Migration von FDM zu FMC über FMT mit der Datei "Configuration.zip"

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die Konfigurationsdatei .zip eines Secure Firewall Device Manager (FDM) generiert wird, der mithilfe von FMT zu einem FMC migriert werden soll.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Firewall Threat Defense (FTD)
- Cisco Firewall Management Center (FMC)
- Firewall Migration-Tool (FMT)
- Postman-API-Plattform

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen.

FTD 7.4.2

FMC 7.4.2

FMT 7.7.0.1

Postbote 11.50.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

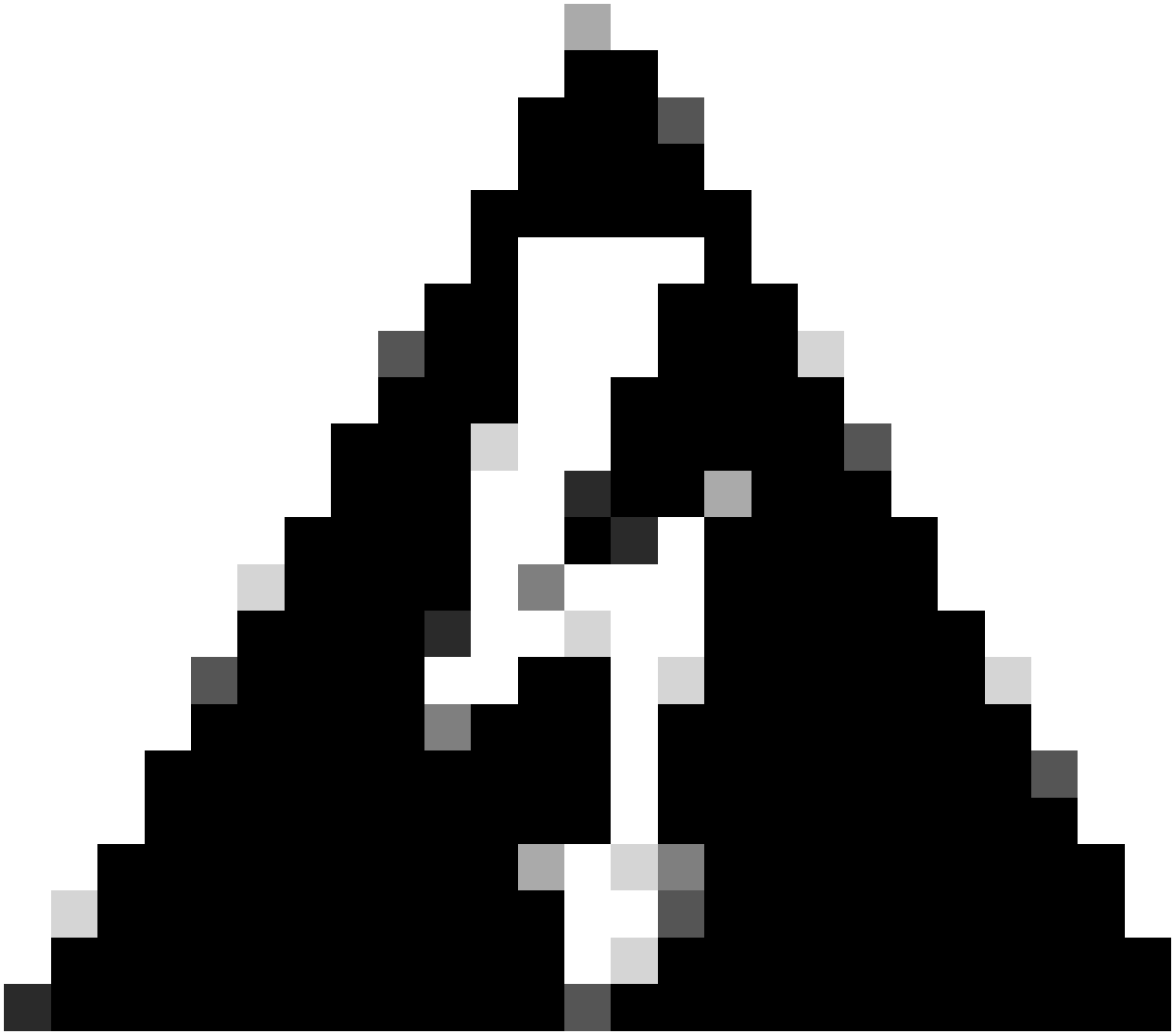
Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

- FDM kann jetzt auf verschiedene Weise zu FMC migriert werden. In diesem Dokument wird das Szenario untersucht, in dem die ZIP-Konfigurationsdatei mithilfe von API-Anforderungen generiert und später an FMT hochgeladen wird, um die Konfiguration zu FMC zu migrieren.
- Die in diesem Dokument beschriebenen Schritte beginnen direkt mit Postman. Es wird daher empfohlen, Postman bereits installiert zu haben. Der PC oder Laptop, den Sie verwenden werden, müssen Zugriff auf FDM und FMC haben, auch FMT muss installiert sein und ausgeführt werden.

Überlegungen

- In diesem Dokument wird die ZIP-Konfigurationsdatei stärker als bei der FMT-Verwendung behandelt.
- Die FDM-Migration mit der ZIP-Konfigurationsdatei ist für nicht aktive Migrationen vorgesehen und erfordert nicht sofort eine FTD-Zieladresse.

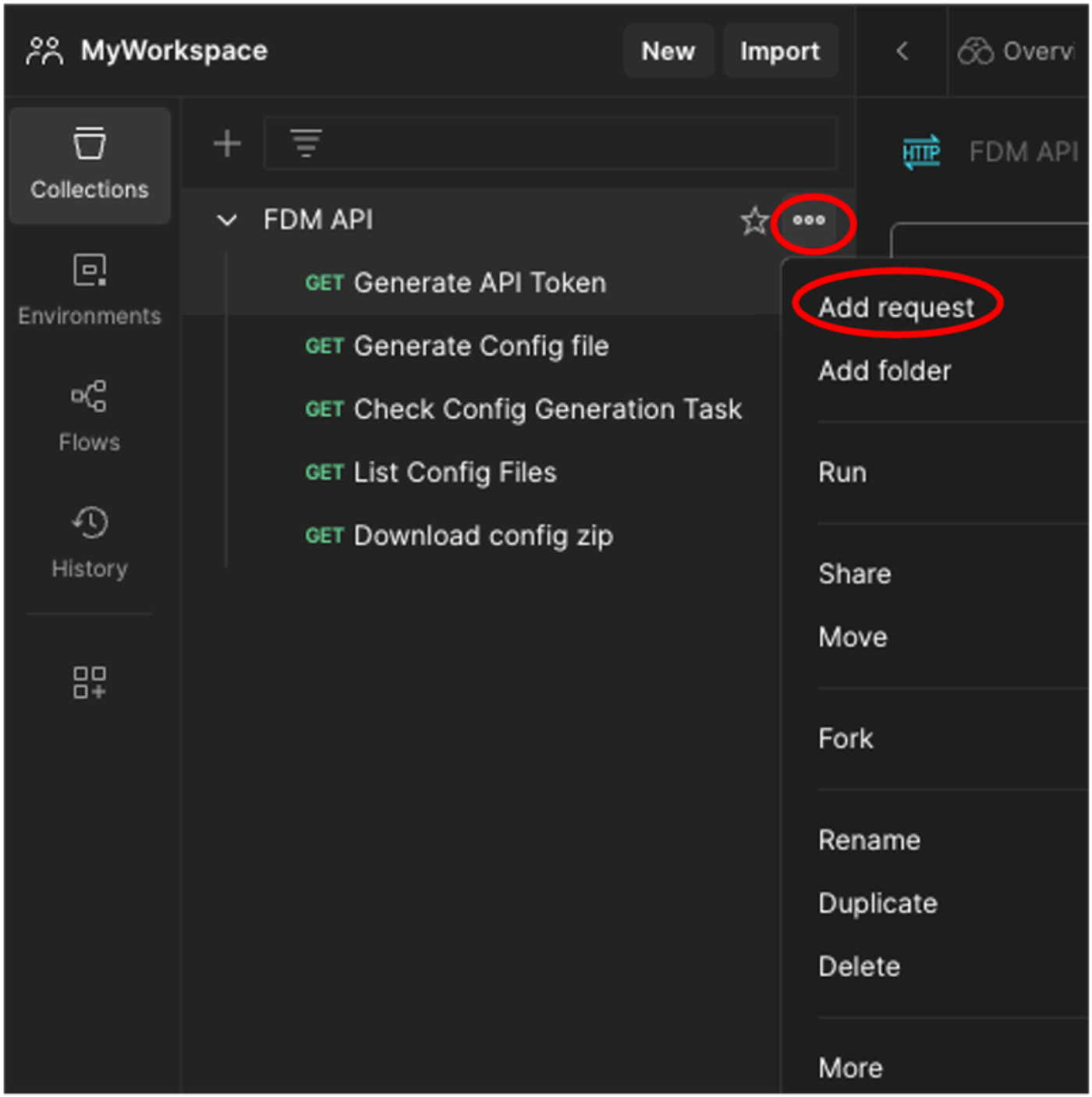


Warnung: Bei Auswahl dieses Modus können nur Zugriffskontrollrichtlinien (ACP), Network Address Translation Policy (NAT) und Objekte migriert werden. In Bezug auf die Objekte müssen diese in einer zu migrierenden ACP-Regel oder NAT verwendet werden, andernfalls werden sie ignoriert.

Konfiguration

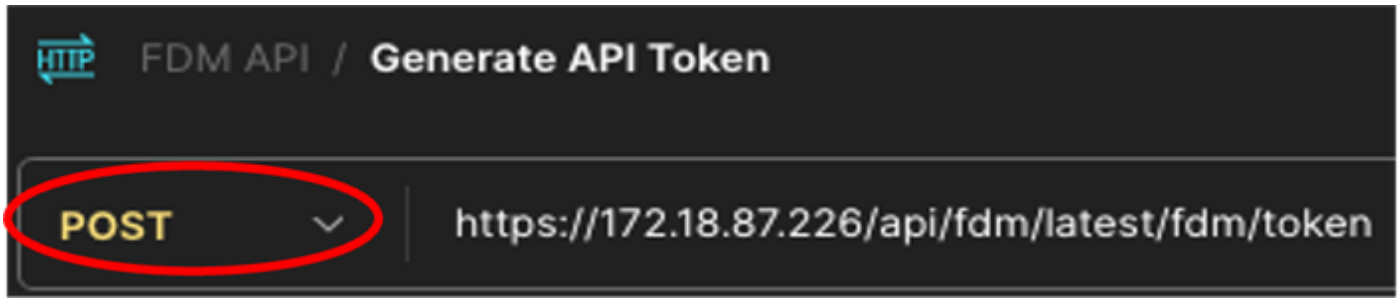
API-Anfragen - Post

1. Erstellen Sie in Postman eine neue Sammlung (in diesem Szenario wird FDM API verwendet).
2. Klicken Sie auf die drei Punkte und anschließend auf Add request (Anforderung hinzufügen).



