Integrierte NFVIS WAN-Edge-Geräte

Inhalt

Einleitung

In diesem Dokument wird der Prozess der Integration NFVIS-fähiger Systeme in eine Catalyst™ SD-WAN-Umgebung für Verwaltung und Betrieb beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco SDWAN
- NFVIS
- Plug-and-Play (PNP)

Es wird angenommen, dass

- SD-WAN-Controller (vManage, vBond und vSmart) werden bereits mit gültigen Zertifikaten bereitgestellt.
- Der Cisco WAN-Edge (in diesem Fall NFVIS) ist mit dem vBond-Orchestrator und anderen SD-WAN-Controllern erreichbar, die über öffentliche IP-Adressen im gesamten WAN-Transportnetz erreichbar sind.

- Die NFVIS-Version muss mit dem Kompatibilitätsleitfaden für Steuerungskomponenten übereinstimmen.

Verwendete Komponenten

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.

Hardware

- C8300-UCPE-1N20 (kann jedoch auf jede NFVIS-fähige Plattform angewendet werden)

Software

- vManage 20.14.1
- vSmart und vBond 20.14.1
- NFVIS 4.14.1

PnP-Workflow

Das Vertrauen in die WAN-Edge-Geräte wird mithilfe der Root-Chain-Zertifikate hergestellt, die in der Fertigung vorinstalliert, manuell geladen, automatisch von vManage verteilt oder während des automatisierten Bereitstellungsprozesses für PnP oder ZTP installiert werden.

Die SD-WAN-Lösung verwendet ein Zulassungslistenmodell, d. h. die WAN-Edge-Geräte, die dem SDWAN-Overlay-Netzwerk beitreten dürfen, müssen zuvor von allen SD-WAN-Controllern bekannt sein. Hierzu fügen Sie die WAN-Edge-Geräte im Plug-and-Play-Verbindungsportal (PnP) unter https://software.cisco.com/software/pnp/devices hinzu.

Bei diesem Verfahren muss das Gerät immer im gleichen Overlay-Netzwerk identifiziert, vertrauenswürdig und als zugelassenes Gerät aufgeführt werden. Die gegenseitige Authentifizierung muss für alle SD-WAN-Komponenten erfolgen, bevor sichere Steuerverbindungen zwischen SD-WAN-Komponenten im gleichen Overlay-Netzwerk hergestellt werden können. Die Identität des WAN-Edge-Geräts wird eindeutig anhand der Chassis-ID und der Seriennummer des Zertifikats identifiziert. Je nach WAN-Edge-Router werden die Zertifikate auf unterschiedliche Weise bereitgestellt:

- Hardwarebasierter vEdge: Das Zertifikat wird auf dem integrierten TPM-Chip (Tamper Proof Module) gespeichert, der bei der Herstellung installiert wurde.
- Hardwarebasiertes Cisco IOS®-XE SD-WAN: Das Zertifikat wird in dem integrierten SUDI-Chip gespeichert, der bei der Herstellung installiert wurde.
- Virtuelle Plattform für Cisco IOS-XE SD-WAN-Geräte: verfügen nicht über vorinstallierte Root-Zertifikate (z. B. die ASR1002-X-Plattform). Für diese Geräte stellt vManage ein einmaliges Kennwort (One-Time Password, OTP) bereit, um das Gerät mithilfe der SD-

WAN-Controller zu authentifizieren.

Für die Zero-Touch-Bereitstellung (ZTP) muss ein DHCP-Server zur Verfügung stehen. Ist dies nicht der Fall, kann eine IP-Adresse manuell zugewiesen werden, um mit den verbleibenden Schritten des Plug & Play (PnP)-Prozesses fortzufahren.

