

# Installation und Deinstallation der UTD-Engine im SD-WAN mit CLI

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konzepte](#)

[Konfigurieren](#)

[UTD deinstallieren](#)

[Precheck](#)

[Konfigurationen](#)

[Überprüfung](#)

[Konfigurieren](#)

[Installation von UTD](#)

[Precheck](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird das Verfahren zur Installation und Deinstallation von Unified Threat Defense (UTD) über CLI in SDWAN-Routern beschrieben.

## Voraussetzungen

### Anforderungen

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

- Cisco Software-defined Wide Area Network (SD-WAN)
- Cisco IOS® XE Befehlszeilenschnittstelle (CLI)

### Verwendete Komponenten

Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- Router ISR4461/K9
- Softwareversion 17.3.4

- Router im Controller-Modus

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 verstehen.

## Hintergrundinformationen

Diese Schritte müssen angewendet werden, wenn sich der cedge im CLI-Modus befindet oder keine Kontrollverbindung zwischen vManage und cedge besteht.

Wenn Sie jedoch eine Kontrollebene haben und sich Ihr cedge im vManage-Modus befindet, lesen Sie diesen anderen Artikel .

## Konzepte

Spezifische Anforderungen für dieses Dokument:

- Cisco vManage Version 20.3 oder höher
- Cisco Integrated Services Router der Serie 4431, Version 17.3.4

Weitere Informationen zu unterstützten Plattformen finden Sie unter [UTD für SDWAN-unterstützte Plattformen und Einschränkungen](#).

## Konfigurieren

### *UTD deinstallieren*

### Precheck

Dies ist ein Beispiel dafür, wie ein Cedge-Router wie eine vorherige UTD-Deinstallation aussieht.

\* Das Gerät befindet sich im Controller-Modus, und es wurde keine Vorlage angehängt, aber die UTD-Konfiguration wurde angewendet.

```
cedge#show sdwan system Viptela (tm) vEdge Operating System Software Copyright (c) 2013-2022 by
Viptela, Inc. Controller Compatibility: 20.3 Version: 17.03.04a.0.5574 Build: Not applicable
```

**Hinweis:** Die UTD-Konfiguration muss vor der Deinstallation entfernt werden.

## Konfigurationen

1. UTD-Dienst beenden.

```
cedge#config-transaction
cedge(config)# app-hosting appid utd
cedge(config-app-hosting)# no start
cedge(config-app-hosting)# commit
```

Commit complete.

**Hinweis:** Der UTD-Status ändert sich von "Running" (Wird ausgeführt) in "Deployed" (Bereitgestellt), sobald **kein Start** angewendet wird.

```
cedge#show app-hosting list App id State -----  
-- utd DEPLOYED cedge#
```

## 2. Entfernen der UTD-Konfiguration

```
cedge#config-transaction  
cedge(config)# utd engine standard multi-tenancy  
cedge(config-utd-multi-tenancy)# no policy utd-policy-vrf-1  
cedge(config-utd-multi-tenancy)# commit  
Commit complete.  
cedge(config-utd-multi-tenancy)#  
cedge#config-transaction  
cedge(config)# utd multi-tenancy  
cedge(config)# utd engine standard multi-tenancy  
cedge(config-utd-multi-tenancy)# no threat-inspection whitelist profile Sig-white-list  
cedge(config-utd-multi-tenancy)# no threat-inspection profile IPS-POLICY  
cedge(config-utd-multi-tenancy)# exit  
cedge(config)# commit  
Commit complete.  
cedge(config)# no utd engine standard multi-tenancy  
cedge(config)# commit  
Commit complete.  
cedge(config)#  
cedge#config-transaction  
cedge(config)# no utd multi-tenancy  
cedge(config)# commit  
Commit complete.  
cedge(config)#  
cedge(config)# app-hosting appid utd  
cedge(config-app-hosting)# no app-vnic gateway0 virtualportgroup 0 guest-interface 0  
cedge(config-app-hosting)# no app-vnic gateway1 virtualportgroup 1 guest-interface 1  
cedge(config-app-hosting)# no app-resource package-profile urlf-low  
cedge(config-app-hosting)# commit  
Commit complete.  
cedge(config-app-hosting)#exit  
cedge(config)# no app-hosting appid utd  
cedge(config)# commit  
Commit complete.  
cedge(config)#  
cedge(config)# no interface VirtualPortGroup0  
cedge(config)# no interface VirtualPortGroup1  
cedge(config)# commit  
Commit complete.  
cedge(config)#  
cedge(config)# no iox  
cedge(config)# commit  
Commit complete.  
cedge(config)#
```