Postman - Sammlung erstellen und Ergänzung beantragen

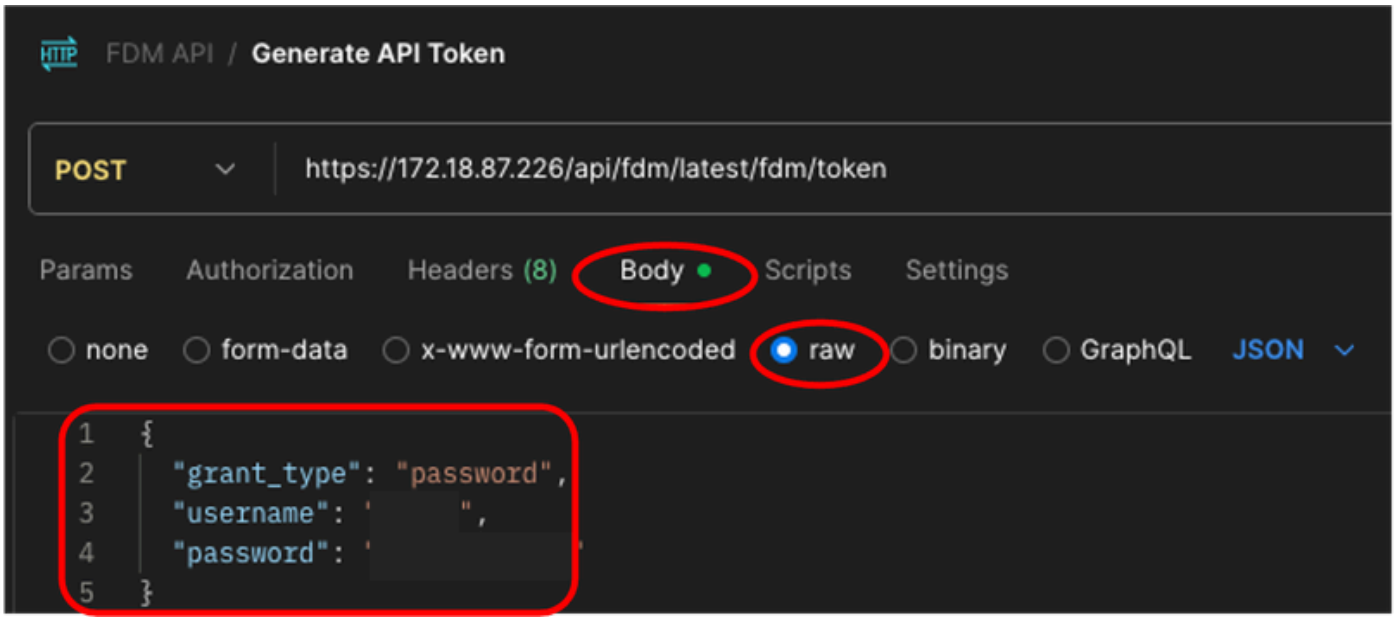
3. Neue Anforderung anrufen: API-Token generieren. Sie wird als GET-Anforderung erstellt. Zum Zeitpunkt der Ausführung muss jedoch POST aus dem Dropdown-Menü ausgewählt werden. Im Textfeld neben POST die nächste Zeile vorstellen: https://<FDM IP ADD>/api/fdm/latest/fdm/token



Postman - Token-Anfrage

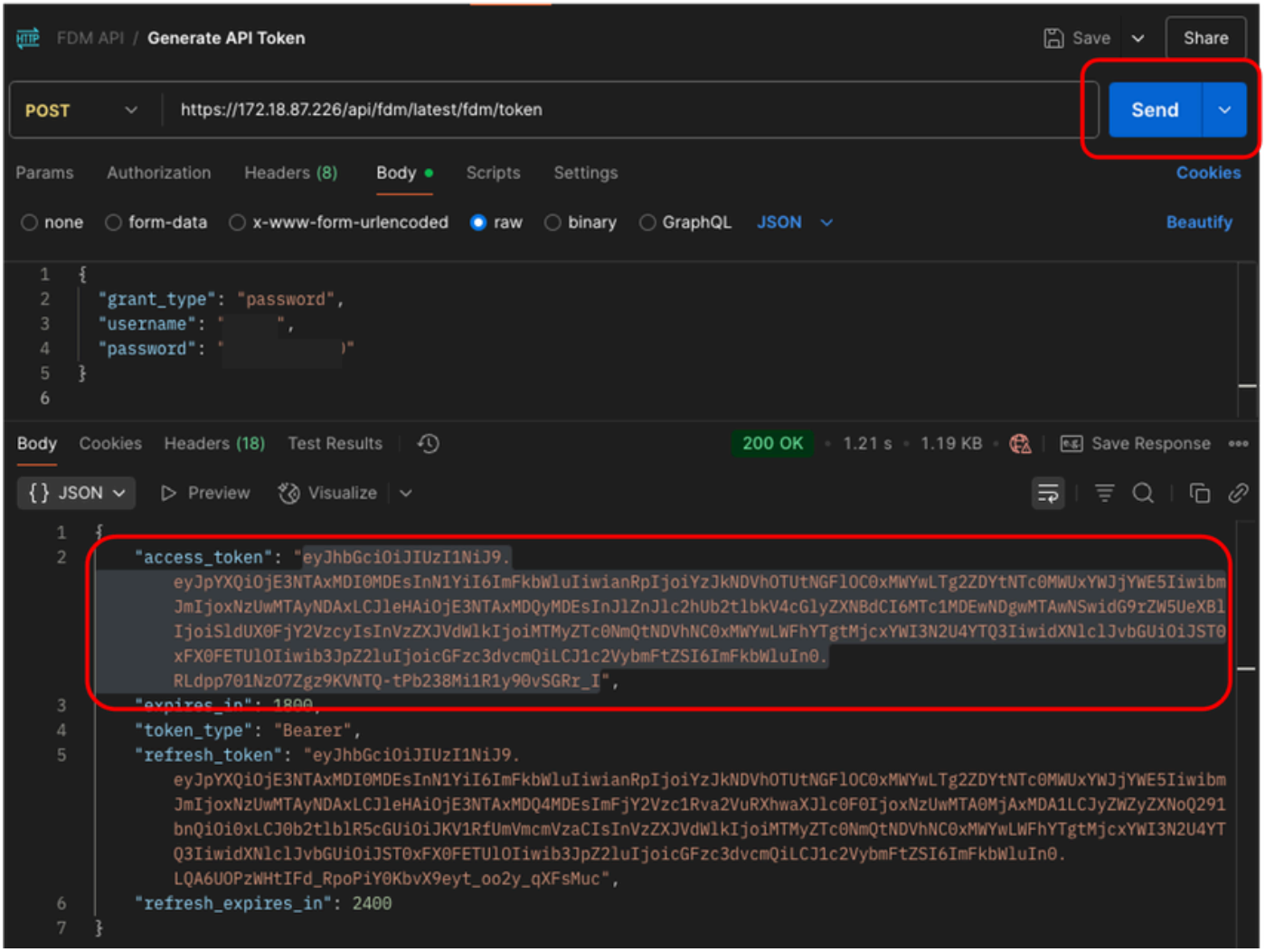
4. Wählen Sie auf der Registerkarte Body die Option raw aus, und stellen Sie die Anmeldeinformationen für den Zugriff auf das FTD-Gerät (FDM) in diesem Format vor.

```
{
   "Grande_type": "Kennwort",
   "Benutzername": "Benutzername",
   "Kennwort": "Kennwort"
}
```



Postman - Token-Anforderungstext

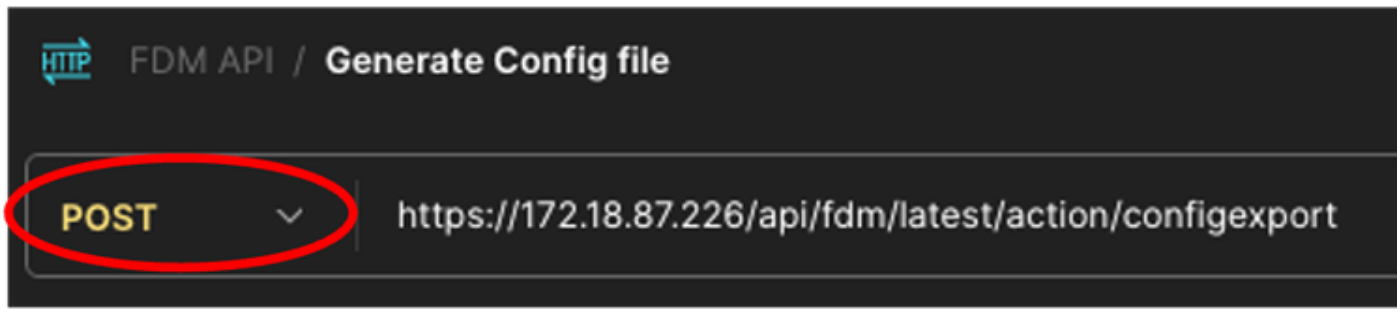
5. Klicken Sie abschließend auf Senden, um Ihr Zugriffs-Token zu erhalten. Wenn alles in Ordnung ist, erhalten Sie eine 200 OK Antwort. Erstellen Sie eine Kopie des gesamten Tokens (innerhalb der doppelten Anführungszeichen), da es in späteren Schritten verwendet wird.



Postman - Token erfolgreich generiert

6. Wiederholen Sie Schritt 2, um eine neue Anforderung zu erstellen, POST wird erneut verwendet.

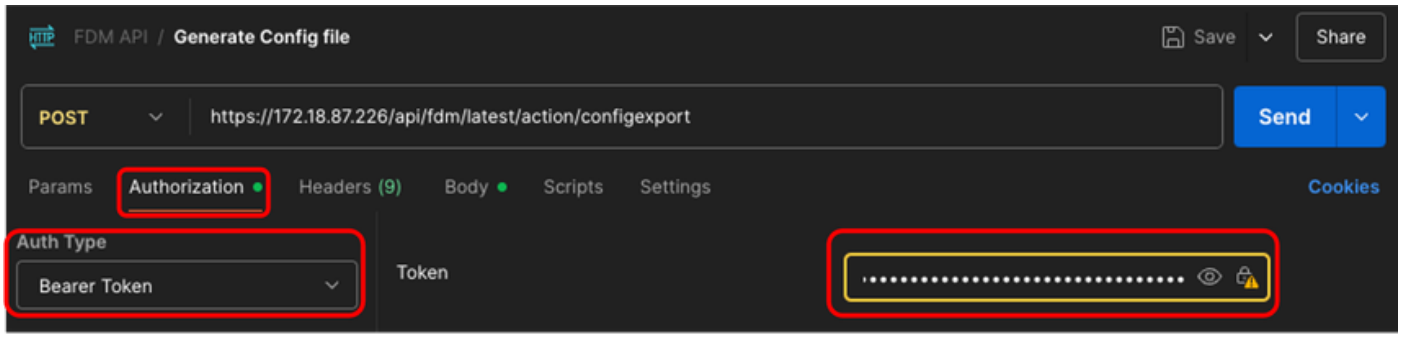
7. Diese neue Anforderung aufrufen: Erstellen der Konfigurationsdatei Sie wird als GET-Anforderung erstellt. Zum Zeitpunkt der Ausführung muss jedoch POST aus dem Dropdown-Menü ausgewählt werden. Führen Sie im Textfeld neben POST die nächste Zeile https://<FDM IP ADD>/api/fdm/latest/action/configureExport ein.



Postman - Konfigurationsdateianforderung generieren

8. Wählen Sie auf der Registerkarte Autorisierung im Dropdown-Menü die Option Träger-Token als Authentifizierungstyp aus, und fügen Sie im Textfeld neben Token das in Schritt 5 kopierte

Token ein.