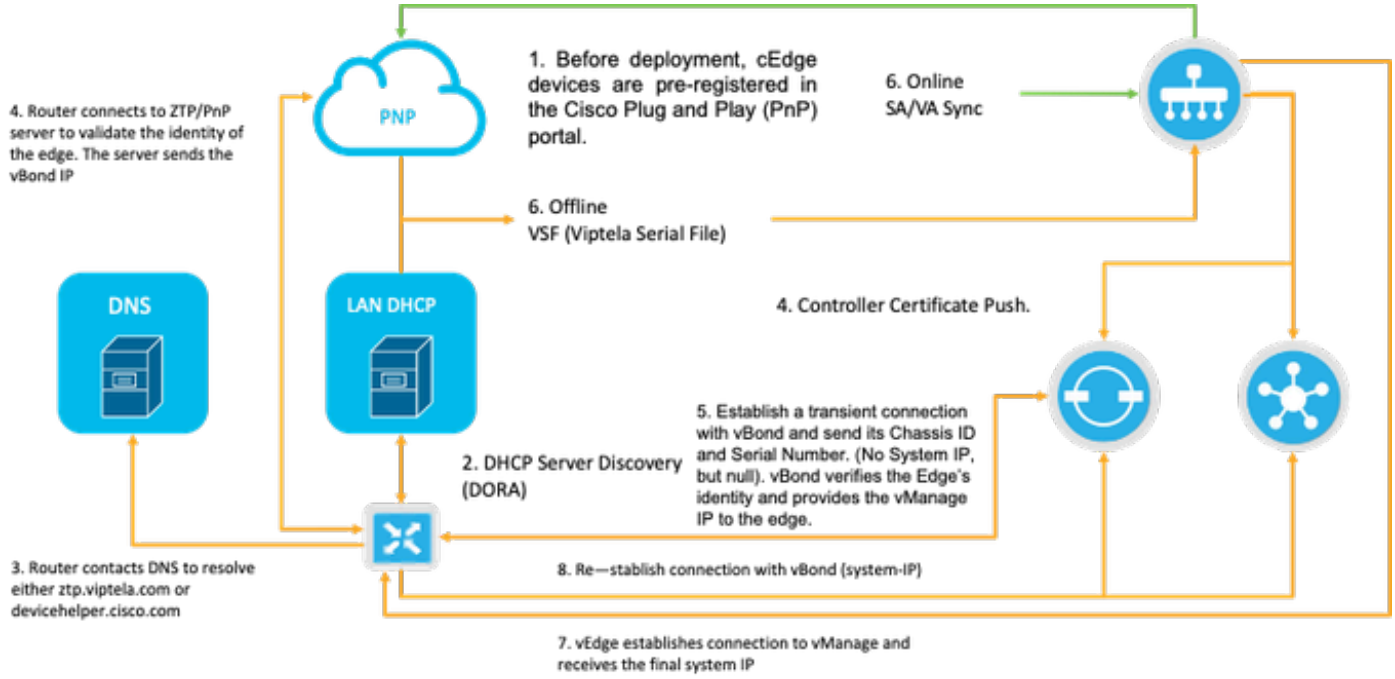


Abb. 1: Diagramm des Vertrauens-Workflows für PnP- und WAN-Edge-Geräte.

Sicheres Onboarding des NFVIS-fähigen Geräts

Abruf von SN und Seriennummer des Zertifikats

Der hardwarebasierte SUDI-Chip (Secure Unique Device Identifier) von NFVIS-fähiger Hardware stellt sicher, dass nur autorisierte Geräte einen sicheren TLS- oder DTLS-Kontrollebenen-Tunnel zum SD-WAN Manager-Orchestrator aufbauen können. Erfassen Sie die entsprechende Seriennummer mit dem Befehl support show chassis executive level:

```
C8300-UCPE-NFVIS# support show chassis
Product Name              : C8300-UCPE-1N20
Chassis Serial Num        : XXXXXXXXX
Certificate Serial Num    : XXXXXXXXXXXXXXXX
```

Hinzufügen des Geräts zum PnP-Portal

Navigieren Sie zu https://software.cisco.com/software/pnp/devices, und wählen Sie den richtigen Smart Account und Virtual Account für Ihre Benutzer- oder Übungsumgebung aus. (Wenn mehrere Smart Accounts im Namen übereinstimmen, können Sie sie mit dem Domain Identifier

unterscheiden).

Wenn Sie oder Ihr Benutzer nicht wissen, mit welchem Smart Account (SA) / Virtual Account (VA) Sie arbeiten sollen, können Sie jederzeit im Textlink "Gerätesuche" nach der vorhandenen/integrierten Seriennummer suchen, um festzustellen, zu welcher SA/VA sie gehört.

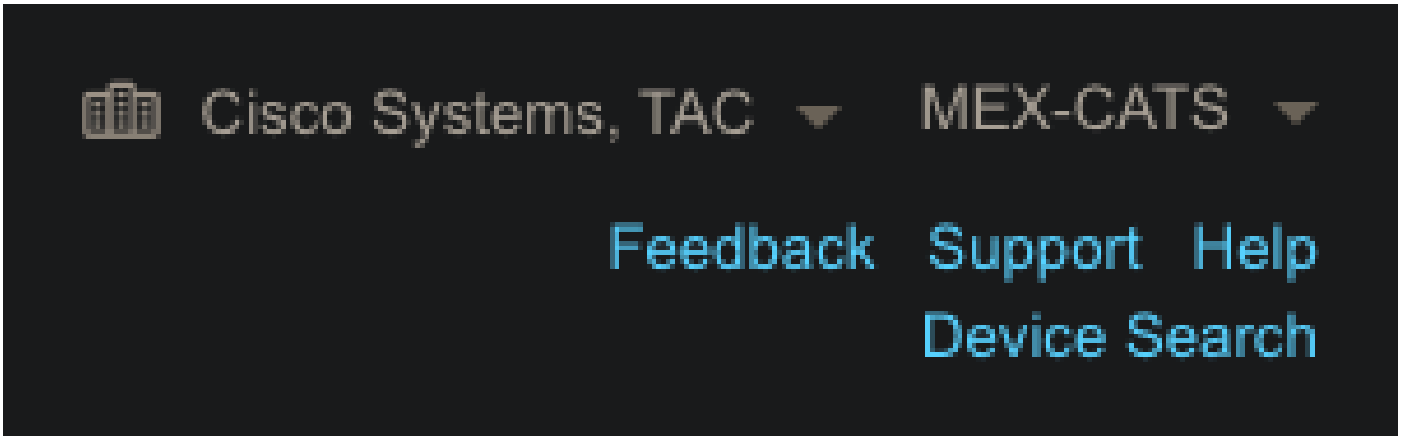


Abb. 2. Schaltfläche SA/VA-Auswahl und Gerätesuche.

