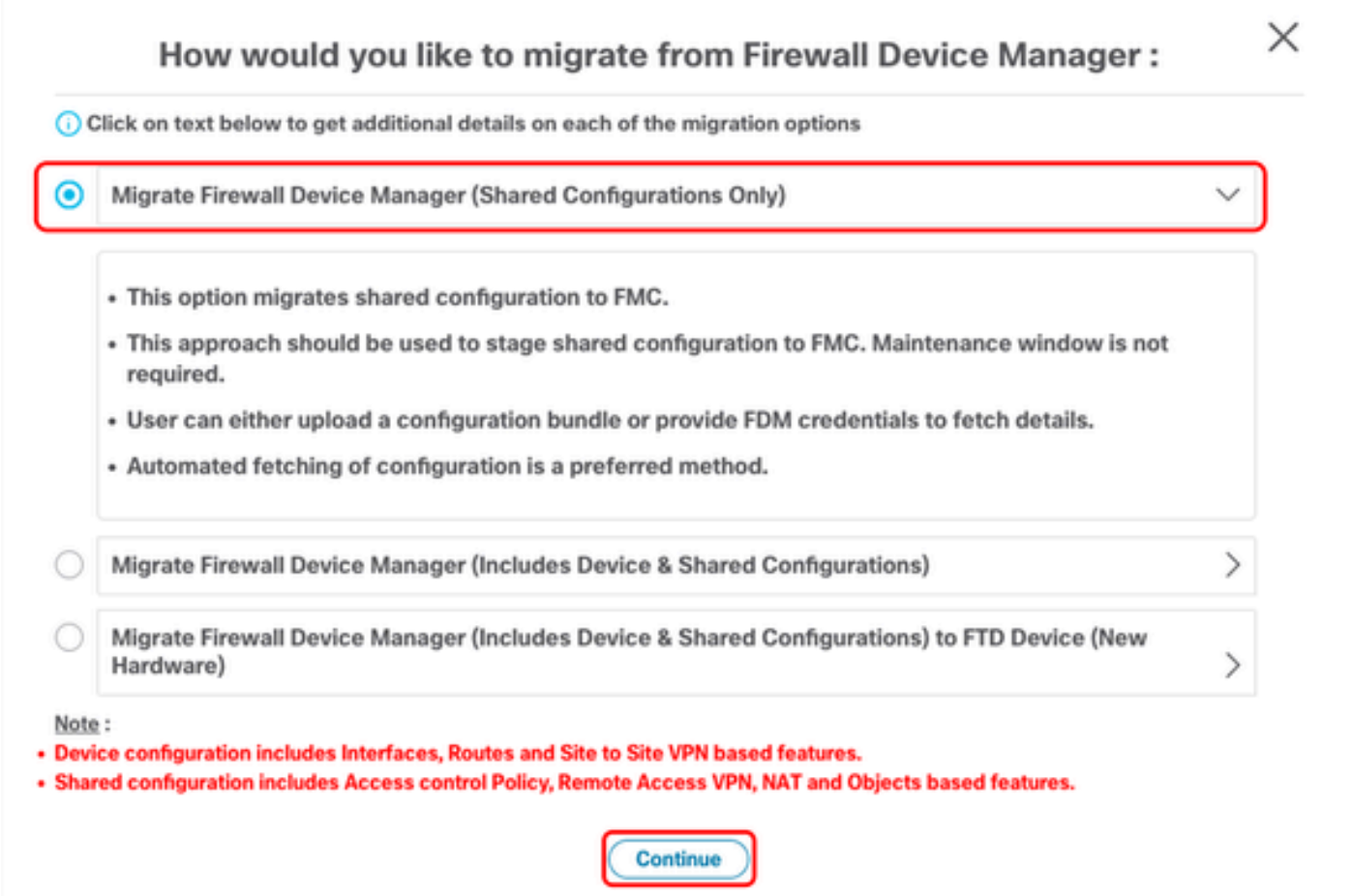
## Ferramenta de migração de firewall

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.