Postman - Generieren einer Konfigurationsdateianforderung - Autorisierung

9. Wählen Sie auf der Registerkarte Haupttext die Option unformatiert, und stellen Sie diese Informationen vor.

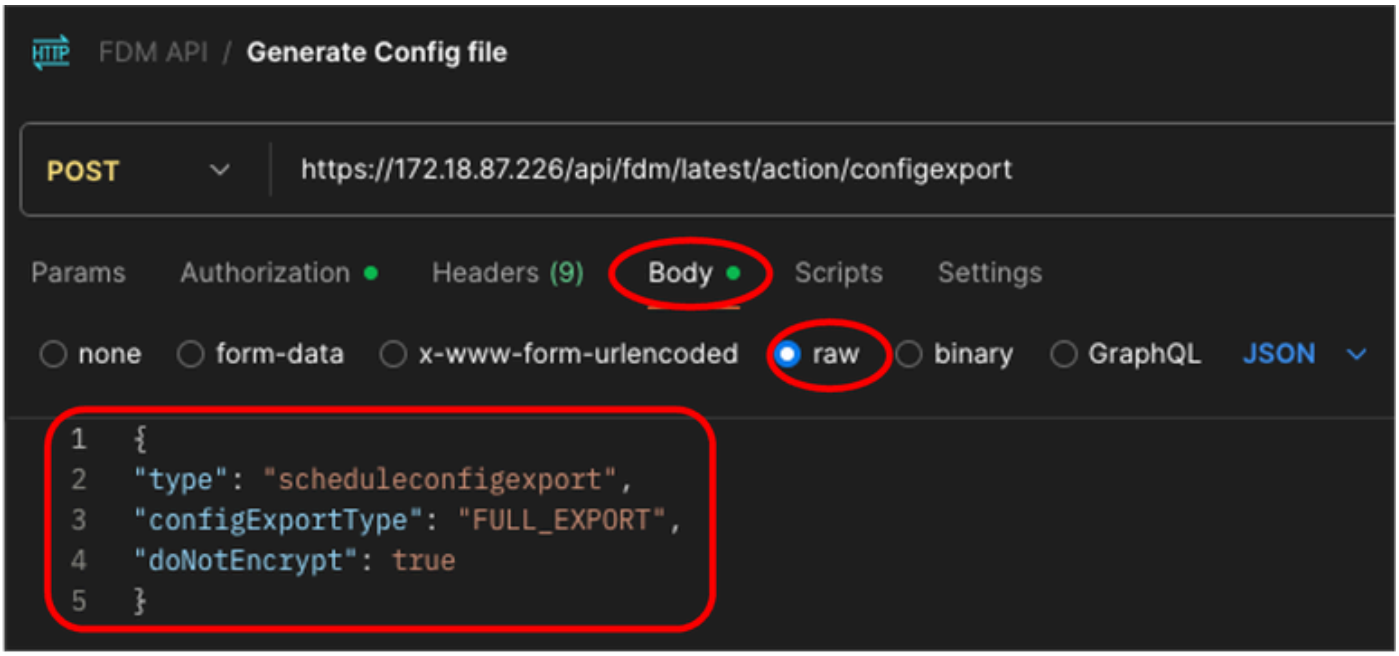
{

Typ: "Scheduleconfigexport",

"configExportType": "VOLLSTÄNDIGER EXPORT",

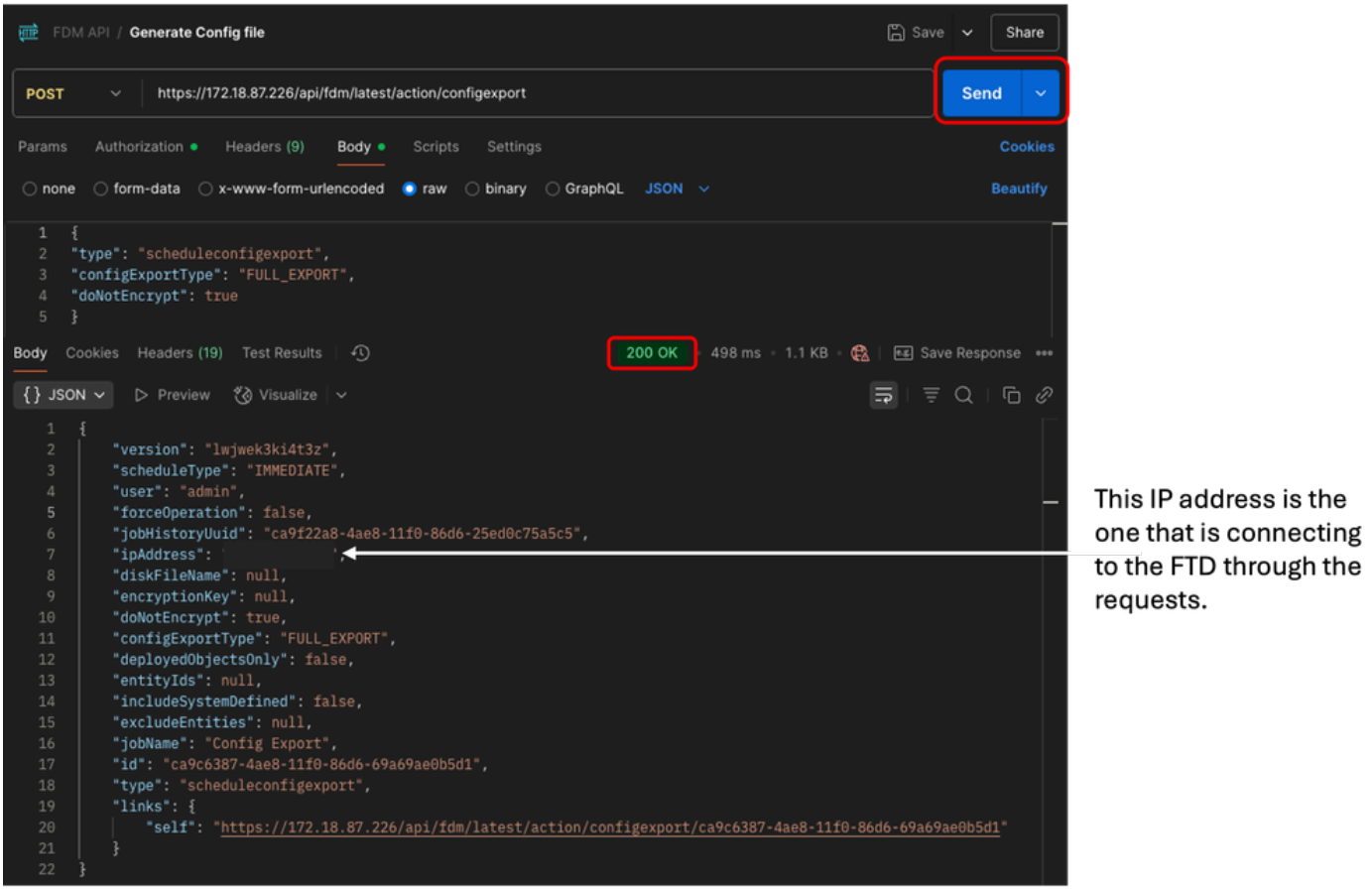
"doNotEncrypt": wahr

}



Postman - Generieren einer Konfigurationsdateianfrage - Text

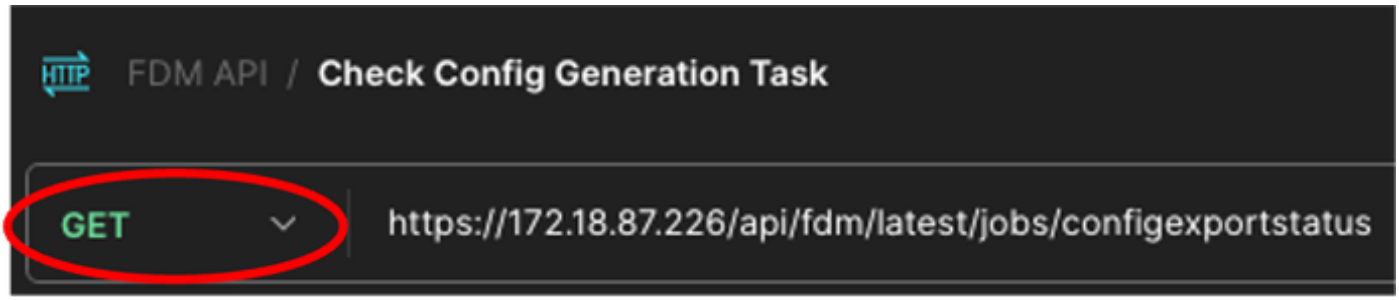
10. Klicken Sie abschließend auf Senden. Wenn alles in Ordnung ist, erhalten Sie eine 200 OK Antwort.



Postman - Generieren einer Konfigurationsdateianforderung - Ausgabe

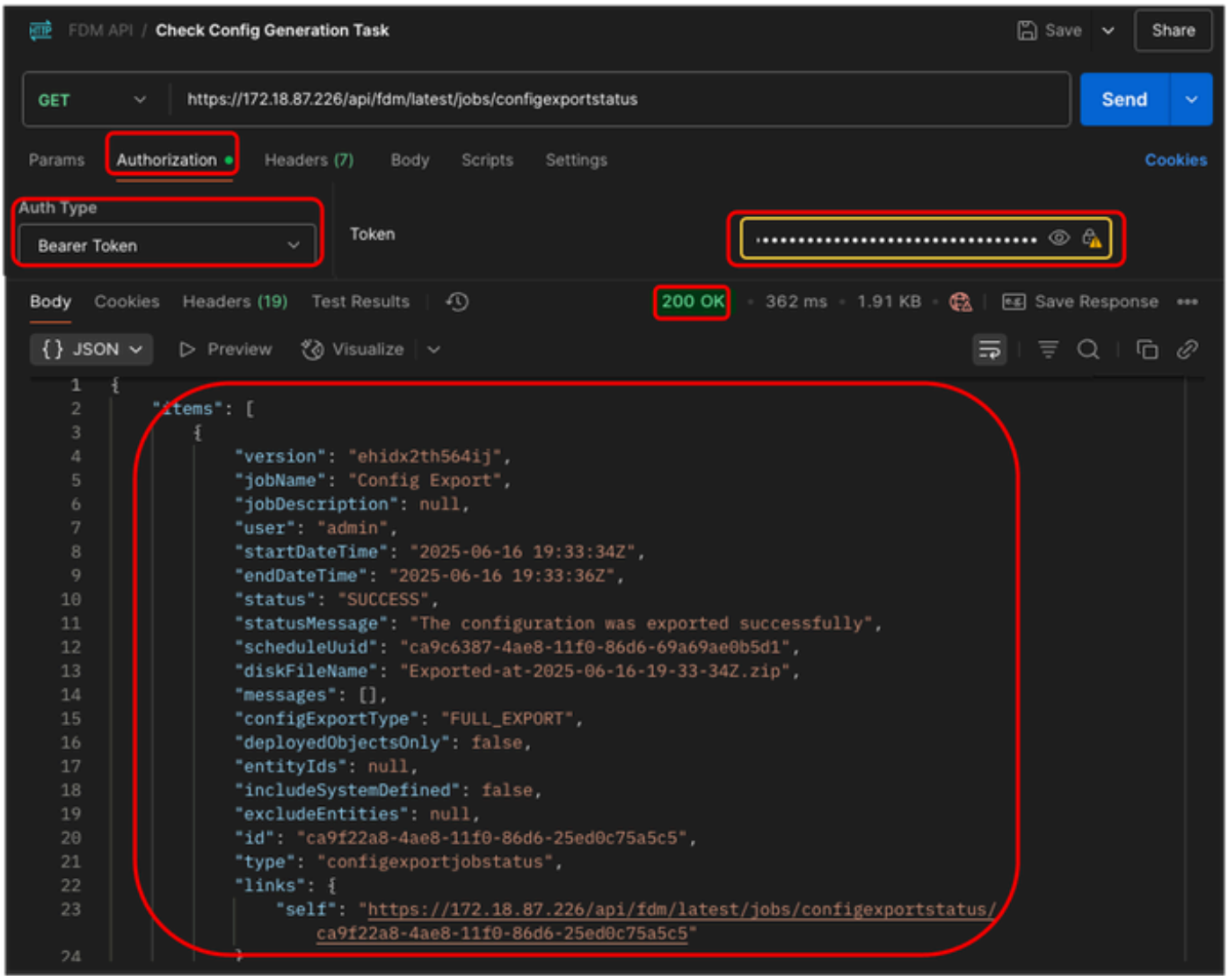
11. Wiederholen Sie Schritt 2, um eine neue Anforderung zu erstellen. Dieses Mal wird GET verwendet.

12. Wählen Sie diese neue Anforderung: Aufgabe zur Konfigurationsgenerierung überprüfen. Sie wird als GET-Anforderung erstellt. Außerdem muss die Option GET aus dem Dropdown-Menü ausgewählt werden, wenn Sie diesen Befehl ausführen. Führen Sie im Textfeld neben GET die nächste Zeile https://<FDM IP ADD>/api/fdm/latest/jobs/configureExportStatus ein.



Postman: Anfrage für Konfigurationsexport prüfen

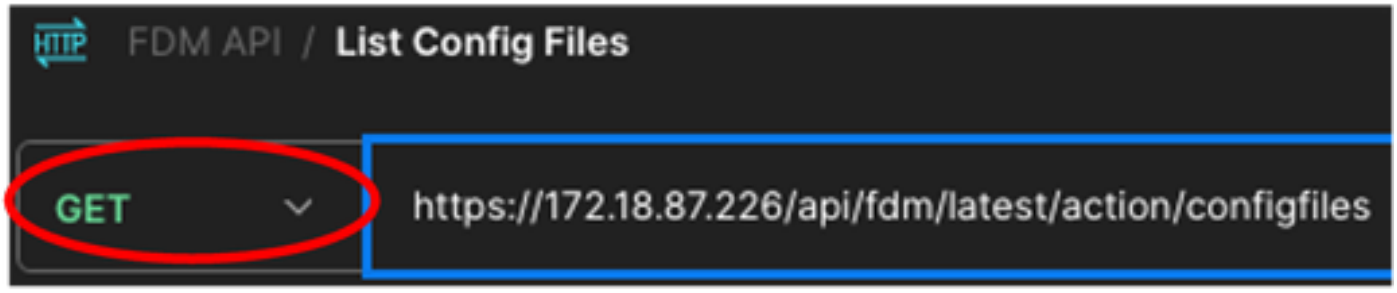
13. Wählen Sie auf der Registerkarte Autorisierung im Dropdown-Menü die Option Träger-Token als Authentifizierungstyp und im Textfeld neben Token fügen Sie das in Schritt 5 kopierte Token ein. Klicken Sie abschließend auf Senden. Wenn alles in Ordnung ist, erhalten Sie eine 200 OK Antwort und im JSON Feld können Sie den Aufgabenstatus und andere Details sehen.