## 3. Validierung.

Dies ist ein Beispiel dafür, wie ein Edge-Router aussieht, wenn die UTD-Konfiguration entfernt wurde.

```
cedge#show running-config | section iox
```

```

cedge#show running-config | section VirtualPortGroup0
cedge#show running-config | section VirtualPortGroup1
cedge#show running-config | section utd
cedge#
cedge#show platform software utd global
UTD Global state
=====
Engine : Standard
Global Inspection : Disabled
Operational Mode : Intrusion Detection
Fail Policy : Fail-open
Container technology : LXC
Redirect interface : Not specified
UTD interfaces
No interfaces are protected by UTD
<snipped>

```

**Hinweis:** Obwohl die Konfiguration entfernt wurde, wird UTD als installiert angezeigt. Das wird erwartet.

```

cedge#show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.16_SV2.9.16.1_XE17.3
IOS-XE Supported UTD Regex: ^1\.0\.[0-9]+\_SV(\.*)_XE17.3$
UTD Installed Version: 1.0.16_SV2.9.16.1_XE17.3

```

```

cedge#show virtual-service
Virtual Service Global State and Virtualization Limits:
Infrastructure version : 1.7
Total virtual services installed : 1
Total virtual services activated : 0
<snipped>

```

```

cedge#show app-hosting list
The process for the command is not responding or is otherwise unavailable >>>> Expected because
UTD config was removed but UTD engine remains installed

```

```

** Before to remove Configuration **
cedge#show virtual-service version name utd running
Virtual service utd running version:
Name : UTD-Snort-Feature
Version : 1.0.16_SV2.9.16.1_XE17.3

```

```

** After configuration is removed **
cedge#
cedge#show virtual-service version name utd running
Virtual service utd running version:
Name : UTD-Snort-Feature
Version : None

```

#### 4. Entfernen Sie den UTD-Motor.

**Tip:** Sie müssen **iox** und **app-hosting appid utd** aktiviert haben, um die UTD-Engine zu deinstallieren.

Hier ist ein Beispiel dafür, was passiert, wenn UTD ohne lox- und App-Hosting-Aktivierung gelöscht wird.

```
cedge#app-hosting uninstall appid utd >>> No action is taken.
cedge#
```

Dies ist ein Beispiel für die erfolgreiche Deinstallation von UTD.

```
cedge#config-transaction
cedge(config)# iox
cedge(config)# app-hosting appid utd
cedge(config-app-hosting)# commit
Commit complete.
cedge(config-app-hosting)#
*Mar 3 20:25:24.889: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server iox has been notified
to start
*Mar 3 20:25:50.268: %IM-6-IOX_RECONCILE_INFO: R0/0: ioxman: App-hosting application reconcile
process start
*Mar 3 20:25:51.956: %IM-6-IOX_ENABLEMENT: R0/0: ioxman: IOX is ready.
cedge#
cedge#app-hosting uninstall appid utd
Uninstalling 'utd'. Use 'show app-hosting list' for progress.

cedge#
*Mar 3 20:26:31.653: %VIRT_SERVICE-5-INSTALL_STATE: Successfully uninstalled virtual service utd
*Mar 3 20:26:32.706: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Uninstall succeeded: utd
uninstalled successfully
cedge#
```