Klicken Sie nach Auswahl der richtigen SA/VA auf "Geräte hinzufügen...":

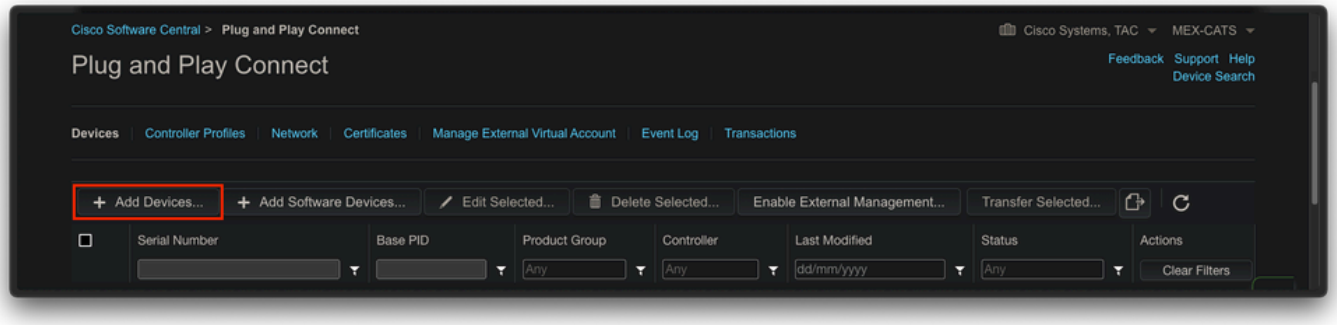


Abb. 3. "Geräte hinzufügen..." Schaltfläche zum Klicken für die Registrierung physischer Geräte

Für diesen speziellen Fall sollte nur ein Gerät integriert sein, sodass eine manuelle Eingabe ausreicht:

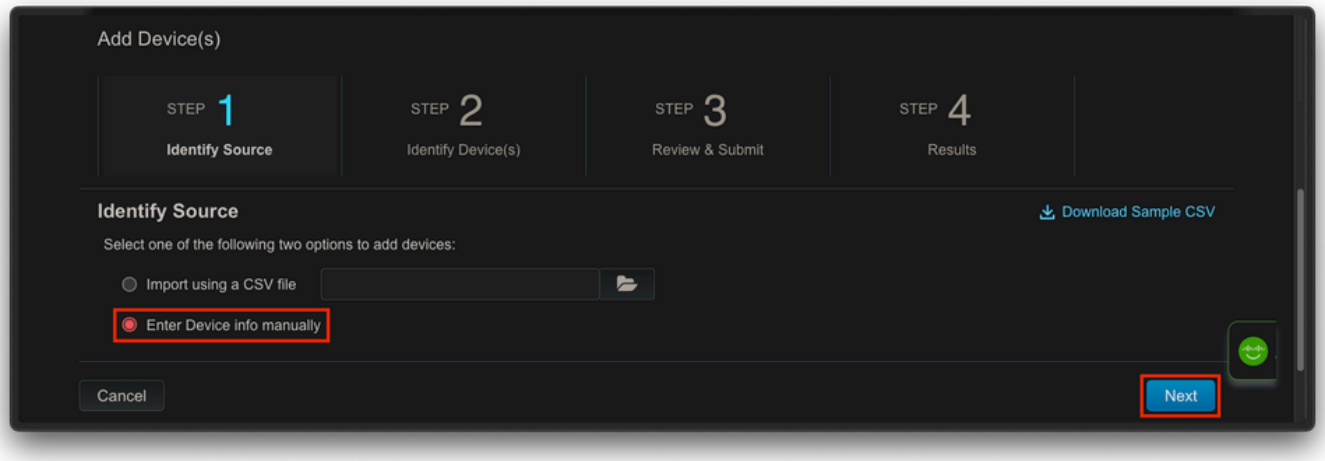


Abb. 4. Alternative "Geräte hinzufügen..." für Geräteinformationseingabe, manuell (individuell) oder CSV (mehrfach).

Klicken Sie in Schritt 2 auf die Schaltfläche "+ Identify Device..." (+ Identifizieren des Geräts..). Ein Form-Modus wird angezeigt. Geben Sie die Details mit den Informationen ein, die auf der Support-Ausgabe von NFVIS angezeigt werden, und wählen Sie das entsprechende vBond-Controller-Profil aus.