Postman - Anfrage für Konfigurationsexport-Status - Autorisierung und Ausgabe

14. Wiederholen Sie Schritt 2, um eine neue Anforderung zu erstellen, GET wird dieses Mal verwendet werden.

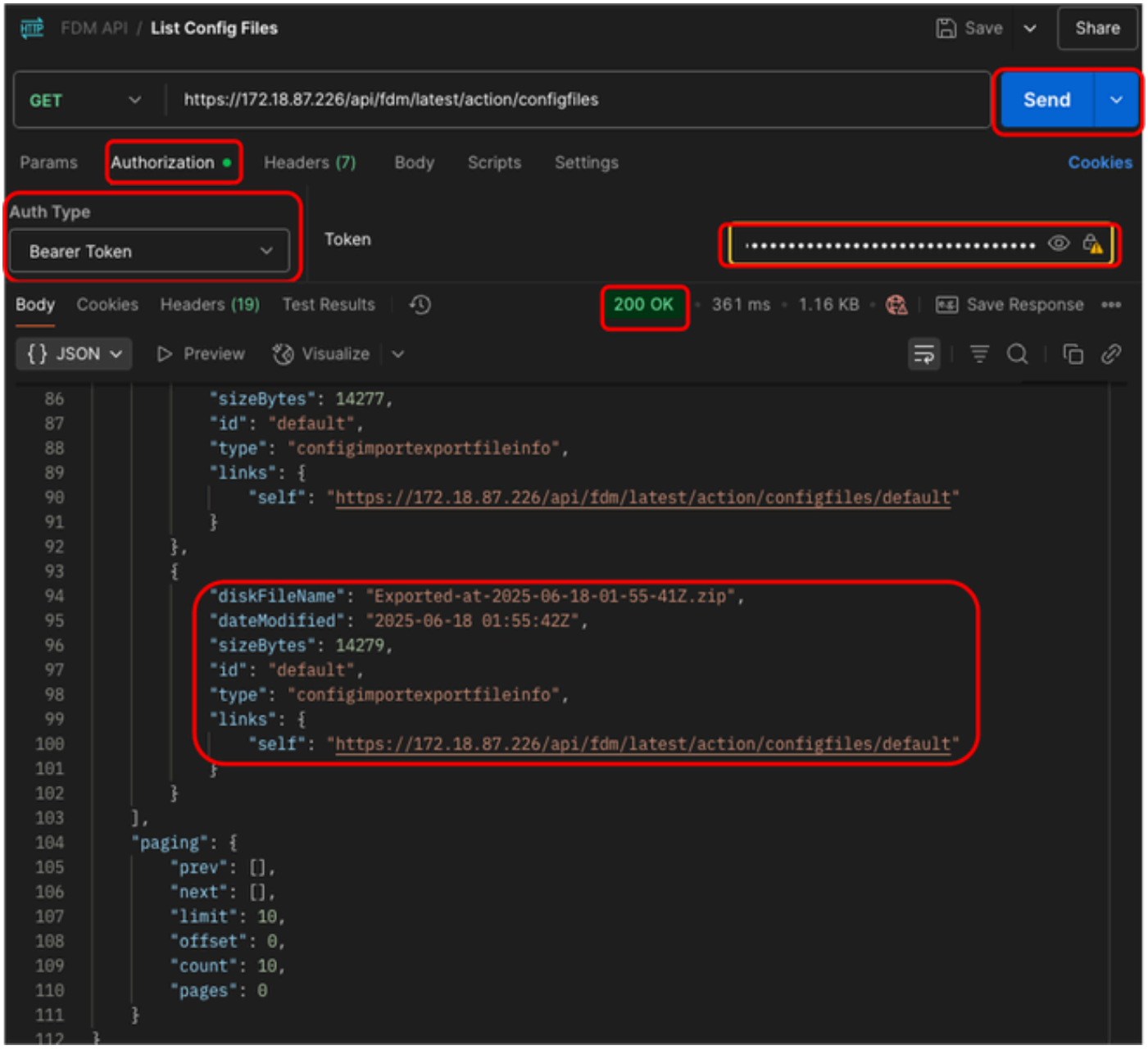
15. Neue Anforderung anrufen: Listen Sie die Konfigurationsdateien auf. Sie wird als GET-Anforderung erstellt. Auch wenn Sie diese Anforderung ausführen, muss GET aus dem Dropdown-Menü ausgewählt werden. Im Textfeld neben GET führen Sie die nächste Zeile ein: https://<FDM IP ADD>/api/fdm/latest/action/configfiles



Postman - Anfrage für exportierte Konfigurationsdateien anzeigen

16. Wählen Sie auf der Registerkarte Autorisierung im Dropdown-Menü die Option Träger-Token

als Authentifizierungstyp und im Textfeld neben Token fügen Sie das in Schritt 5 kopierte Token ein. Klicken Sie abschließend auf Senden. Wenn alles in Ordnung ist, erhalten Sie eine 200 OK-Antwort. Im JSON-Feld wird die Liste der exportierten Dateien angezeigt. Die aktuellere ist unten aufgelistet. Kopieren Sie den aktuellen Dateinamen (aktuelleres Datum im Dateinamen), da er im letzten Schritt verwendet wird.



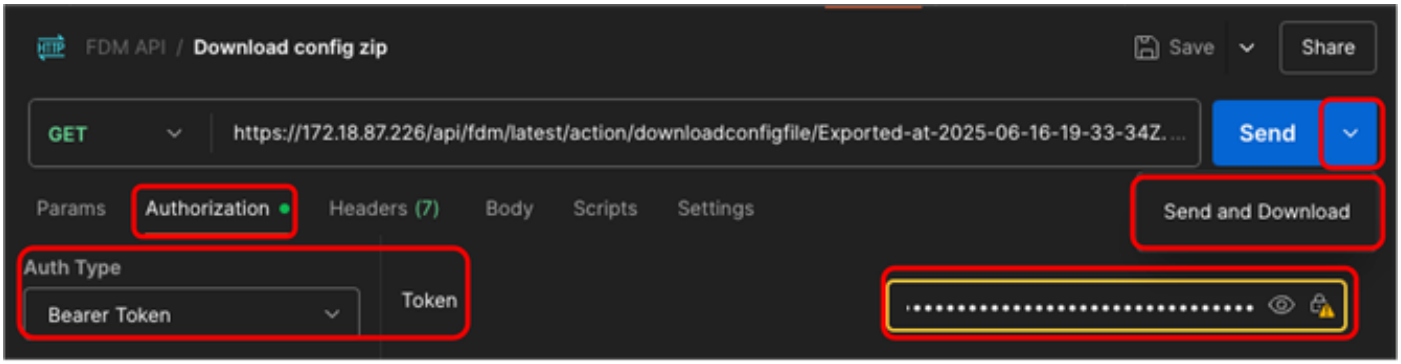
Postman - Anfrage für exportierte Konfigurationsdateien auflisten - Autorisierung und Ausgabe

17. Wiederholen Sie Schritt 2, um eine neue Anforderung zu erstellen, GET wird dieses Mal verwendet.

18. Neue Anforderung anrufen: Konfigurationszip herunterladen Sie wird als GET-Anforderung erstellt. Auch wenn Sie diese Anforderung ausführen, muss GET aus dem Dropdown-Menü ausgewählt werden. Führen Sie im Textfeld neben GET die nächste Zeile ein, und fügen Sie am Ende den Dateinamen ein, den Sie in Schritt 16 kopiert haben. https://<FDM IP ADD>/api/fdm/latest/action/downloadconfigfile/<Exported_File_name.zip >

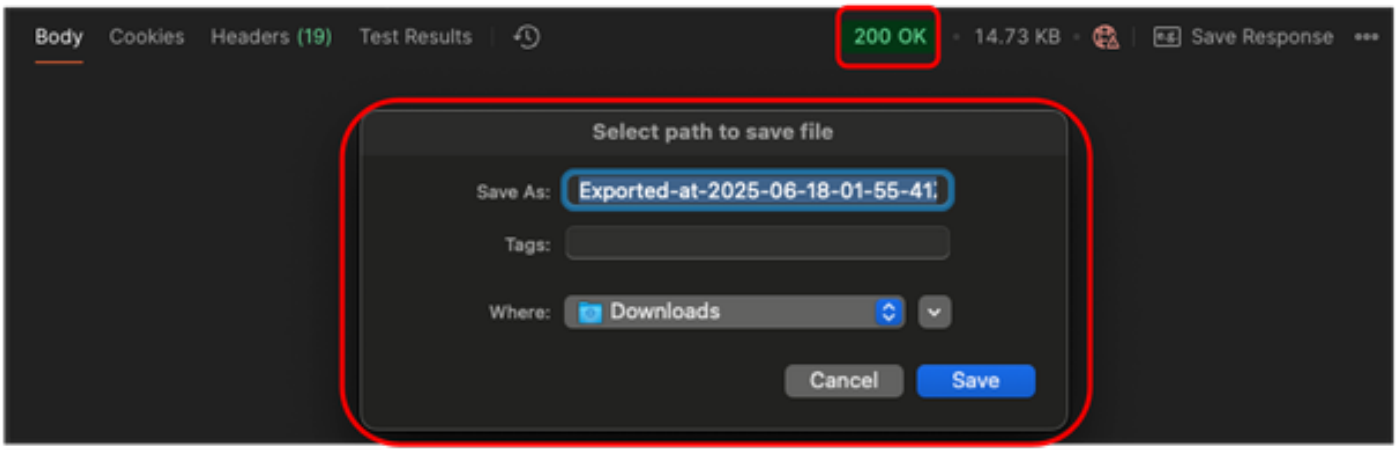
Postman - Config.zip-Dateianforderung herunterladen

19. Wählen Sie auf der Registerkarte Autorisierung im Dropdown-Menü die Option Träger-Token als Authentifizierungstyp, und fügen Sie das in Schritt 5 kopierte Token in das Textfeld neben Token ein. Klicken Sie abschließend auf den Abwärtspfeil neben Senden, und wählen Sie Senden und Herunterladen aus.



Postman - Config.zip-Dateianforderung herunterladen - Autorisierung

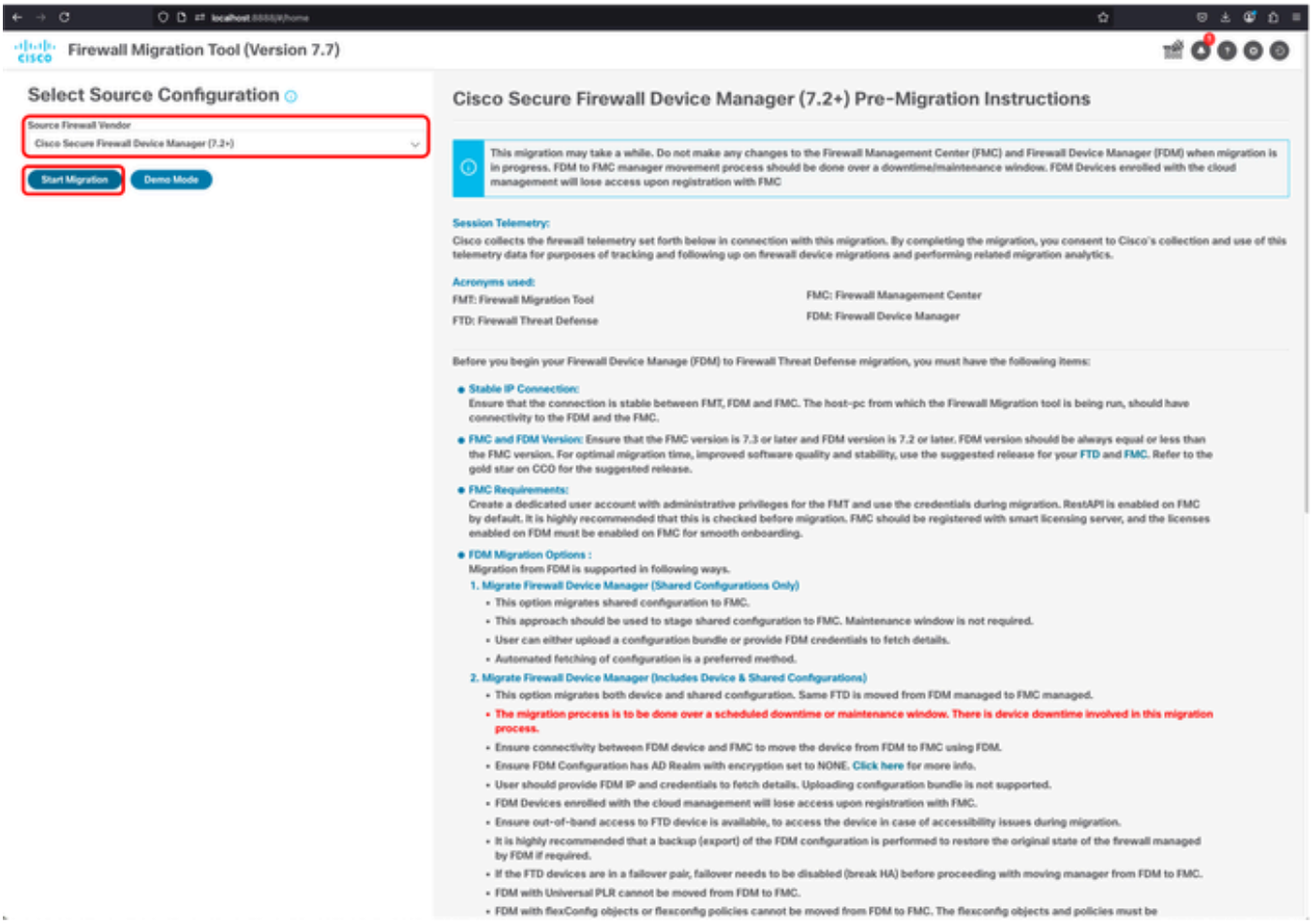
20. Wenn alles in Ordnung ist, erhalten Sie eine Antwort von 200 OK und ein Popup-Fenster wird angezeigt, in dem Sie nach dem Zielordner gefragt werden, in dem die Datei configuration.zip gespeichert werden soll. Diese ZIP-Datei kann jetzt in das Firewall Migration Tool hochgeladen werden.