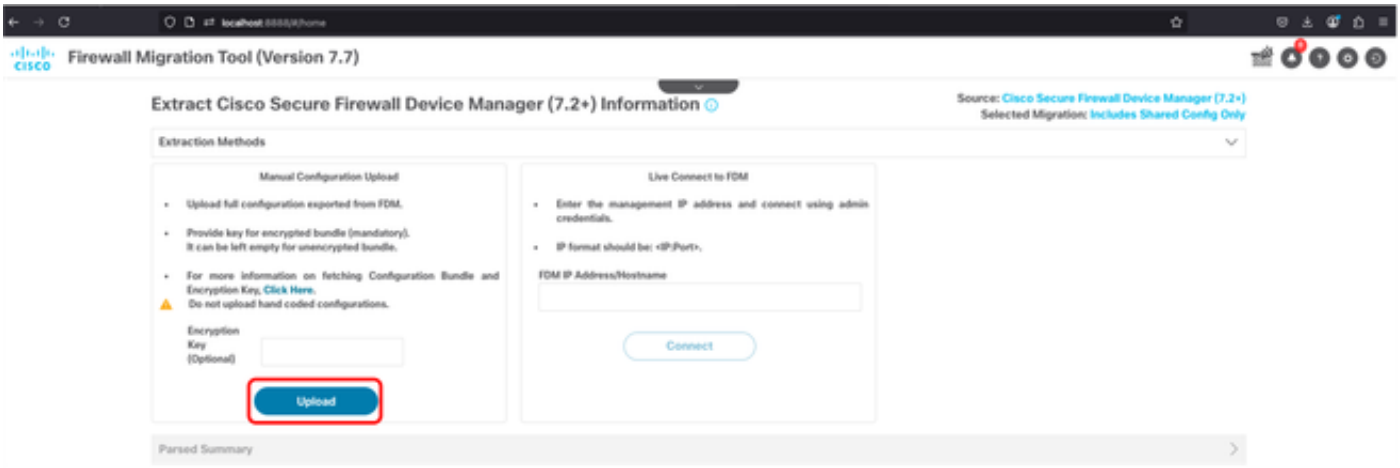

FMT - Seleção do FDM

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



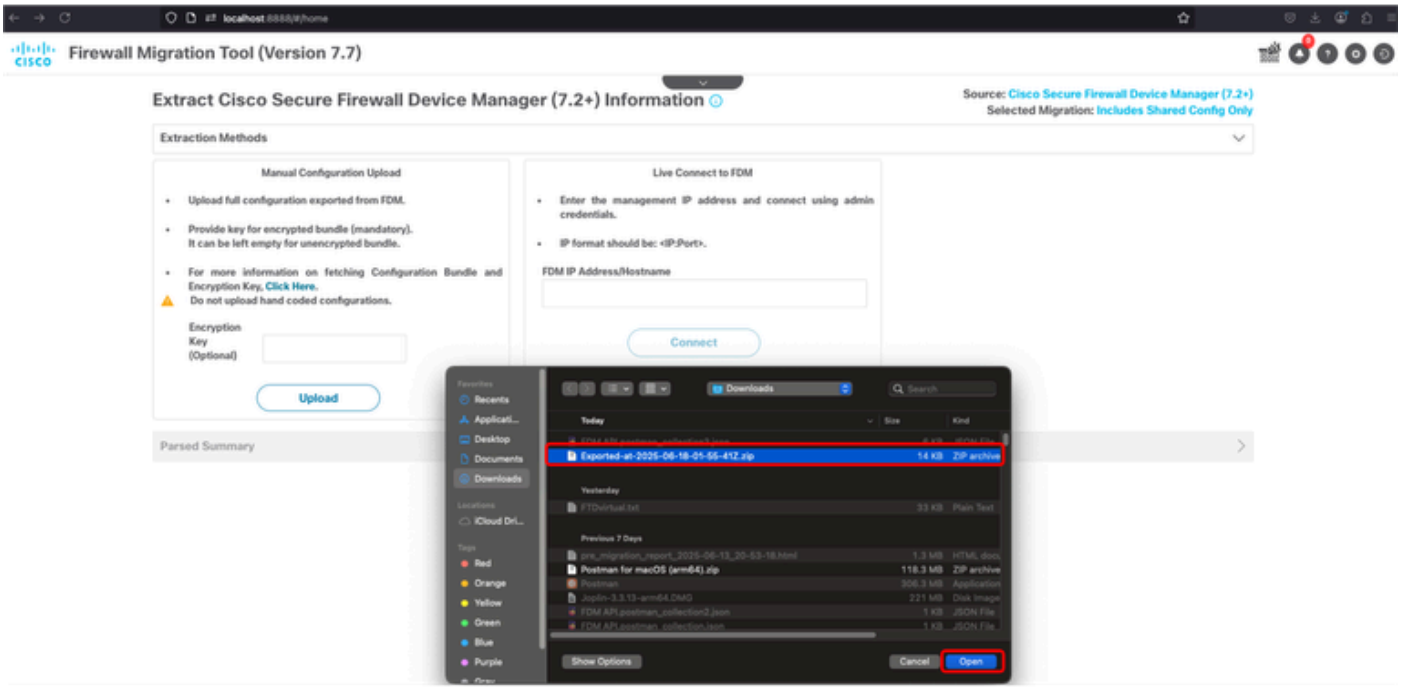

FMT - Somente Configurações Compartilhadas de Migração do FDM

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