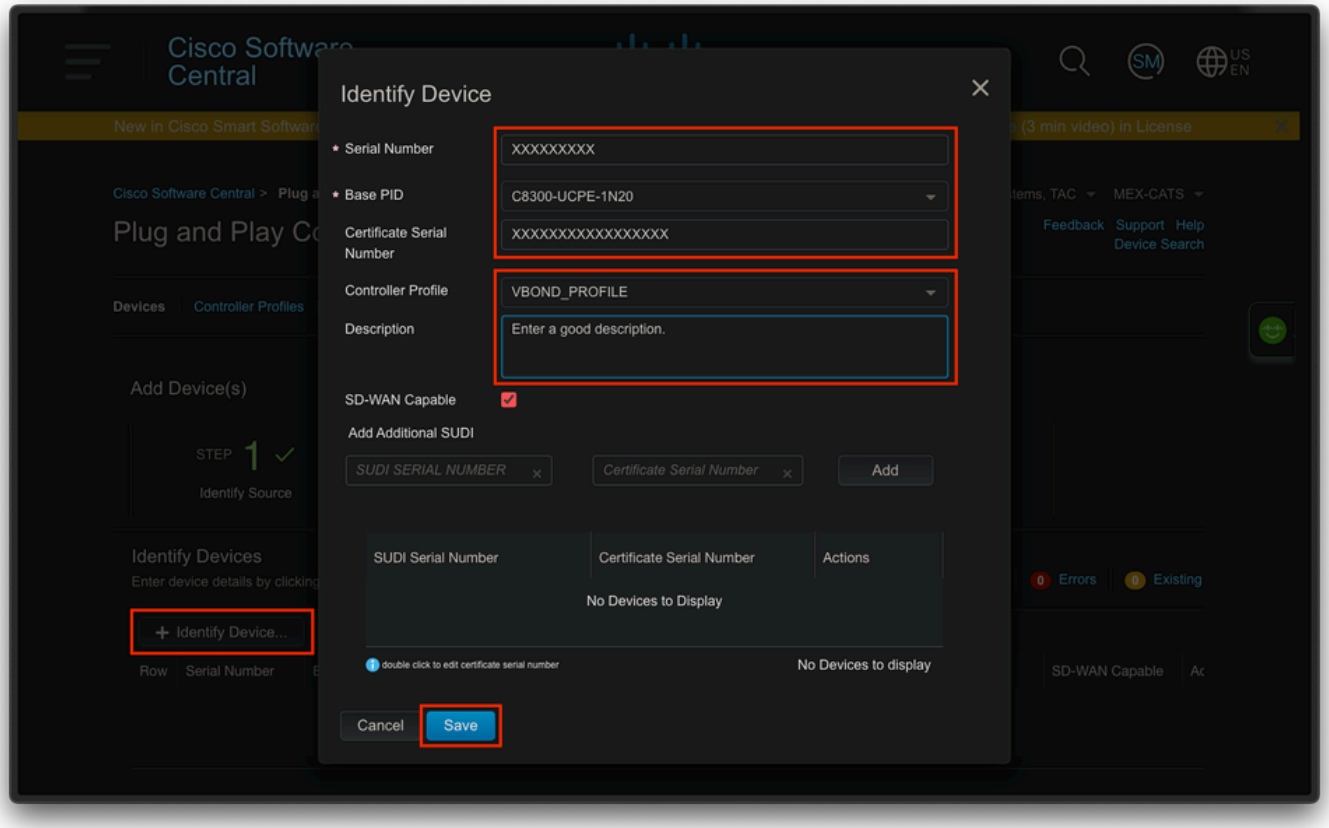


Abb. 5. Gerätekennungsformular.

Klicken Sie nach dem Speichern für Schritt 3 auf Weiter und für Schritt 4 auf Senden.

PnP in NFVIS

Weitere Informationen zu den verschiedenen Konfigurationseinstellungen für PnP in NFVIS, die sowohl den automatischen als auch den statischen Modus abdecken, finden Sie in der Ressource: [NFVIS PnP Commands.]

Es ist zu beachten, dass PnP in allen NFVIS-Versionen standardmäßig aktiviert ist.

vManage-Synchronisierung mit PnP

Online-Modus

Wenn vManage auf das Internet und das PnP-Portal zugreifen kann, müssen Sie nur in der Lage

sein, eine SA/VA-Synchronisierung durchzuführen. Navigieren Sie zu Configuration > Devices (Konfiguration > Geräte), und klicken Sie auf eine Textschaltfläche, die "Sync Smart Account" (Smart Account synchronisieren) anzeigt. Anmeldeinformationen, die für die Anmeldung bei Cisco Software Central verwendet werden, sind erforderlich. Stellen Sie sicher, dass der Zertifikat-Push an alle Controller gesendet wird.

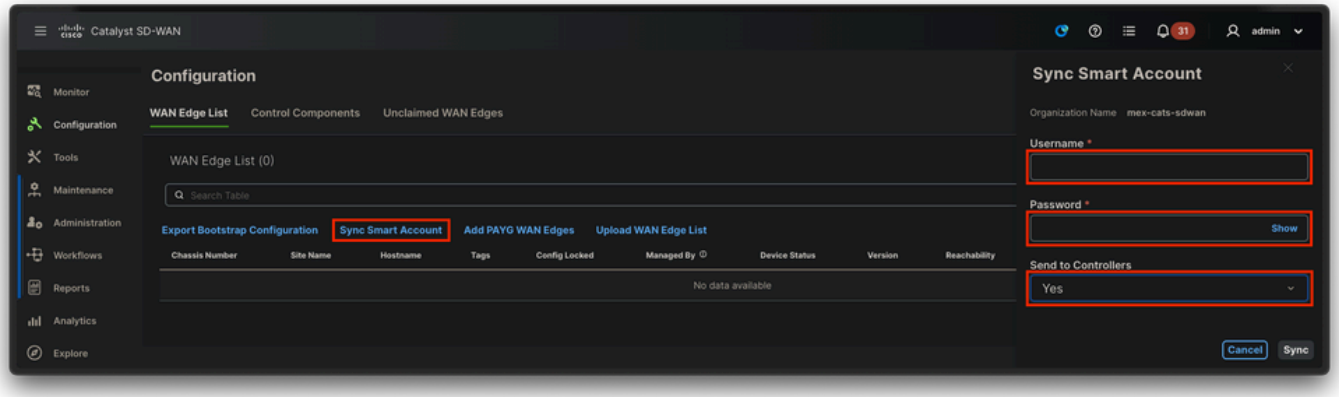


Abb. 6. WAN Edge Router-Update über SA/VA-Synchronisierung.