Postman - Config.zip-Dateianforderung herunterladen - Speichern

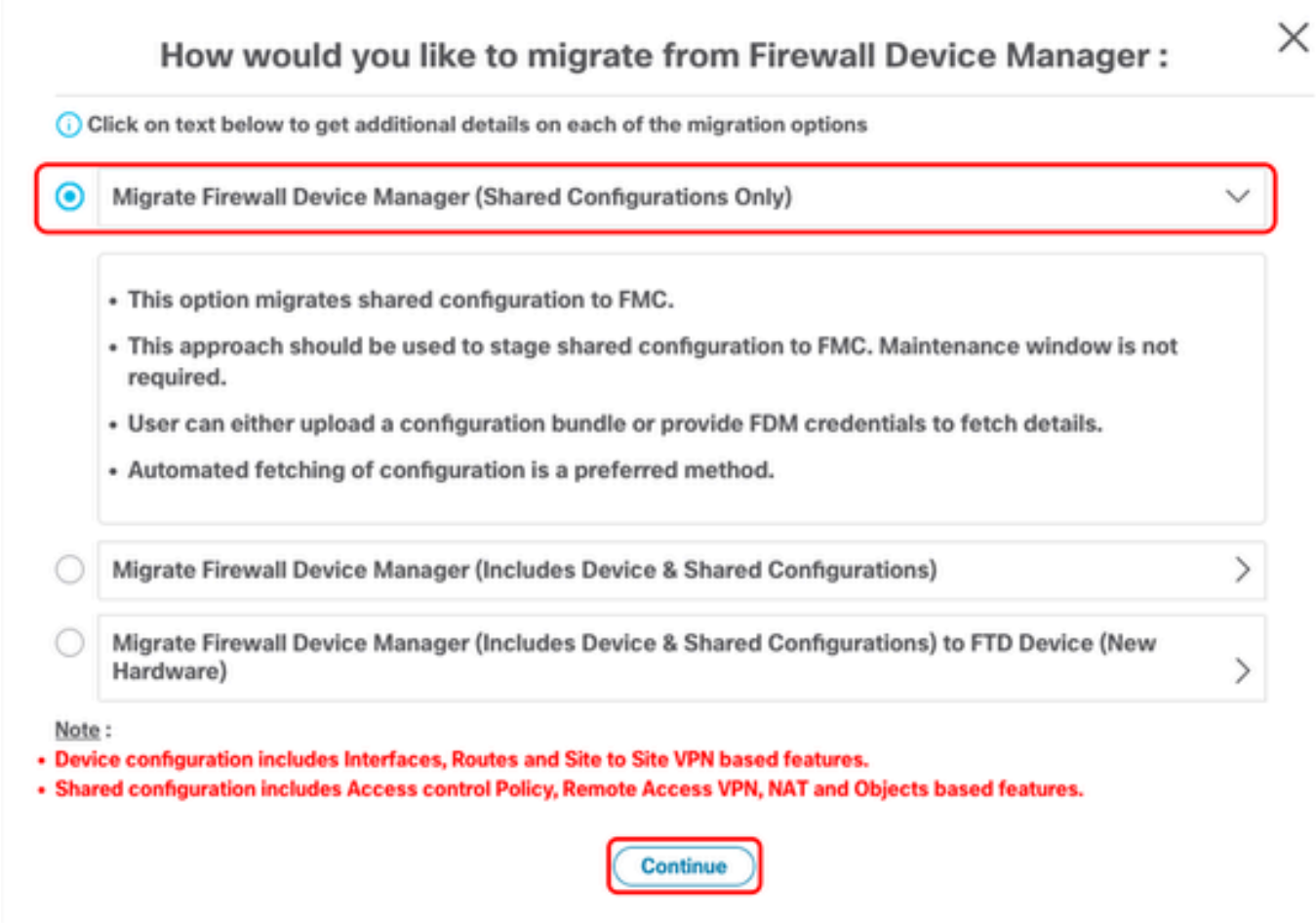
Firewall Migration-Tool

21. Öffnen Sie das Firewall Migration Tool, wählen Sie im Dropdown-Menü Select Source Configuration die Option Cisco Secure Firewall Device Manager (7.2+) aus, und klicken Sie auf Migration starten.



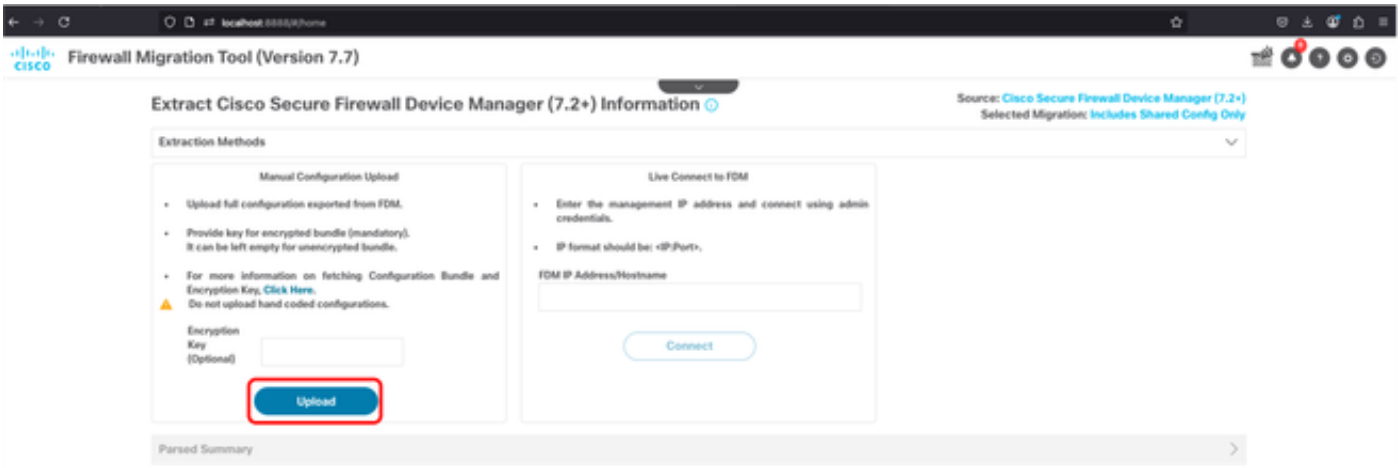
FMT - FDM-Auswahl

22. Aktivieren Sie das erste Optionsfeld, Firewall-Gerätemanager migrieren (nur freigegebene Konfigurationen) und klicken Sie auf Weiter.



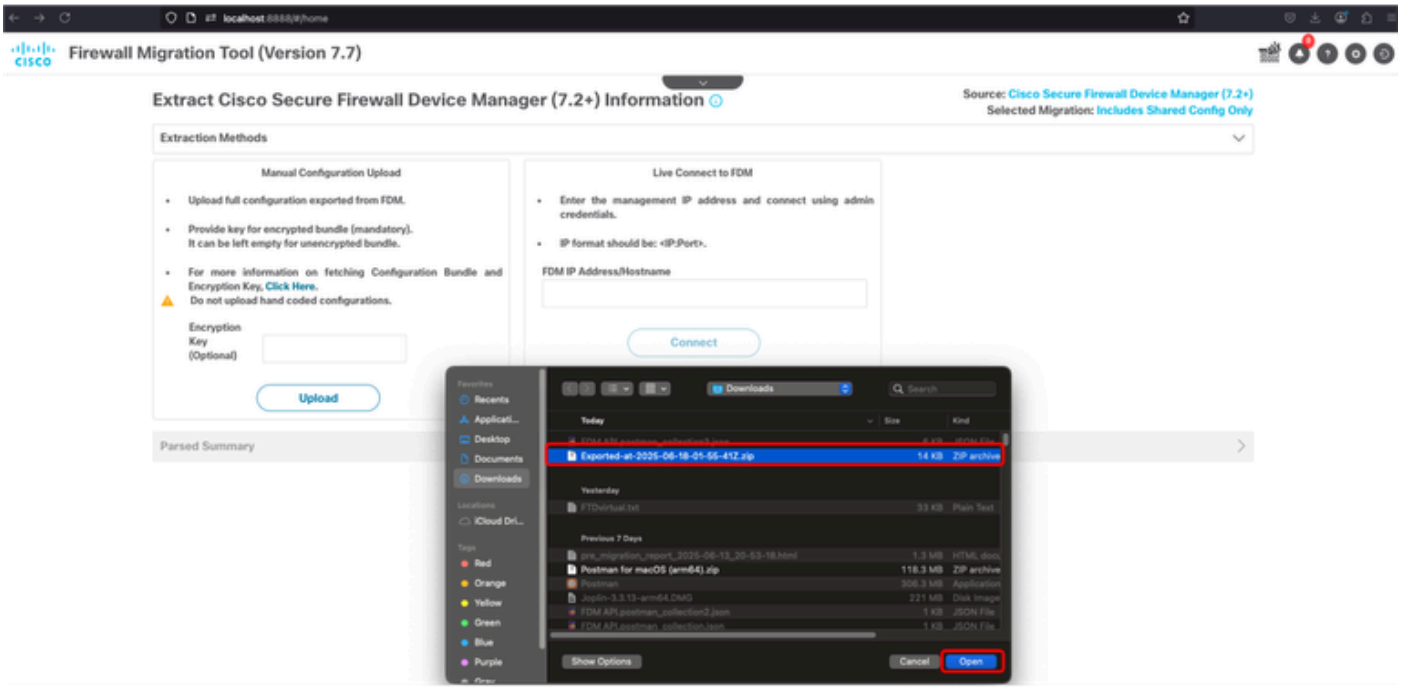
FMT = FDM Migration Shared Configurations Only