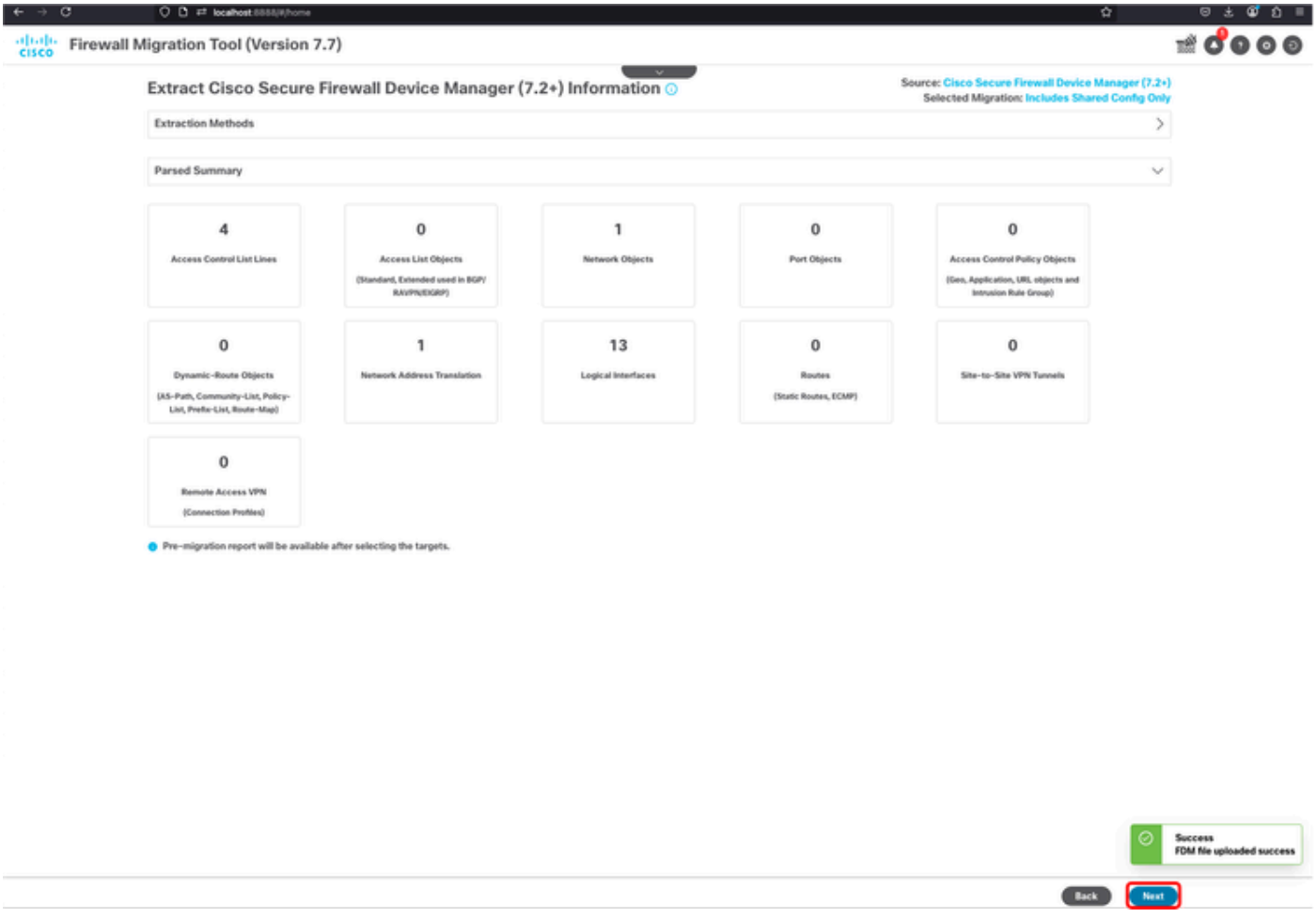

FMT - Carregar arquivo Config.zip

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



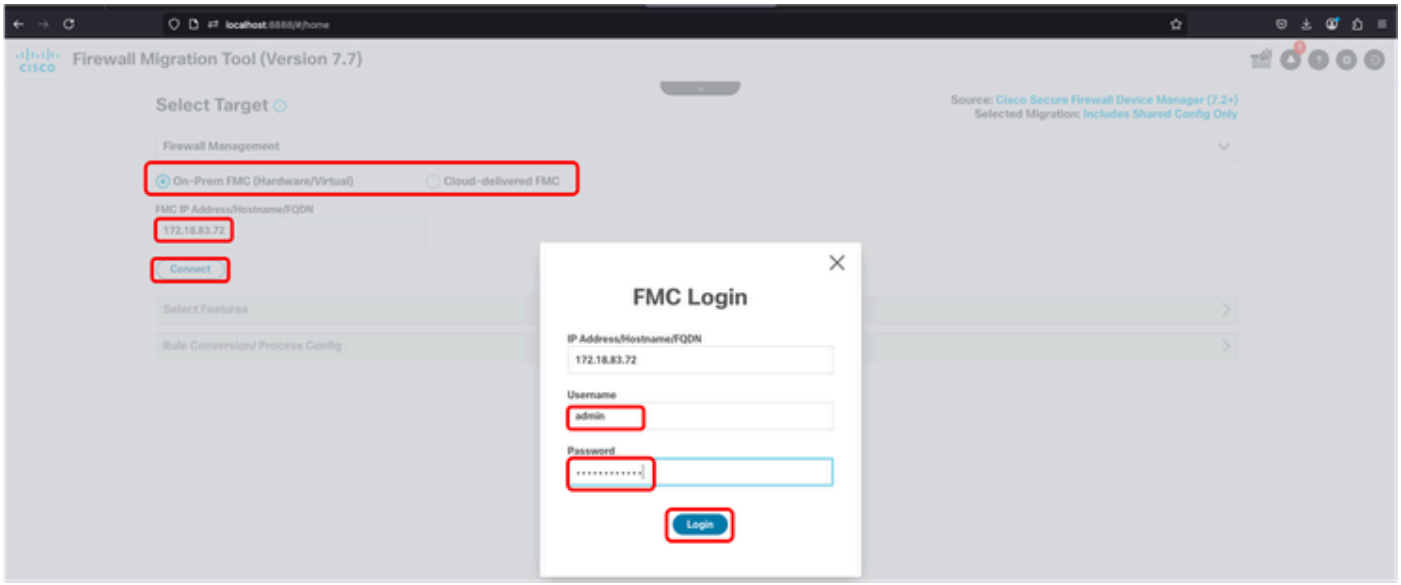

FMT - Seleção de arquivo Config.zip

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.