Offline-Modus

Wenn sich vManage in einer Laborumgebung befindet oder nicht auf das Internet zugreifen kann, können Sie manuell eine Bereitstellungsdatei aus PnP hochladen, die die SN enthalten muss, die der Geräteliste hinzugefügt wurde. Diese Datei ist vom Typ .viptela (Serielle Viptela-Datei), der über die Registerkarte "Controller-Profile" abgerufen werden kann:

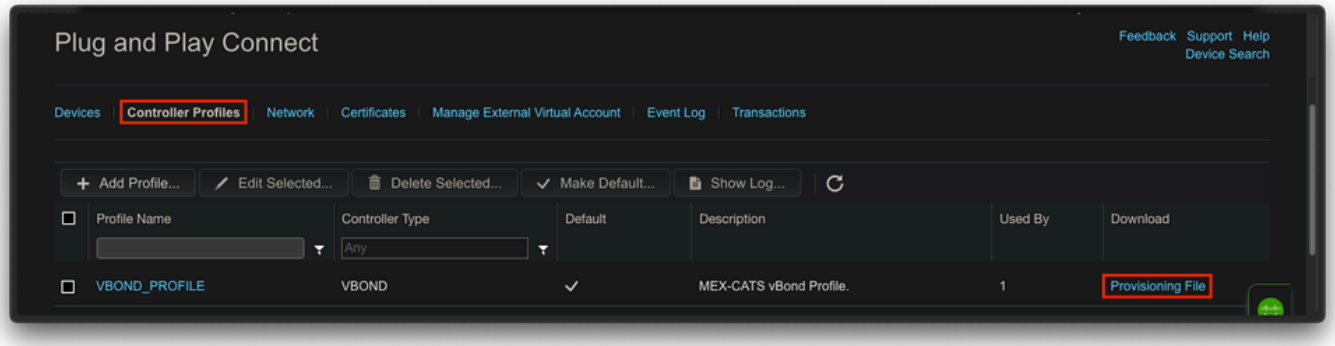


Abb. 7. Provisioning-Datei-Download für CEdge WAN-Listenaktualisierung

Um die Bereitstellungsdatei manuell hochzuladen, navigieren Sie zu Configuration > Devices, und klicken Sie auf eine Textschaltfläche, die "Upload WAN Edge List" (WAN-Edgelliste hochladen) anzeigt. Eine Seitenleiste wird angezeigt, in der Sie die jeweilige Datei per Drag-and-Drop verschieben können (wenn die Schaltfläche Hochladen nach Ausführung dieser Aktionen nicht hervorgehoben wird, klicken Sie auf Datei auswählen und suchen Sie im Popup-Fenster des Datei-Explorers manuell nach der Datei). Stellen Sie sicher, dass der Zertifikat-Push an alle Controller gesendet wird.

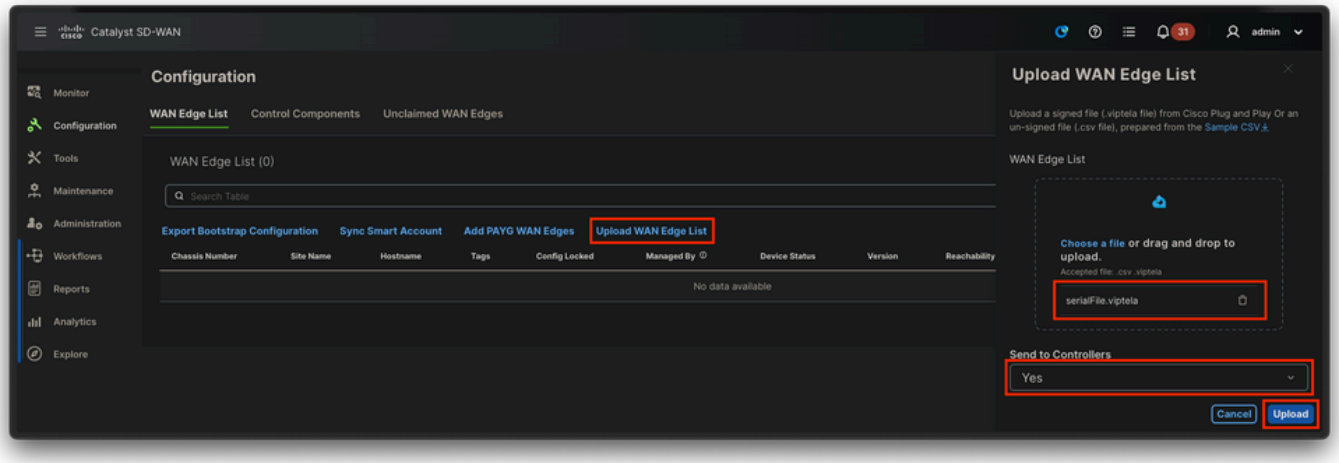


Abb. 8. WAN-Listenaktualisierung mit der aus dem PnP-Portal heruntergeladenen Bereitstellungsdatei (VSF, Viptela Serial File).