23. Klicken Sie im linken Bereich (Manuelles Hochladen der Konfiguration) auf Hochladen.



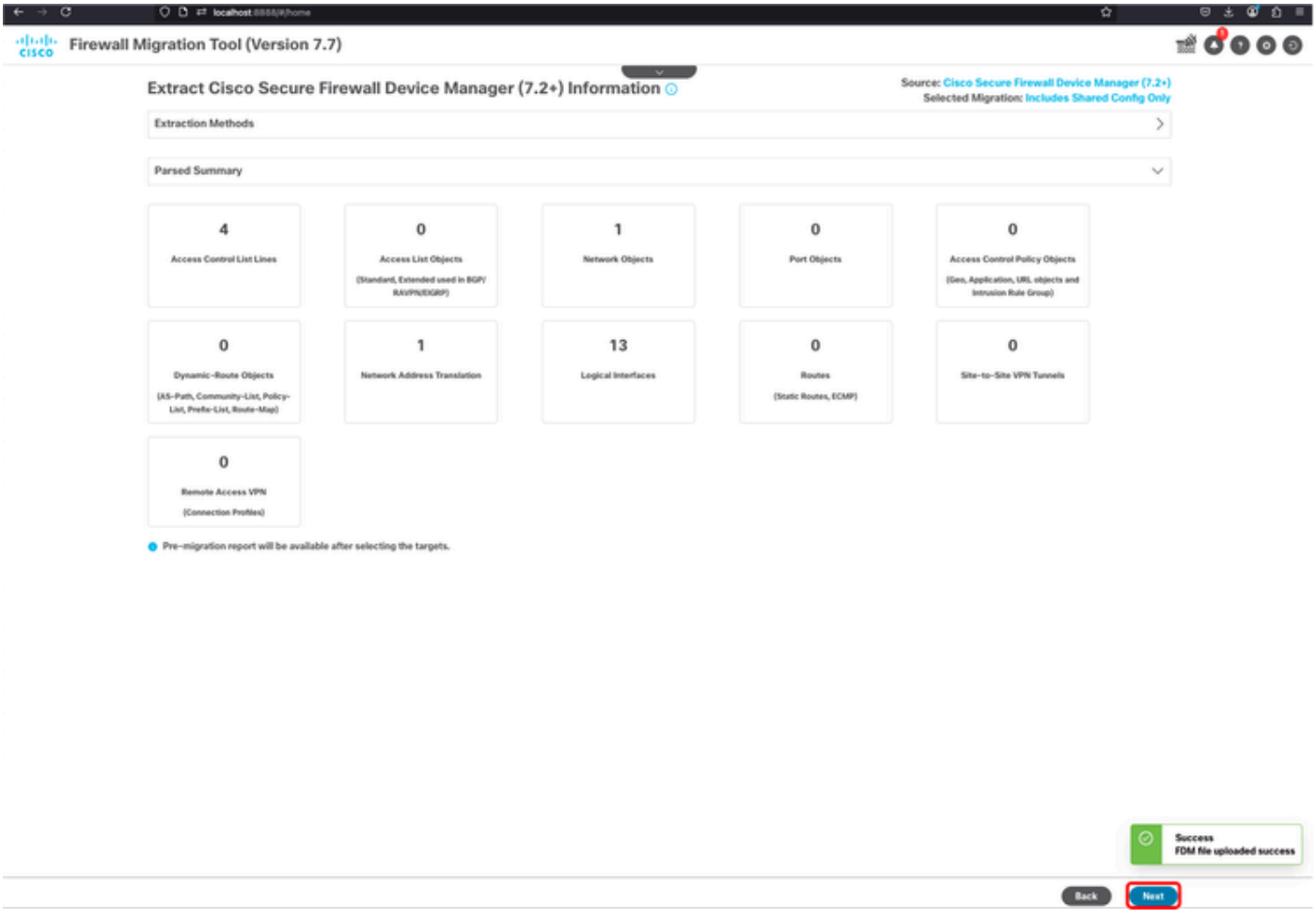
FMT - Config.zip-Datei hochladen

24. Wählen Sie die exportierte ZIP-Konfigurationsdatei im zuvor gespeicherten Ordner, und klicken Sie auf Öffnen.



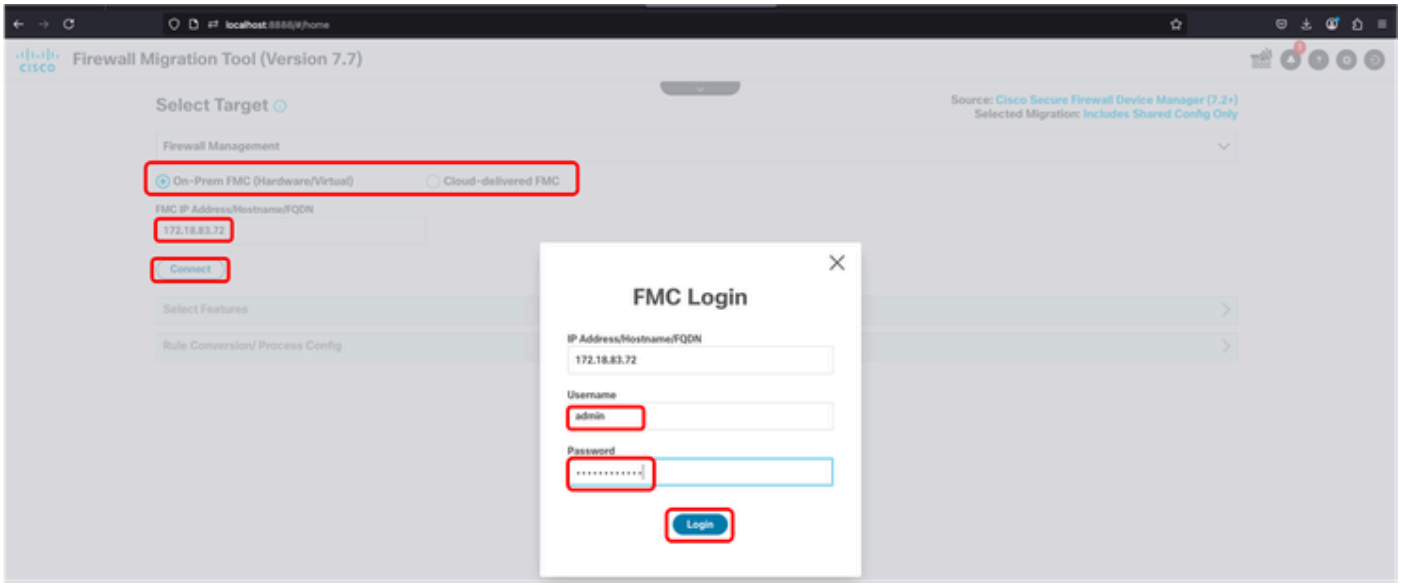
FMT - Config.zip-Dateiauswahl

25. Wenn alles wie erwartet verläuft, wird die analysierte Zusammenfassung angezeigt. In der rechten unteren Ecke wird ein Popup-Fenster mit der Meldung angezeigt, dass die FDM-Datei erfolgreich hochgeladen wurde. Klicken Sie auf Next (Weiter).



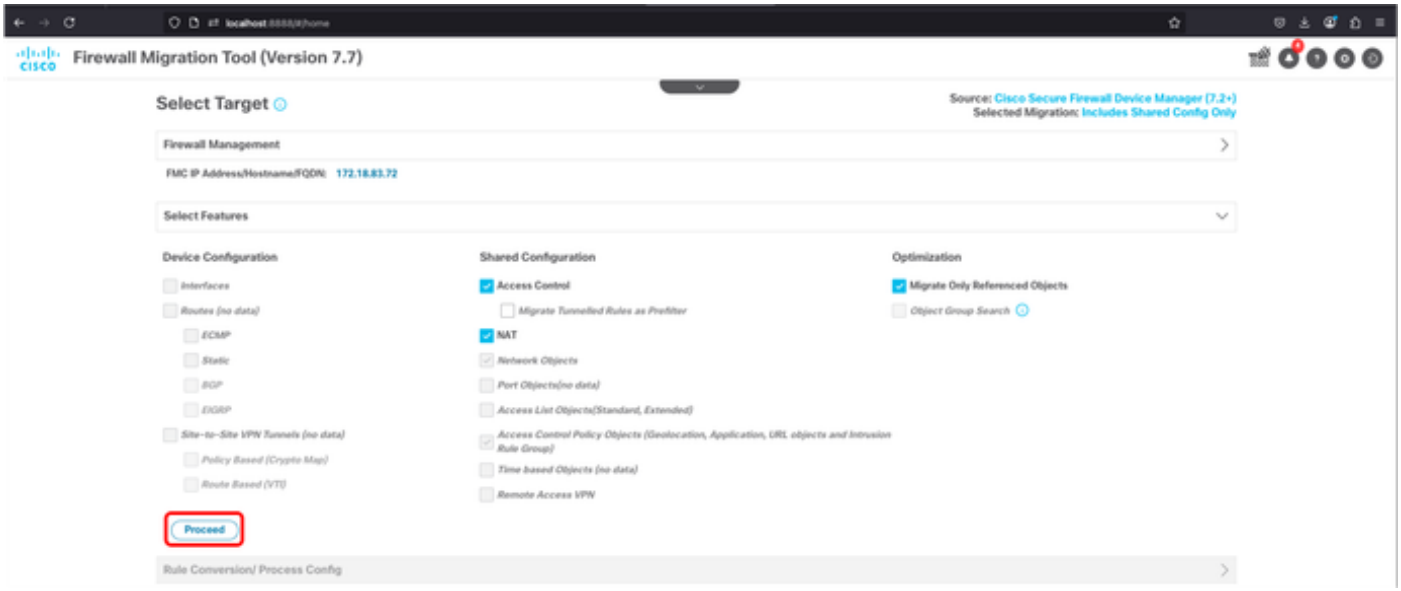
FMT - Zusammenfassung der Analyse

26. Aktivieren Sie die Option, die Ihrer Umgebung besser entspricht (Vor-Ort-FMC oder Cd-FMC). In diesem Szenario wird ein standortbasiertes FMC verwendet. Geben Sie die IP-Adresse des FMC ein, und klicken Sie auf Verbinden. Ein neues Popup-Fenster fordert FMC-Anmeldeinformationen an. Klicken Sie nach Eingabe dieser Informationen auf Anmelden.



FMT - FMC Zielanmeldung

27. Der nächste Bildschirm zeigt das Ziel-FMC und die Funktionen, die migriert werden sollen. Klicken Sie auf Fortfahren.