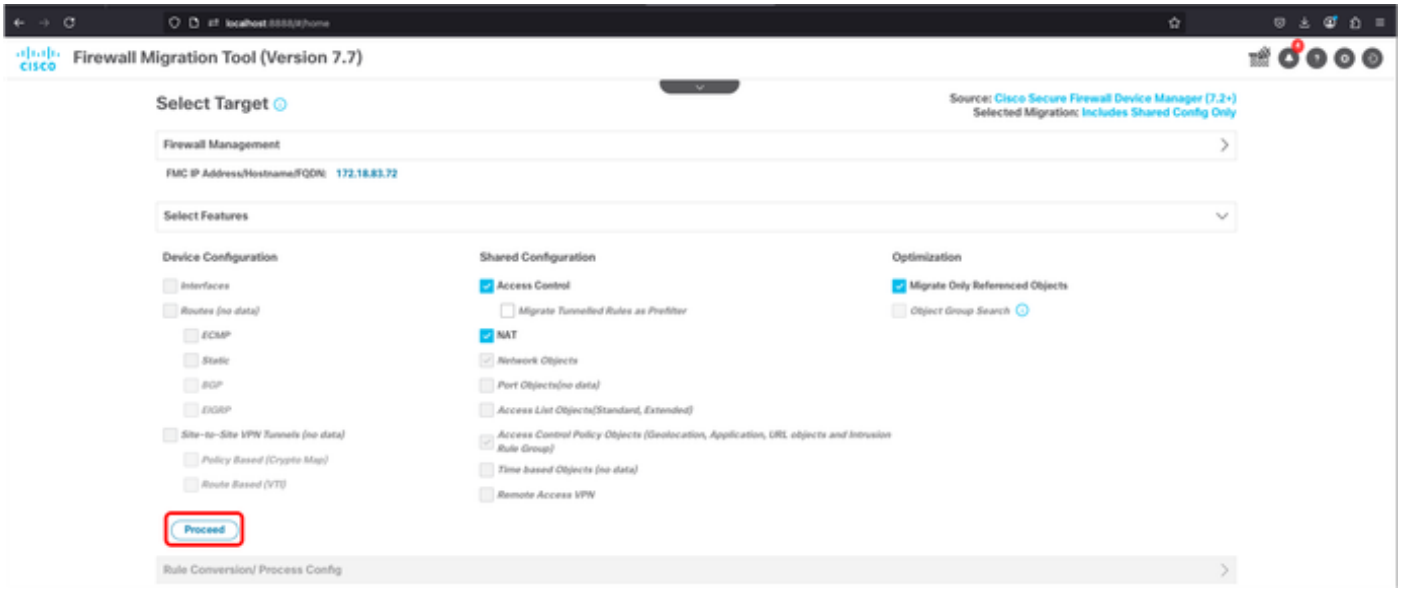

FMT - Resumo de Análise

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.