## Überprüfung

Führen Sie die nächsten Befehle aus, um zu überprüfen, ob UTD entfernt wurde.

```
cedge#show app-hosting list
No App found

cedge#show virtual-service version name utd running
% Error: Virtual-service utd is not found

cedge#show utd engine standard version
IOS-XE Recommended UTD Version: 1.0.16_SV2.9.16.1_XE17.3
IOS-XE Supported UTD Regex: ^1\.0\.[0-9+]_SV(.*)_XE17.3$

cedge#show virtual-service
Virtual Service Global State and Virtualization Limits:
Infrastructure version : 1.7
Total virtual services installed : 0
Total virtual services activated : 0
<snipped>
```

## Konfigurieren

### *Installation von UTD*

### Precheck

Überprüfen Sie die von UTD unterstützte Version, und laden Sie sie in den Bootflash herunter.

```
cedge#
cedge#show utd engine standard version
```

IOS-XE Recommended UTD Version: **1.0.16\_SV2.9.16.1\_XE17.3**  
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)\_SV(.\*)\_XE17.3\$

```
cedge#  
cedge#dir bootflash: | i utd  
36 -rw- 55050240 Mar 1 2022 01:08:29 +00:00 secapp-  
utd.17.03.04a.1.0.16_SV2.9.16.1_XE17.3.x86_64.tar  
cedge#
```

## Konfigurationen

### 1. Iox und App-Hosting aktivieren.

```
cedge#config-transaction  
cedge(config)# iox  
cedge(config)# app-hosting appid utd  
cedge(config-app-hosting)# commit  
Commit complete.  
cedge(config-app-hosting)#  
*Mar 3 20:25:24.889: %UICFGEXP-6-SERVER_NOTIFIED_START: R0/0: psd: Server iox has been notified to start  
*Mar 3 20:25:50.268: %IM-6-IOX_RECONCILE_INFO: R0/0: ioxman: App-hosting application reconcile process start  
*Mar 3 20:25:51.956: %IM-6-IOX_ENABLEMENT: R0/0: ioxman: IOX is ready.  
cedge#
```

### 2. Installieren Sie das UTD-Modul.

```
cedge#app-hosting install appid utd package bootflash:secapp-  
utd.17.03.04a.1.0.16_SV2.9.16.1_XE17.3.x86_64.tar  
Installing package 'bootflash:secapp-utd.17.03.04a.1.0.16_SV2.9.16.1_XE17.3.x86_64.tar' for  
'utd'. Use 'show app-hosting list' for progress.  
cedge#  
*Mar 3 21:07:43.529: %VMAN-5-PACKAGE_SIGNING_LEVEL_ON_INSTALL: R0/0: vman: Package 'secapp-  
utd.17.03.04a.1.0.16_SV2.9.16.1_XE17.3.x86_64.tar' for service container 'utd' is 'Cisco  
signed', signing level cached on original install is 'Cisco signed'  
*Mar 3 21:07:56.332: %VIRT_SERVICE-5-INSTALL_STATE: Successfully installed virtual service utd  
*Mar 3 21:07:56.922: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install succeeded: utd  
installed successfully Current state is deployed  
cedge#
```

### 3. Stellen Sie sicher, dass das UTD-Modul installiert ist. Ausführen der nächsten Befehle

**Hinweis:** Der Status "**BEREITGESTELLT**" bedeutet, dass **UTD installiert, aber nicht konfiguriert ist**. Der Status **RUNNING** bedeutet "**UTD installiert und konfiguriert**".

```
cedge#show app-hosting list App id State -----  
-- utd DEPLOYED cedge#show virtual-service version name utd running Virtual service utd running  
version: Name : UTD-Snort-Feature Version : None >>>> "None", it is expected due to the fact  
that no config yet cedge#show utd engine standard version UTD Virtual-service Name: utd IOS-XE  
Recommended UTD Version: 1.0.16_SV2.9.16.1_XE17.3 IOS-XE Supported UTD Regex: ^1\.0\.([0-  
9]+)_SV(.*)_XE17.3$ UTD Installed Version: 1.0.16_SV2.9.16.1_XE17.3 >>>> UTD Package installed  
cedge# cedge#show virtual-service Virtual Service Global State and Virtualization Limits:  
Infrastructure version : 1.7 Total virtual services installed : 1 >>>> Installed 1 but Activated  
0 as expected Total virtual services activated : 0
```