Nach Abschluss der Online- oder Offline-Methode muss in der Tabelle "WAN Edge List" (WAN-Edge-Liste) ein Geräteeintrag angezeigt werden, der der SN des in PnP registrierten Geräts entspricht:

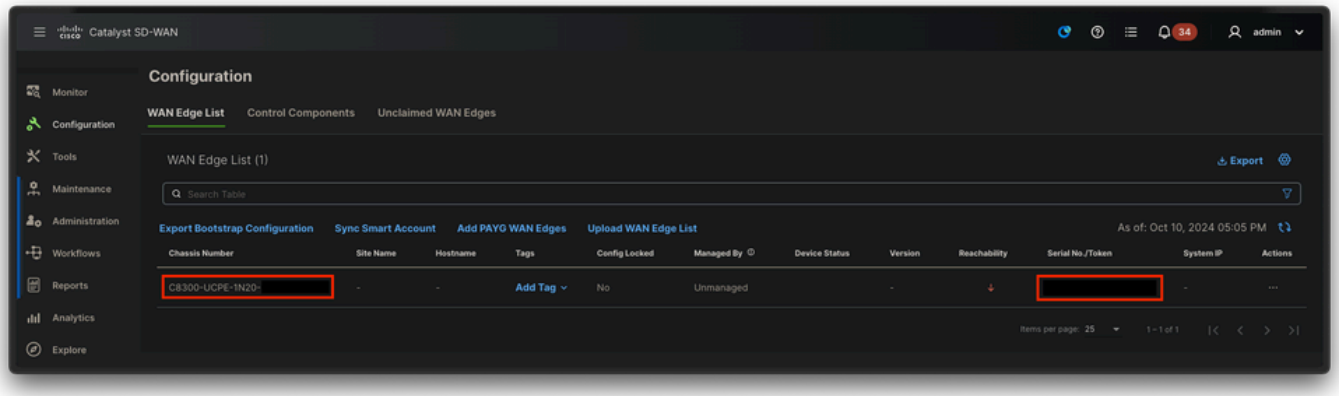
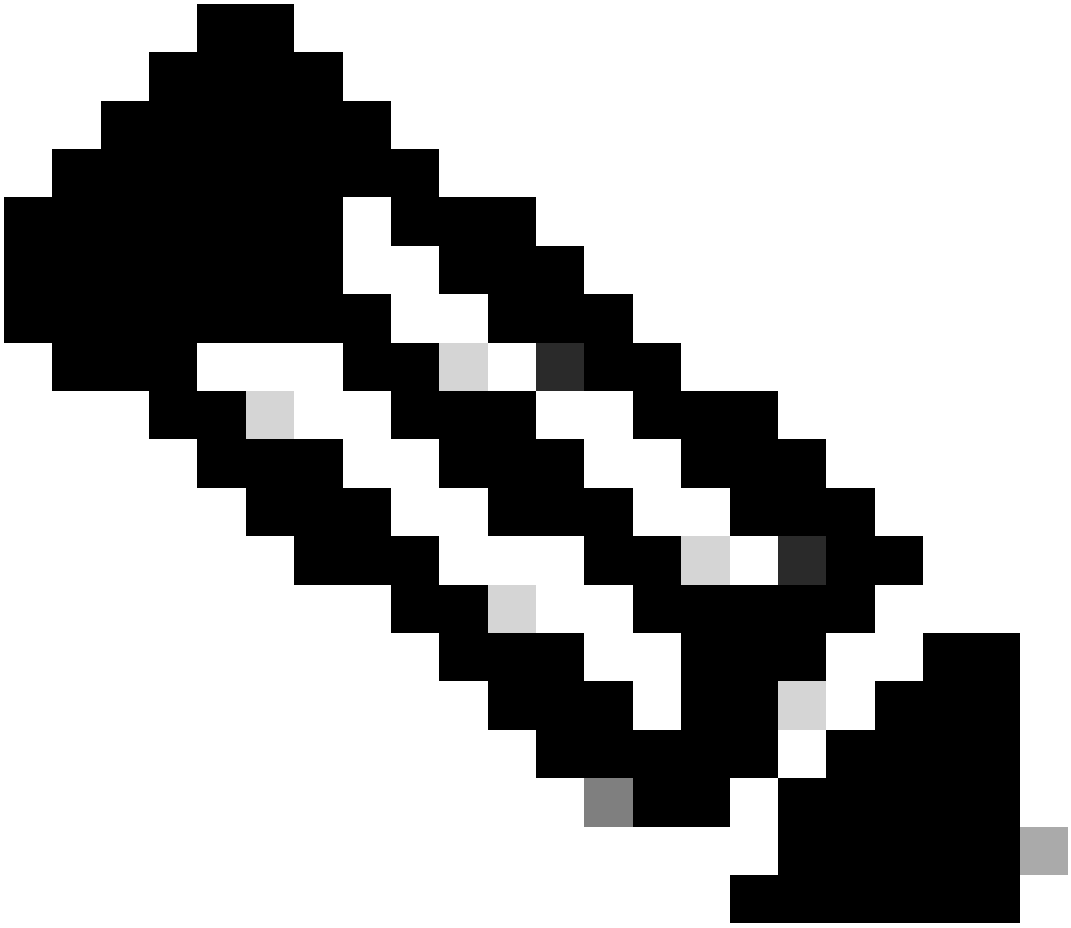


Abb. 9. 8300 Gerät in der Edge-Liste.