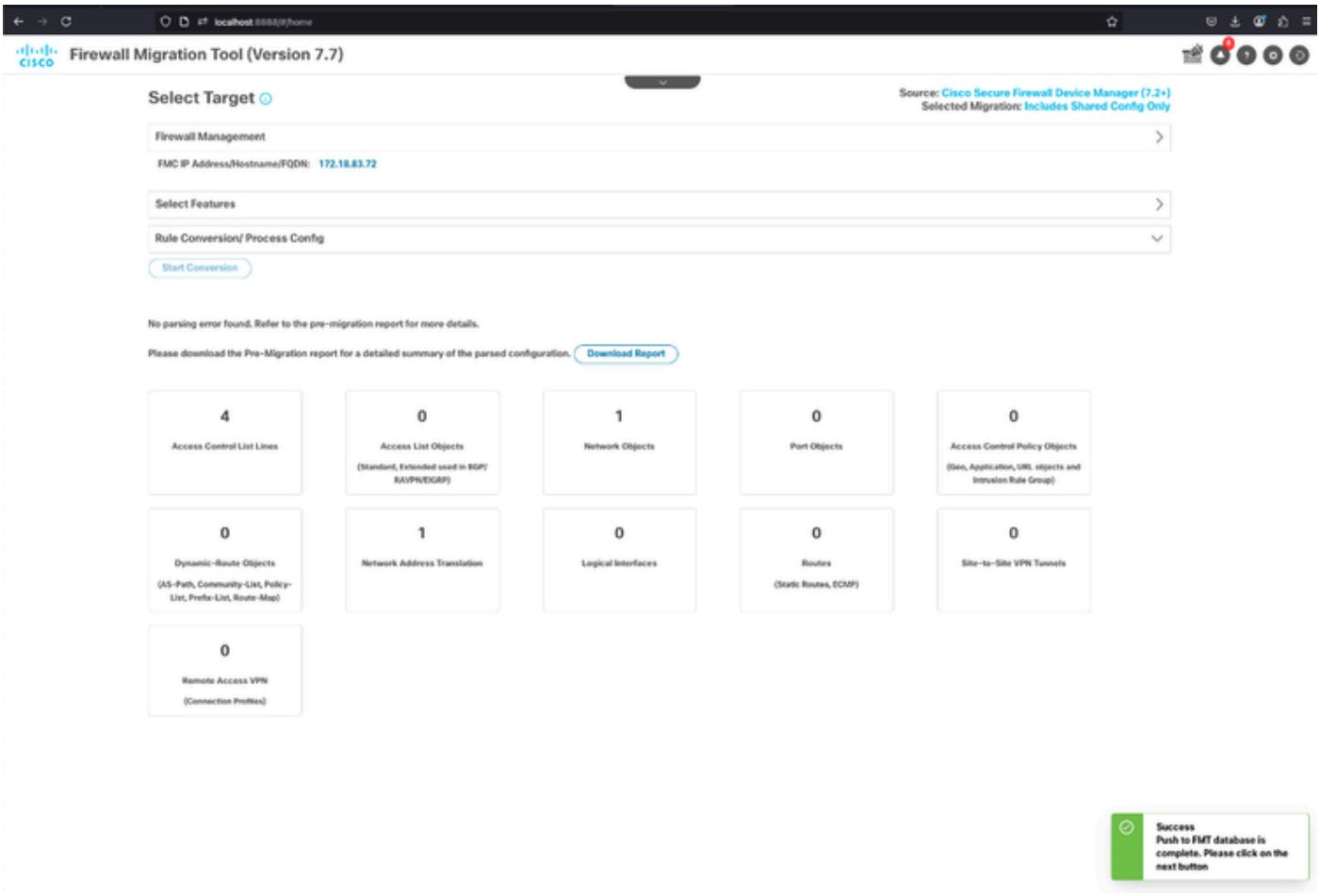



FMT - Destino FMC - Seleção de recursos

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

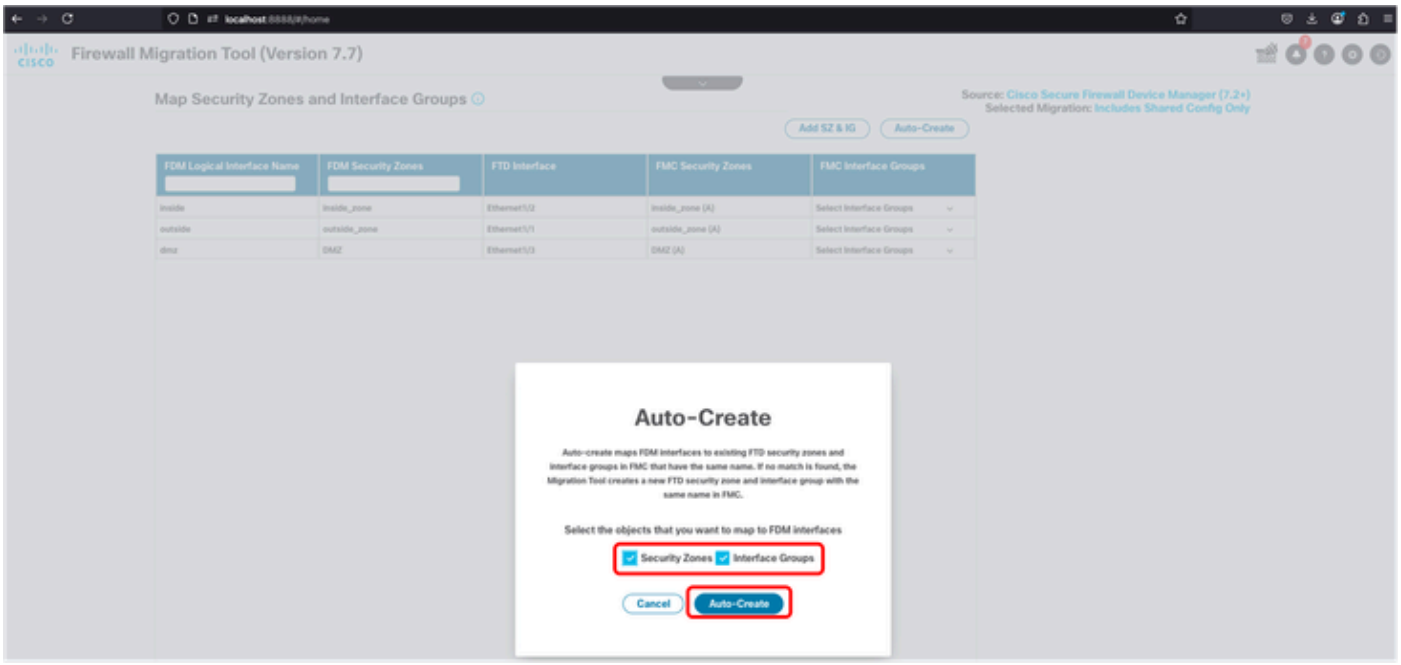

FMT - Iniciando a conversão da configuração

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.



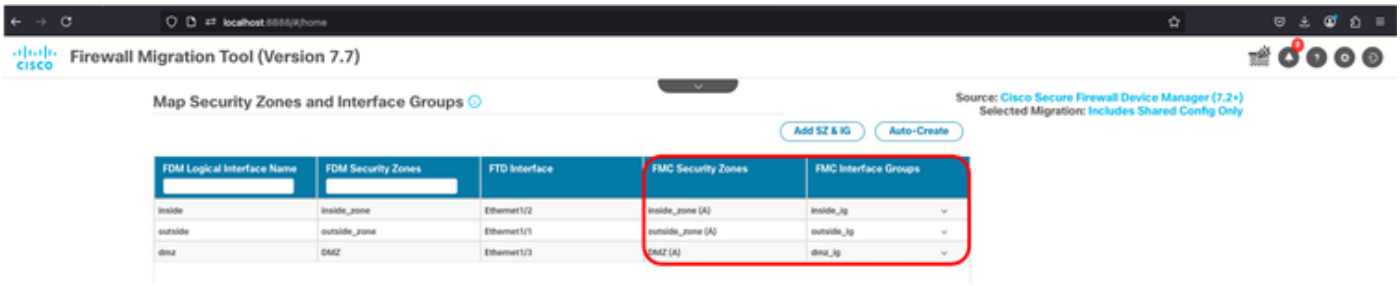

FMT - Envio de Banco de Dados Concluído com Êxito

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.