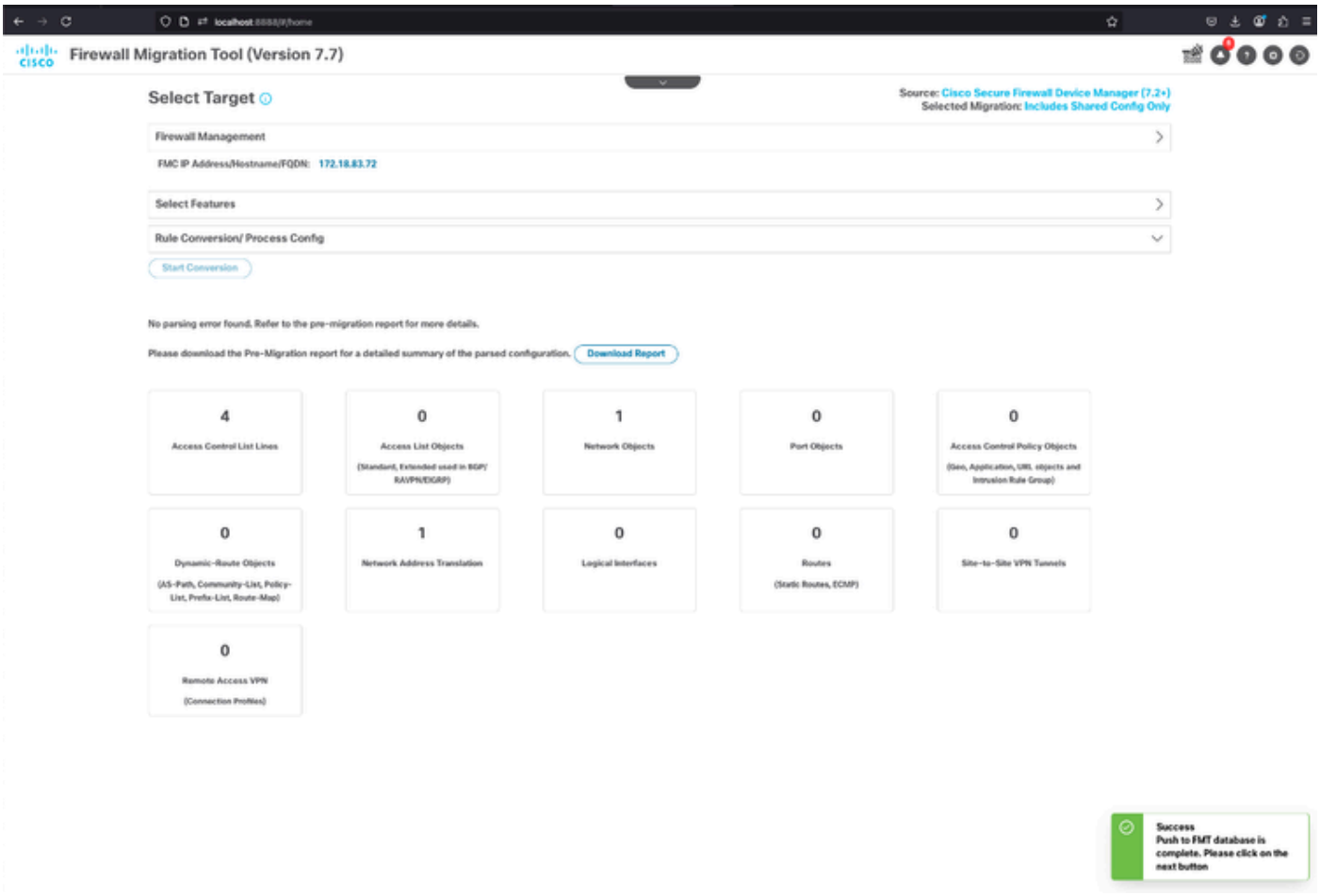


FMT - FMC-Ziel - Funktionsauswahl

28. Sobald FMC Target bestätigt ist, klicken Sie auf Start Conversion button.

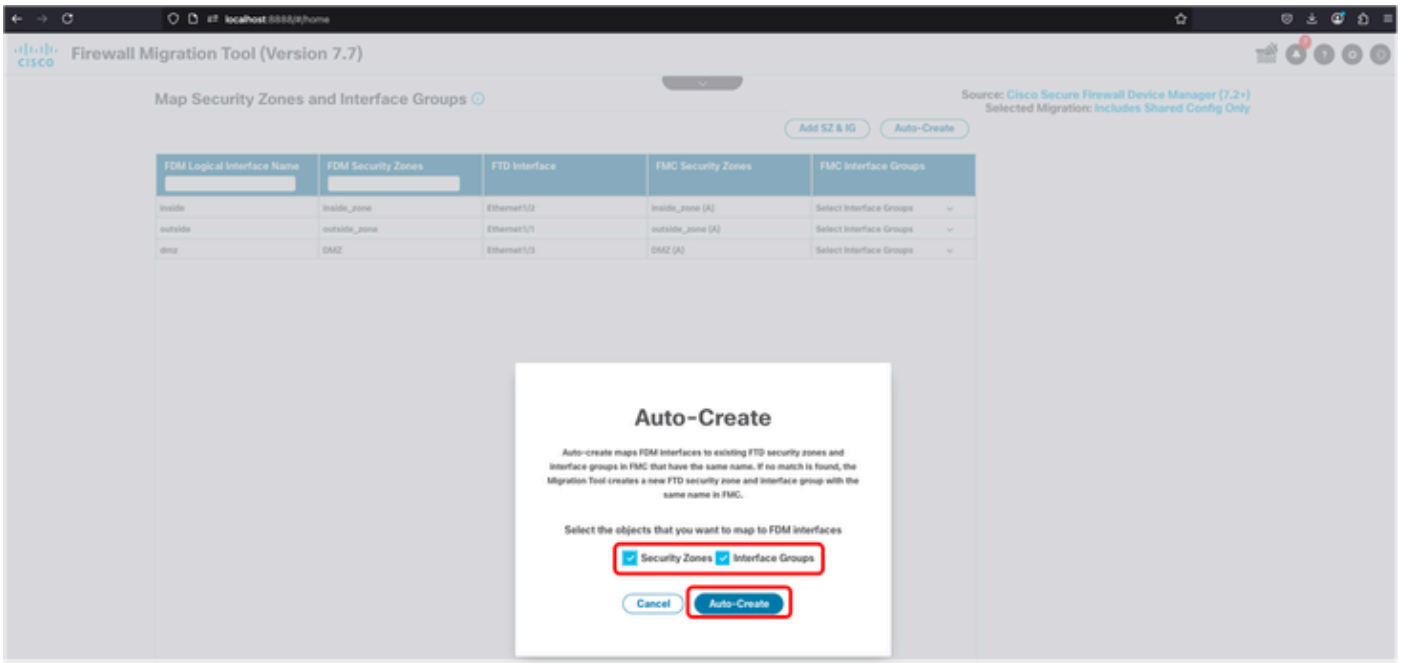
FMT - Konfig.-Konfiguration starten

29. Wenn alles wie erwartet läuft, wird ein Pop-Up in der rechten unteren Ecke angezeigt, das informiert, dass Push zur FMT-Datenbank abgeschlossen ist. Klicken Sie auf Next (Weiter).



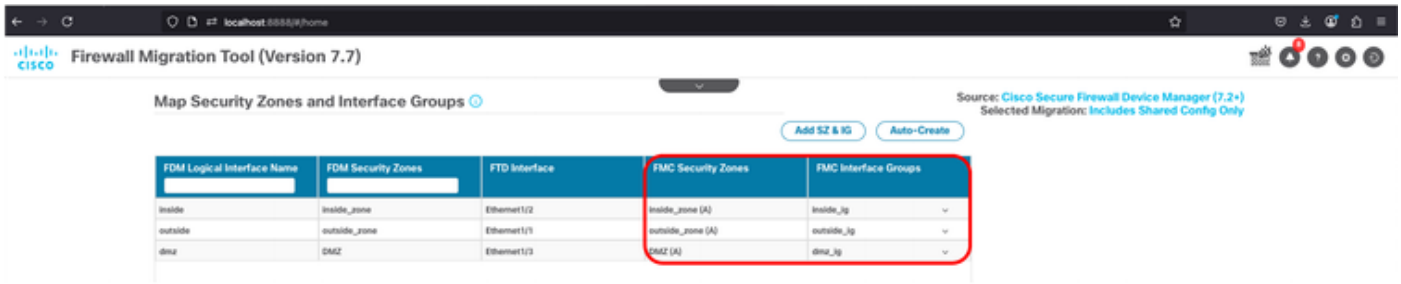
FMT - Datenbank-Push erfolgreich abgeschlossen

30. Auf dem nächsten Bildschirm müssen Sie die Sicherheitszonen und Schnittstellengruppen manuell erstellen oder die Option zum automatischen Erstellen auswählen. In diesem Szenario wird auto-create verwendet.



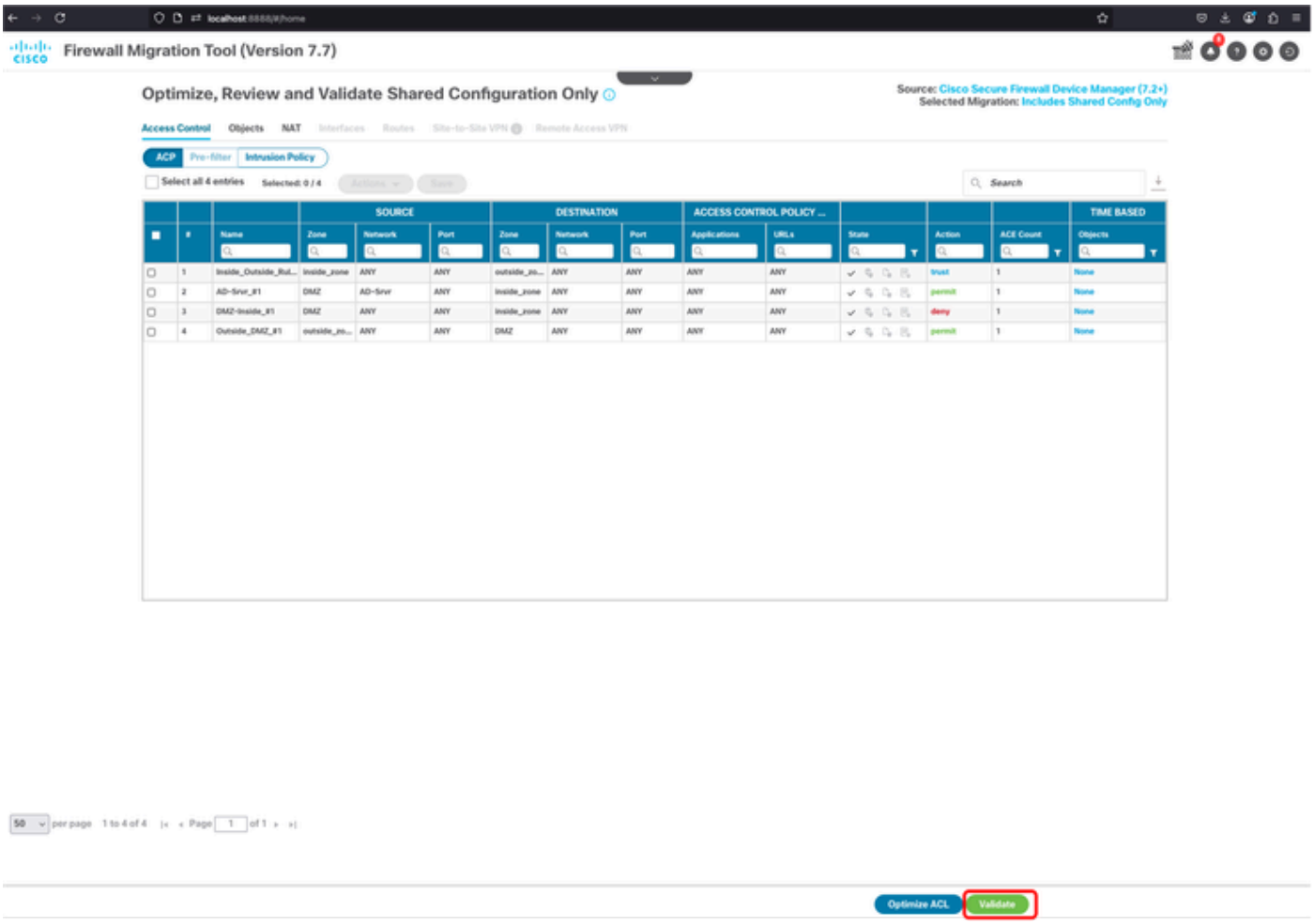
FMT - Auto Creating Security Zones and Interface Groups (Automatisches Erstellen von Sicherheitszonen und Schnittstellengruppen)

31. Nach Abschluss dieser Schritte werden in der 4. und 5. Spalte die Sicherheitszone bzw. die Schnittstellengruppe angezeigt.



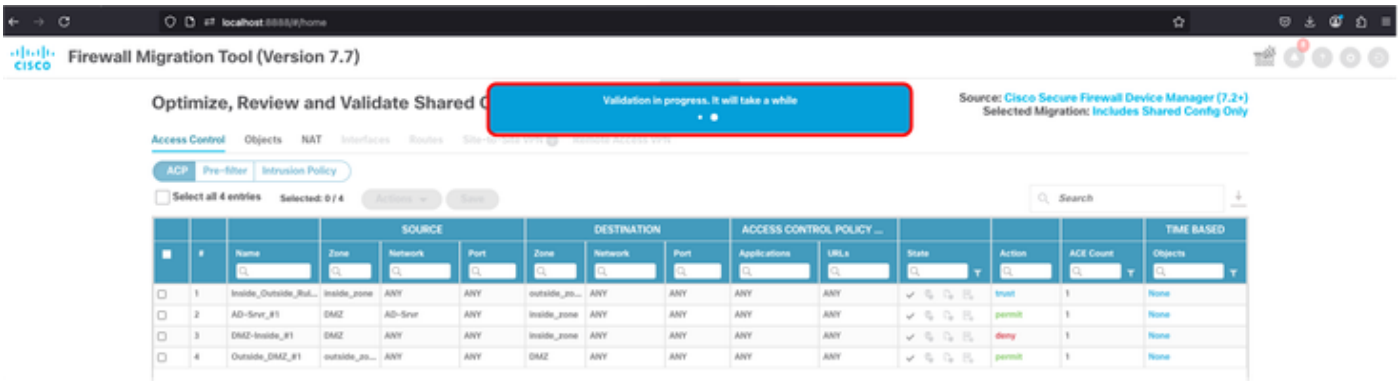
FMT - Sicherheitszonen und Schnittstellengruppen erfolgreich erstellt

32. Im nächsten Bildschirm können Sie die Zugriffskontrollliste optimieren oder nur ACP, Objects und NAT validieren. Klicken Sie abschließend auf die Schaltfläche Validieren.



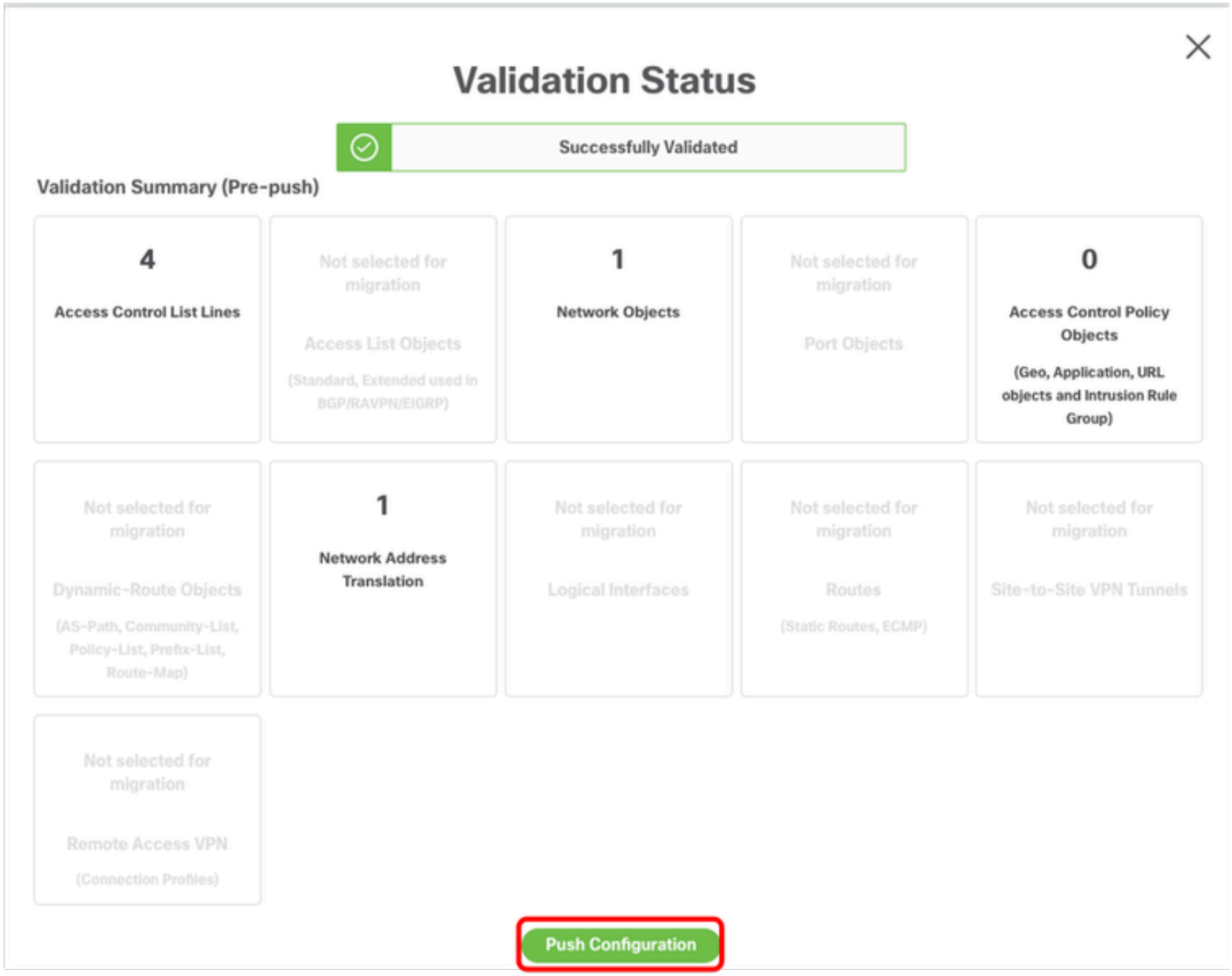
FMT = Optimization ACL = Validate Migration