Automatische Onboarding- und Steuerungsanschlüsse von NFVIS

Wenn NFVIS devicehelper.cisco.com lösen kann (PnP über das Internet erreichen), wird das Onboarding automatisch durchgeführt. Ein integriertes NFVIS-System präsentiert automatisch eine Konfiguration für viptela-system:system und vpn 0, die grundlegende Controller-Informationen enthält.

Ab Cisco NFVIS Version 4.9.1 wird die Herstellung einer Steuerverbindung zur Verwaltungsebene über den Management-Port unterstützt. Der Management-Port muss über den SD-WAN-Manager erreichbar sein, damit eine erfolgreiche Verbindung mit der Kontrollebene möglich ist.



Anmerkung: Jeder Befehl, der das "system"-Schlüsselwort enthält, muss als system:system geschrieben werden. Wenn die Tabulatortaste zur Fertigstellung verwendet wird, passt sie sich automatisch an diesen neuen Standard an.

```
C8300-UCPE-NFVIS# show running-config viptela-system:system
viptela-system:system
 admin-tech-on-failure
 no vrrp-advt-with-phymac
 sp-organization-name "Cisco Systems"
 organization-name "Cisco Systems"
 vbond
```

```
port 12346 logging disk enable ! ! ntp parent no enable stratum 5 exit ! !
```

VPN 0 ist das vordefinierte Transport-VPN der SD-WAN-Lösung. Sie kann weder gelöscht noch geändert werden. Zweck dieses VPN ist die Durchsetzung einer Trennung zwischen den WAN-Transportnetzwerken (dem Underlay) und den Netzwerkdiensten (dem Overlay):

```
C8300-UCPE-NFVIS# show running-config vpn 0
vpn 0
 interface wan-br
  no shutdown
  tunnel-interface
   color gold
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   encapsulation ipsec
  !
 !
!
```

Steuerungsverbindungen sind DTLS-Sitzungen, die zwischen verschiedenen Knoten (Controllern und Edge-Routern) der SD-WAN-Fabric eingerichtet werden. Da NFVIS keine Routingplattform ist, die für Routingentscheidungen zuständig ist, bildet es keine Steuerungsverbindungen mit den vSmarts. Sofort können Sie einen "Challenge"-Status für vManage beobachten:

```
C8300-UCPE-NFVIS# show control connection
                                                                                PEER
PEER    PEER PEER            SITE       DOMAIN PEER                            PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                      PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      10.88.247.79                    12346 10.88.247.
vmanage dtls 10.10.10.10     100        0      10.88.247.71                    12946 10.88.247.
```

Dies weist in der Regel darauf hin, dass keine System-IP vorhanden ist und/oder dass der Organisationsname falsch oder gar nicht konfiguriert ist. Das PnP-Portal und vBond müssen den Organisationsnamen festlegen und sobald die Steuerverbindung mit vManage hergestellt wurde. Andernfalls können Sie diese Informationen innerhalb einer NFV-Konfigurationsgruppe (unterstützt ab Version 20.14.1) mit der entsprechenden System-IP und Standort-ID in der Vorlage weiterleiten oder sie statisch in der Unterkonfiguration viptela-system:system konfigurieren:

```
C8300-UCPE-NFVIS#(config)# viptela-system:system
C8300-UCPE-NFVIS#(config-viptela-system:system)# system-ip
```

```
C8300-UCPE-NFVIS#(config-viptela-system:system)# site-id
```

```
C8300-UCPE-NFVIS#(config-viptela-system:system)# organization-name
```

```
C8300-UCPE-NFVIS#(config-viptela-system:system)# commit Commit complete.
```

Sie finden diese Elemente in vManage:

- Name der Organisation: Administration > Einstellungen > System > Organisationsname
- Validator-IP und -Port: Administration > Settings > System > Validator

Nachdem die verbleibende Konfiguration in die Unterkonfiguration viptela-system:system eingegeben wurde, benötigen Sie aktive/aufgebaute Steuerungsverbindungen.

```
C8300-UCPE-NFVIS# show control connections
                                                                                PEER
PEER    PEER PEER            SITE       DOMAIN PEER                            PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                      PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      10.88.247.79                    12346 10.88.247.
vmanage dtls 10.10.10.10     100        0      10.88.247.71                    12946 10.88.247.
```

NFVIS verwalten

Wenn Sie NFVIS in den Status "Nicht verwaltet" zurücksetzen möchten, müssen Sie folgende

Schritte ausführen:

1. Entfernen Sie den Geräteeintrag aus dem PnP-Portal:

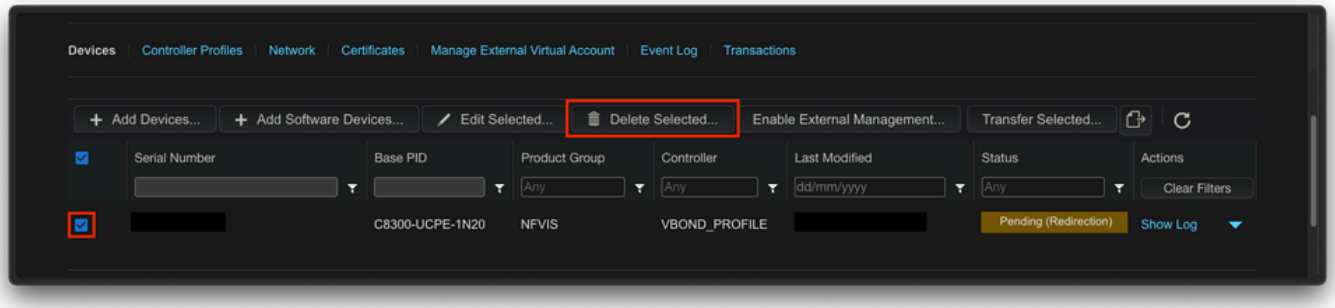


Abb. 10. 8300 Geräteentfernung aus dem PnP-Portal.

2. NFVIS auf Werkseinstellungen zurücksetzen.

```
C8300-UCPE-NFVIS# factory-default-reset all
```

3. Optionale Schritte: Entfernen Sie das Gerät aus der vManage Edge-Liste:

3.1 Das Gerätezertifikat ungültig machen.

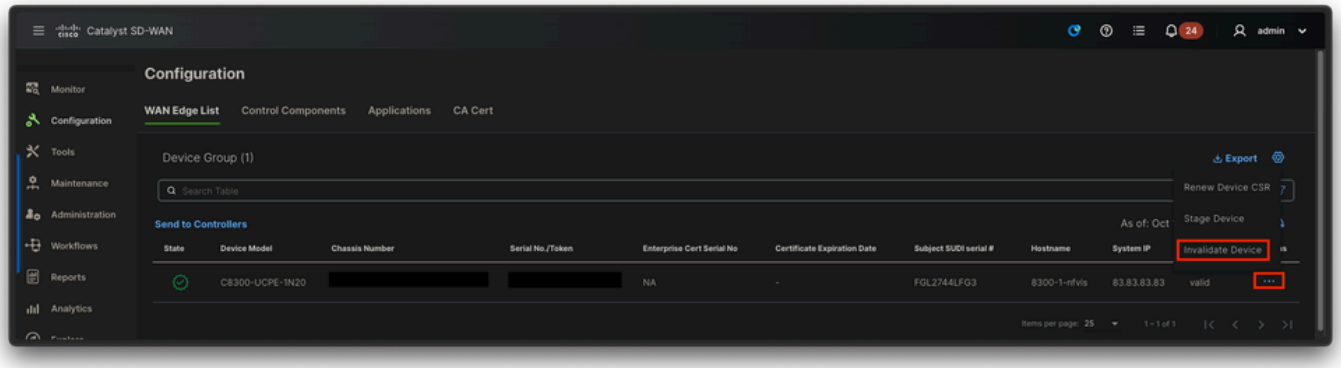


Abb. 11. 8300 Ungültigerklärung des Zertifikats.

3.2 Löschen Sie das Gerät aus der Liste der WAN-Edges.

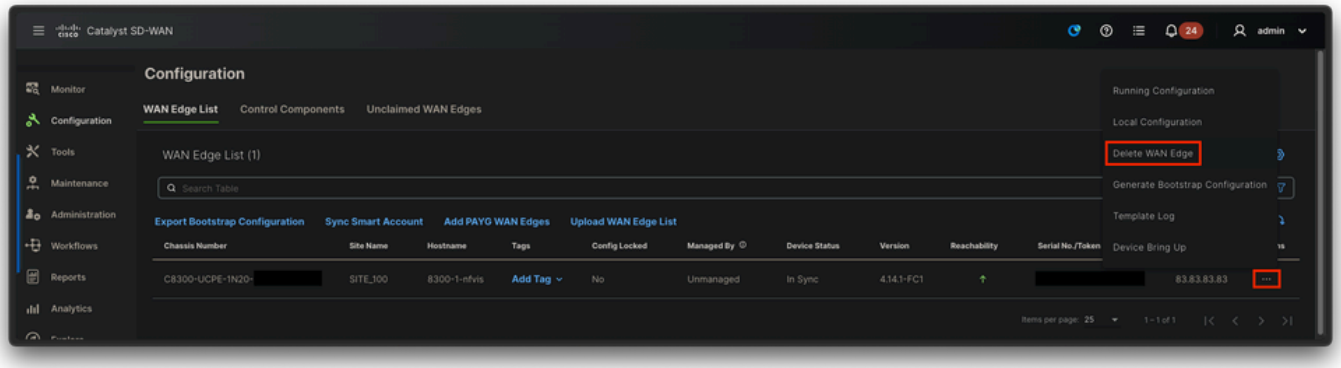


Abb. 12. 8300 Entfernung aus der WAN Edge-Liste.

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.