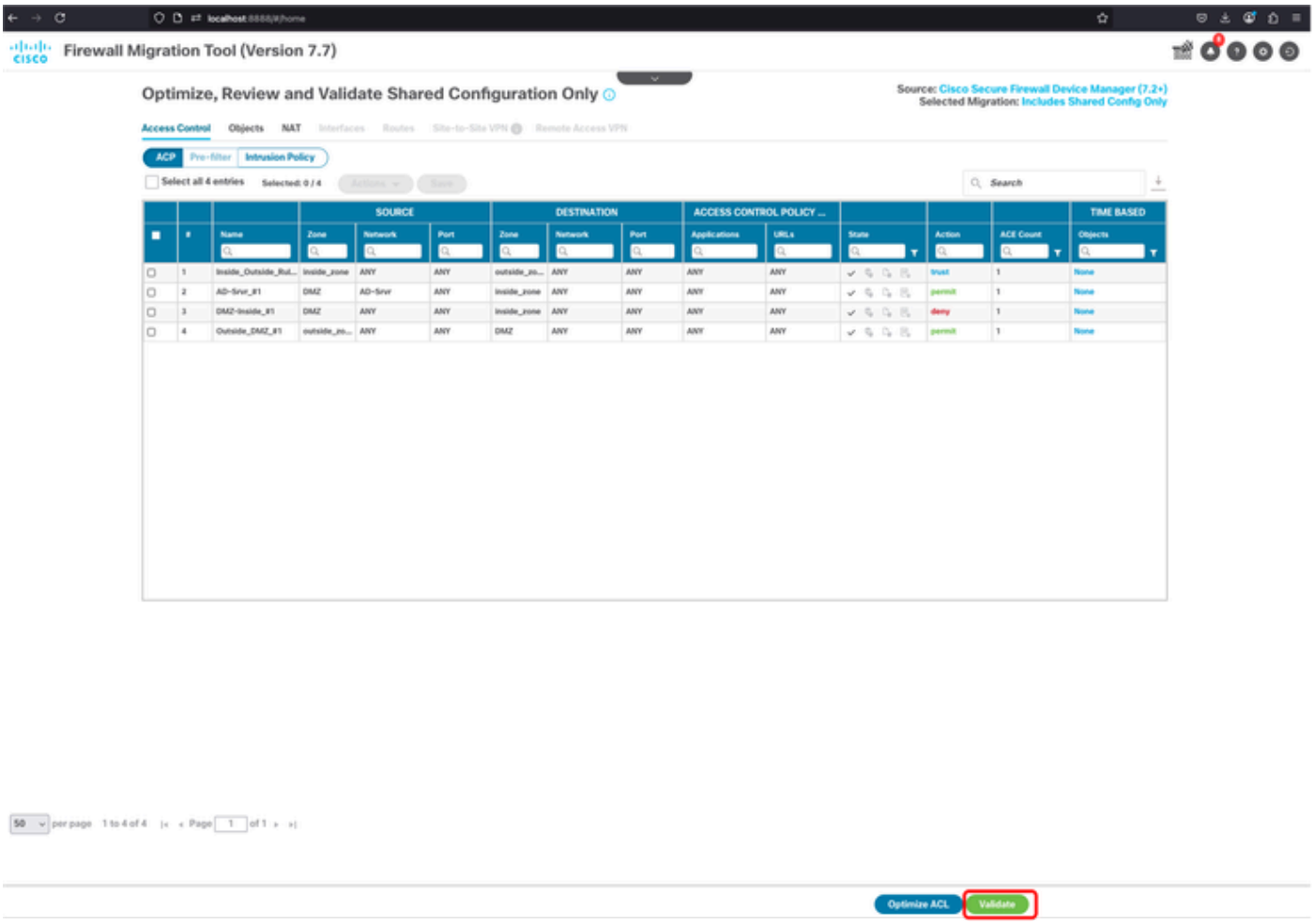

FMT - Criação Automática de Zonas de Segurança e Grupos de Interface

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



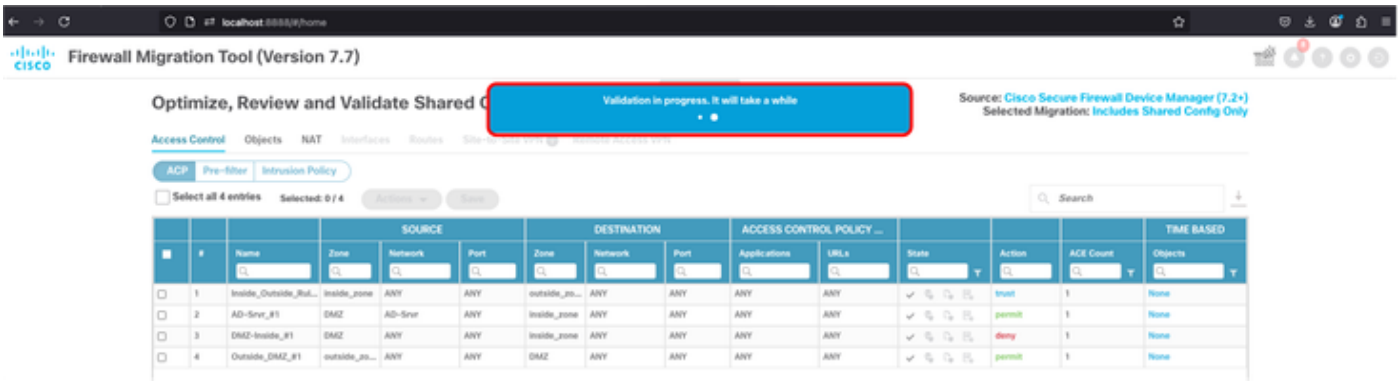

FMT - Zonas de segurança e grupos de interface criados com êxito