33. Validierung dauert einige Minuten abgeschlossen werden.



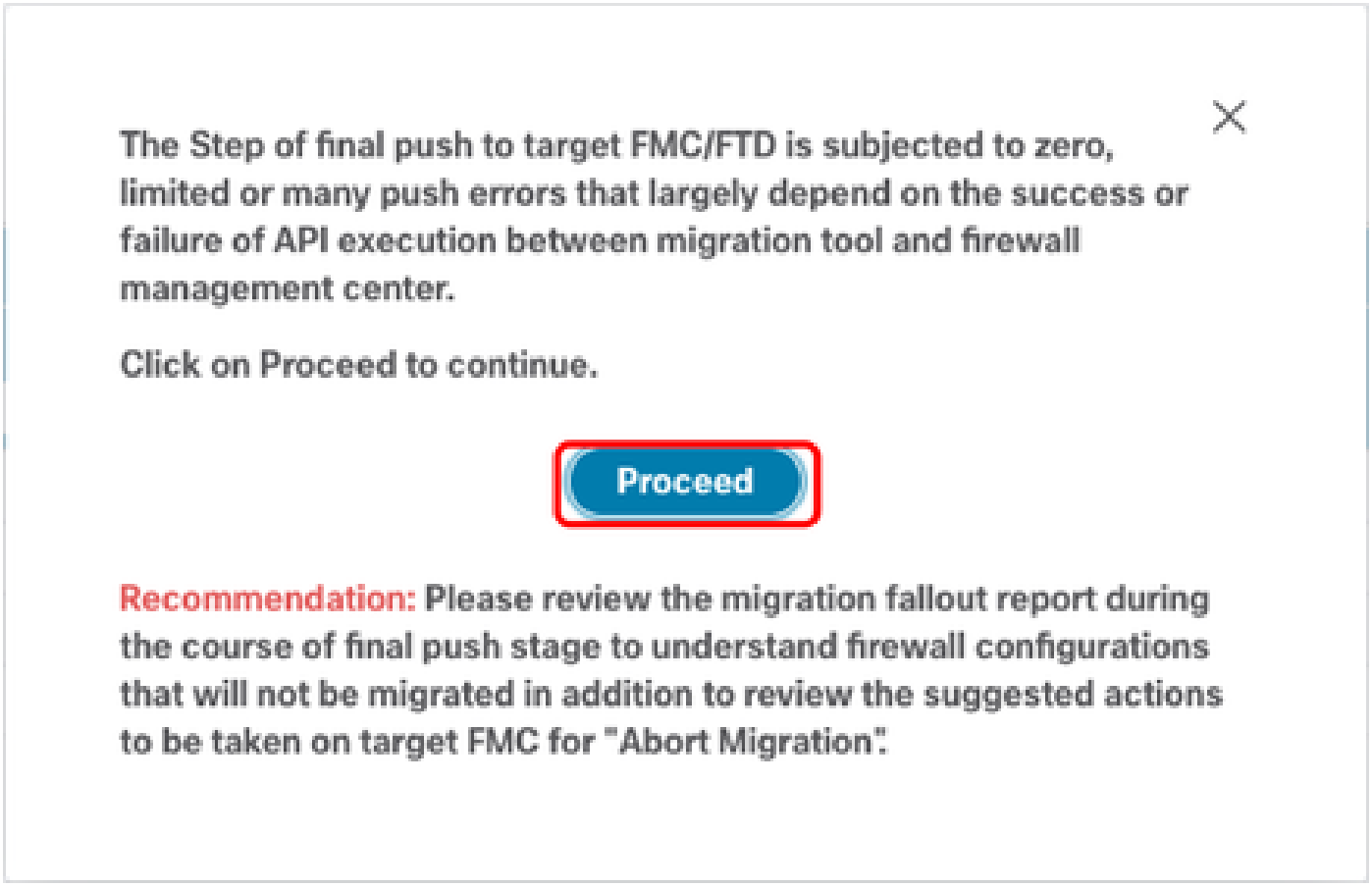
FMT - Validierung in Bearbeitung

34. Nach Abschluss des Vorgangs informiert FMT Sie, dass die Konfiguration erfolgreich validiert wurde, und als Nächstes klicken Sie auf die Schaltfläche "Push Configuration".



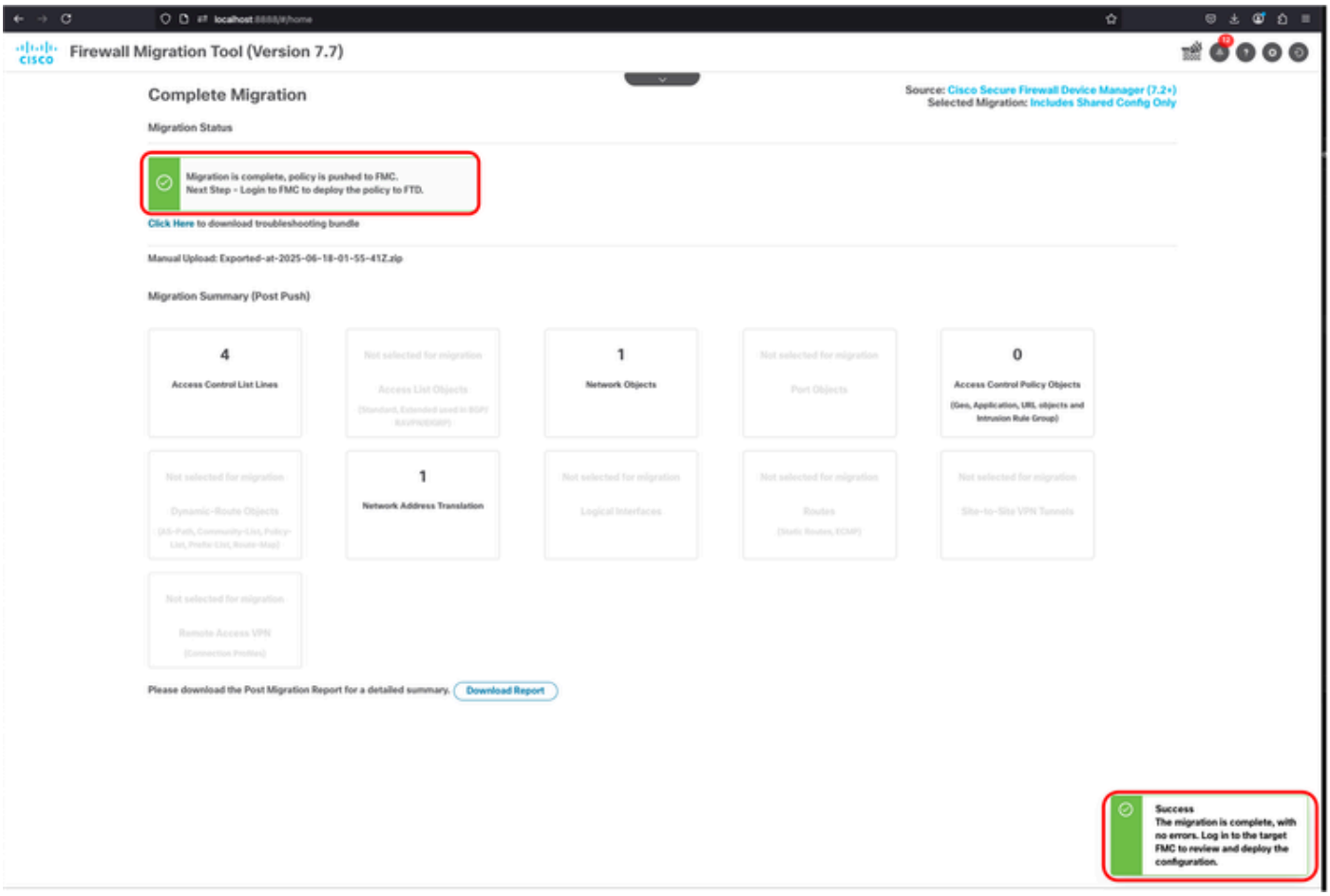
FMT - Validierung erfolgreich - Push-Konfiguration an FMC

35. Schließlich, klicken Sie auf Fortfahren Schaltfläche.



FMT - Mit Config Push fortfahren

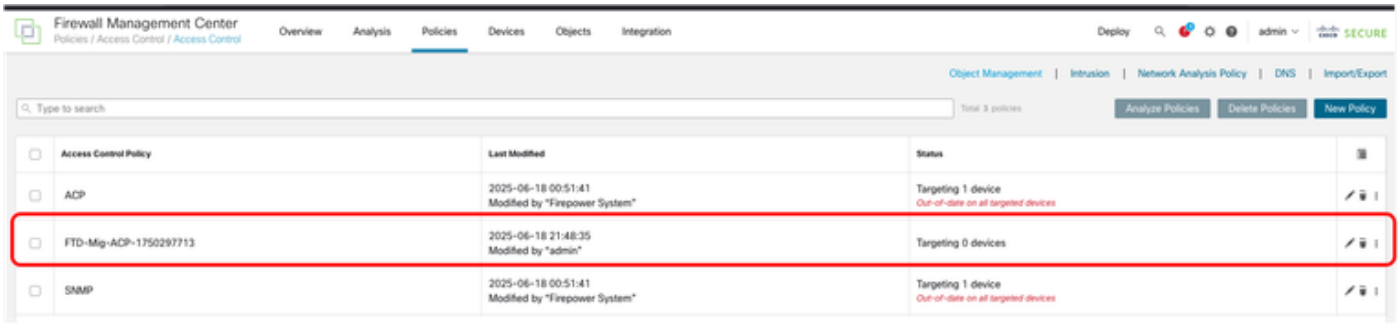
36. Wenn alles wie erwartet verläuft, wird die Meldung Migration erfolgreich angezeigt. FMT fordert Sie auf, sich bei FMC anzumelden und die migrierte Richtlinie in FTD bereitzustellen.



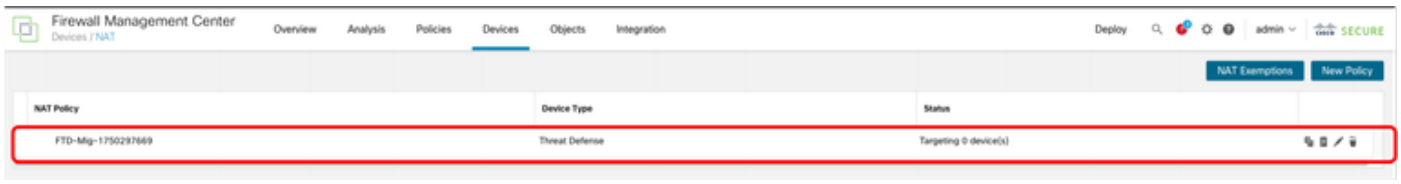
FMT - Benachrichtigung über erfolgreiche Migration

FMC-Verifizierung

37. Nach der Anmeldung bei FMC werden die ACP- und NAT-Richtlinien als FTD-Mig angezeigt. Jetzt können Sie mit der Bereitstellung für die neue FTD fortfahren.



FMC - ACP Migriert



FMC - NAT-Richtlinienmigration

Zugehörige Informationen

- FMT - FDM Migration Guide to FMC
- FMT-Versionshinweise

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.