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



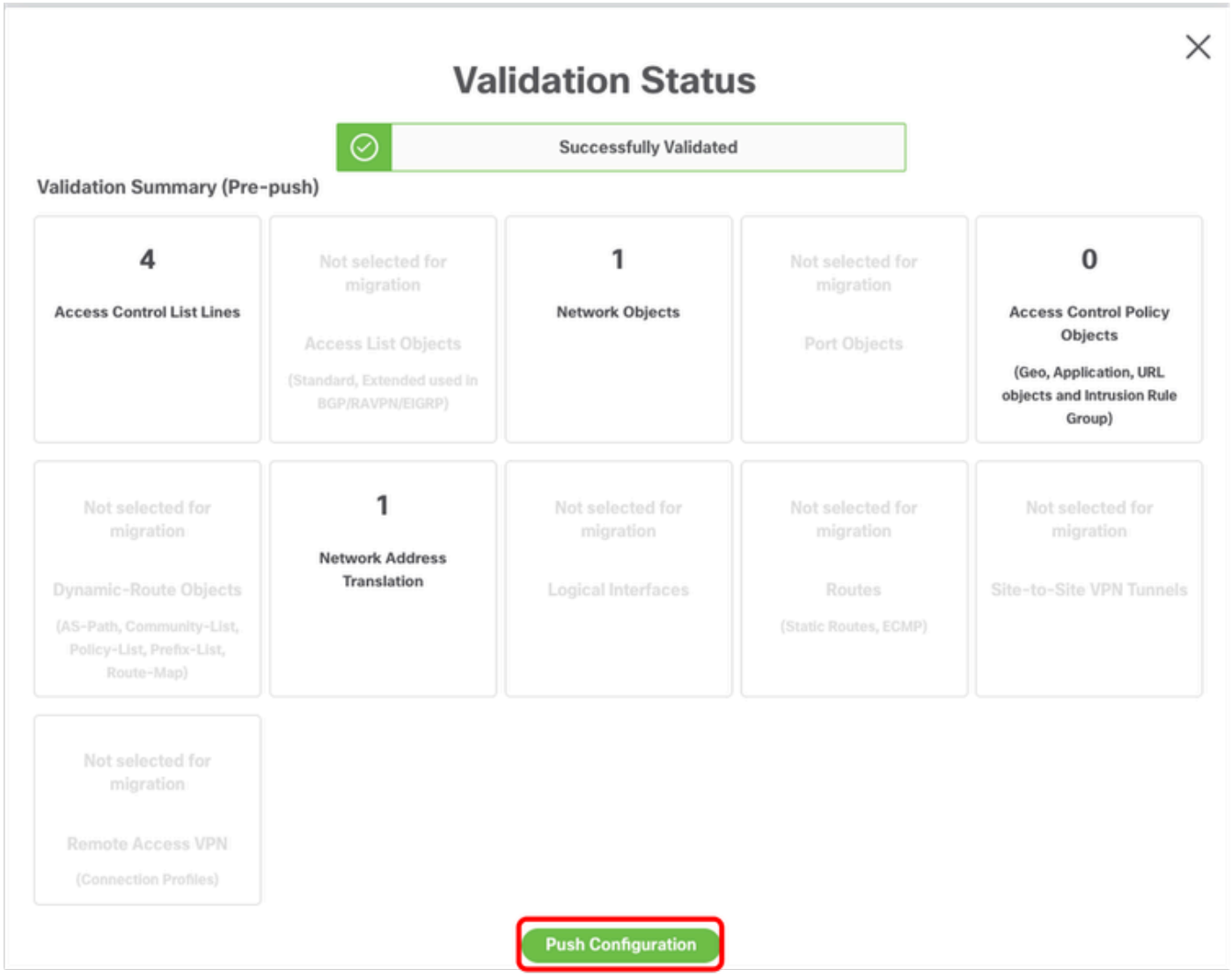

FMT - Otimizar ACL - Validar Migração

33. A validação demora alguns minutos para ser concluída.



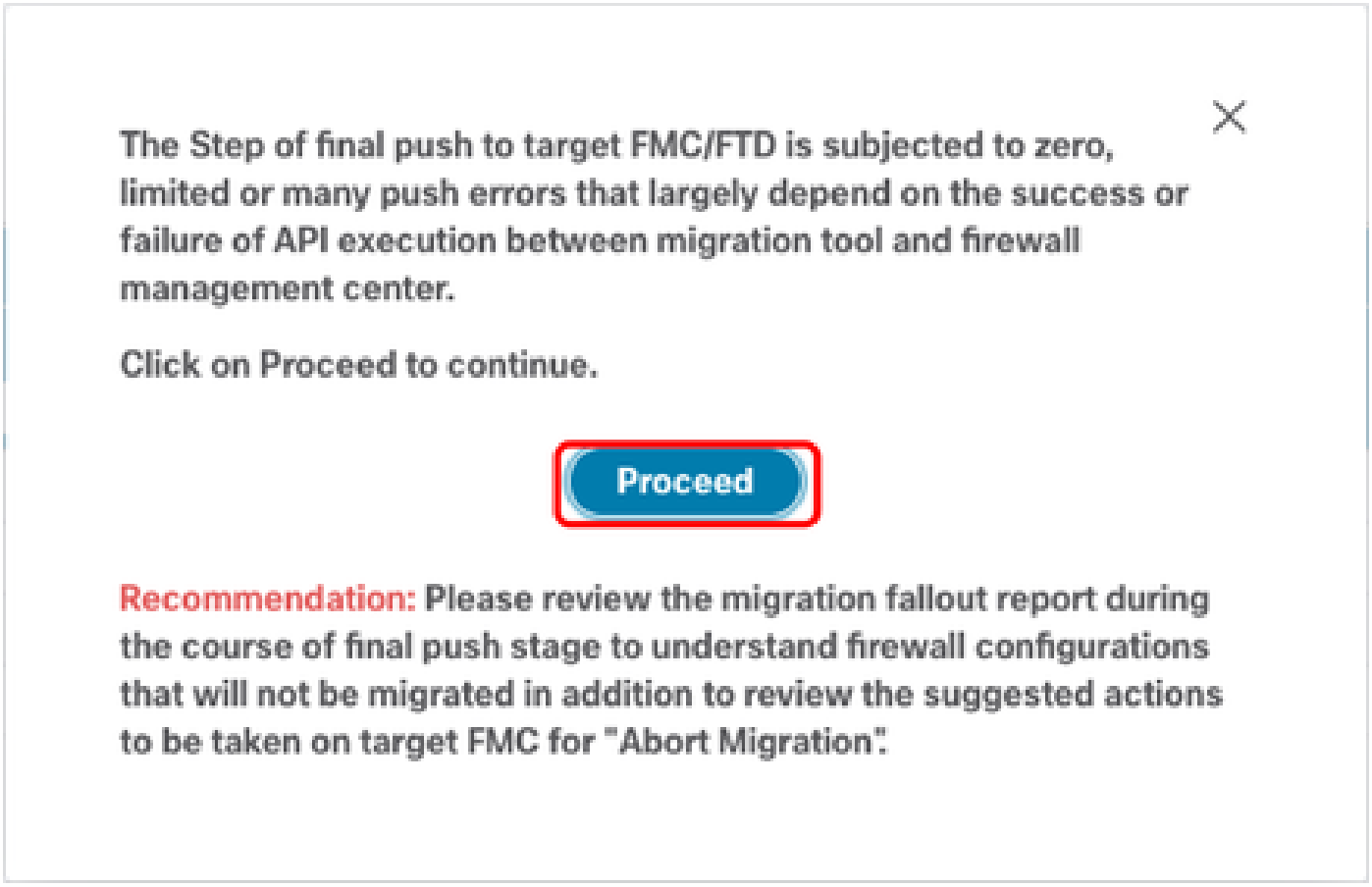

FMT - Validação em Andamento

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.



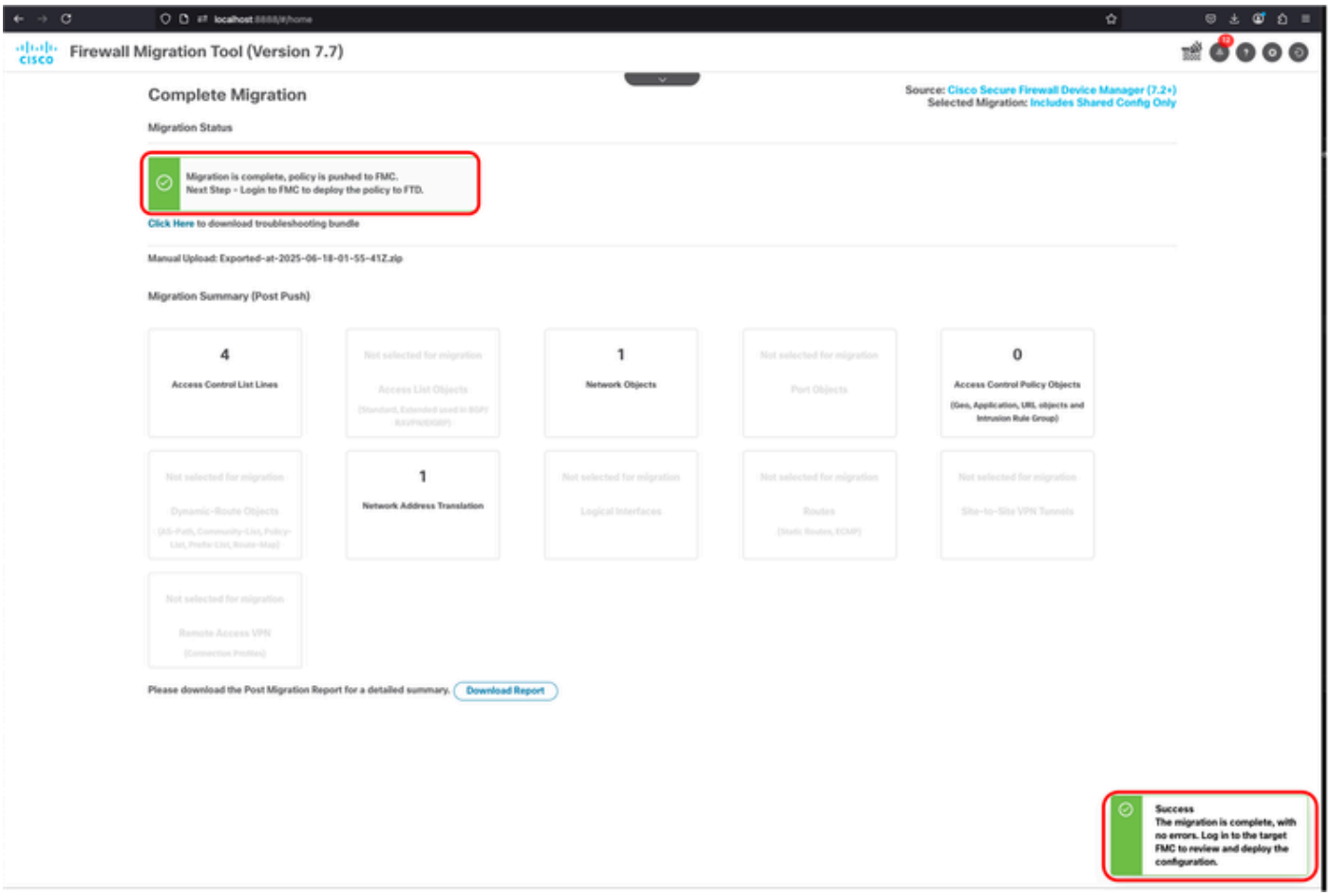

FMT - Validação Bem-sucedida - Enviar Configuração para FMC

35. Finalmente, clique no botão Prosseguir.




FMT - Prosseguir com envio de configuração

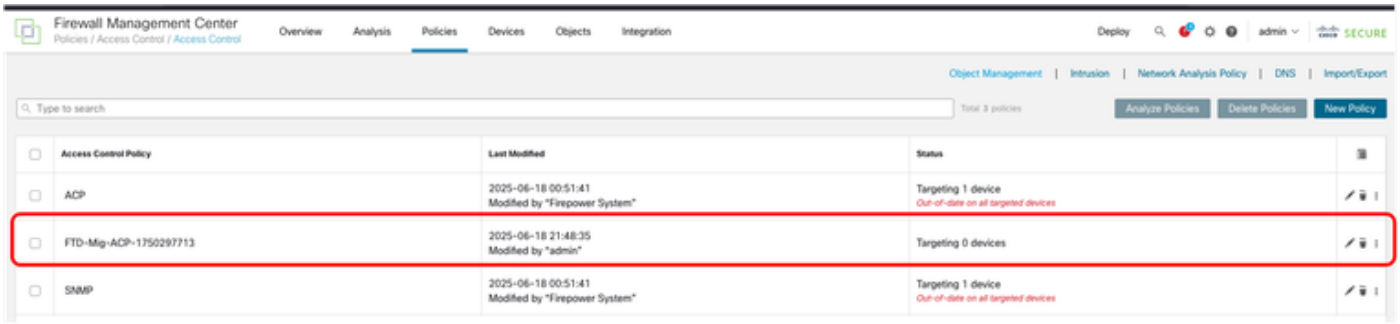
36. Se tudo correr conforme esperado, será exibida a notificação de Migração bem-sucedida. O FMT solicita que você faça login no FMC e implante a política migrada no FTD.



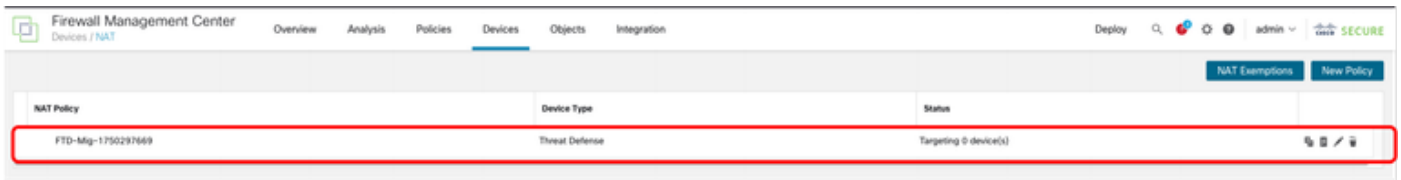

FMT - Notificação de Migração Bem-sucedida

## 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.