### 4. Um den Status "RUNNING" für UTD festzulegen, fahren Sie mit der Konfiguration von IPS/URL fort. Dies ist ein Beispiel aus dem Labor.

```

cedge#config-transaction
cedge(config)# interface VirtualPortGroup0
cedge(config-if)# description Management interface
cedge(config-if)# vrf forwarding 65529
cedge(config-if)# ip address 192.168.1.1 255.255.255.252
cedge(config-if)# exit
cedge(config)# commit
Commit complete.
cedge(config)#
cedge(config)# interface VirtualPortGroup1
cedge(config-if)# description Data interface
cedge(config-if)# ip address 192.168.2.1 255.255.255.252
cedge(config-if)# exit
cedge(config)# commit
Commit complete.
cedge(config)#
cedge(config)# app-hosting appid utd
cedge(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 0
cedge(config-app-hosting-gateway)# guest-ipaddress 192.168.1.2 netmask 255.255.255.252
cedge(config-app-hosting-gateway)# exit
cedge(config-app-hosting)# app-vnic gateway1 virtualportgroup 1 guest-interface 1
cedge(config-app-hosting-gateway)# guest-ipaddress 192.168.2.2 netmask 255.255.255.252
cedge(config-app-hosting-gateway)# exit
cedge(config-app-hosting)# app-resource package-profile urlf-low
cedge(config-app-hosting)# start
cedge(config-app-hosting)# commit
Commit complete.
cedge(config-app-hosting)#
cedge(config-app-hosting)# exit
cedge(config)# utd multi-tenancy
cedge(config)# utd engine standard multi-tenancy
cedge(config-utd-multi-tenancy)# threat-inspection whitelist profile Sig-white-list
cedge(config-utd-mt-whitelist)# generator id 3 signature id 22089
cedge(config-utd-mt-whitelist)# generator id 3 signature id 36208
cedge(config-utd-mt-whitelist)# exit
cedge(config-utd-multi-tenancy)# threat-inspection profile IPS-POLICY
cedge(config-utd-mt-threat)# threat detection
cedge(config-utd-mt-threat)# policy balanced
cedge(config-utd-mt-threat)# whitelist profile Sig-white-list
cedge(config-utd-mt-threat)# logging level alert
cedge(config-utd-mt-threat)# exit
cedge(config-utd-multi-tenancy)# commit
Commit complete.
cedge(config-utd-multi-tenancy)#
cedge(config-utd-multi-tenancy)# policy utd-policy-vrf-1
cedge(config-utd-mt-policy)# vrf 511
cedge(config-utd-mt-policy)# all-interfaces
cedge(config-utd-mt-policy)# fail close
cedge(config-utd-mt-policy)# threat-inspection profile IPS-POLICY
cedge(config-utd-mt-policy)# exit
cedge(config-utd-multi-tenancy)# commit
Commit complete.
cedge(config-utd-multi-tenancy)#
cedge(config-utd-multi-tenancy)# end
cedge#

```

## 5. Sicherstellen, dass die Konfiguration abgeschlossen ist

```

cedge#show run | section utd
utd multi-tenancy
utd engine standard multi-tenancy
threat-inspection whitelist profile Sig-white-list

```

```

generator id 3 signature id 22089
generator id 3 signature id 36208
threat-inspection profile IPS-POLICY
threat detection
policy balanced
logging level alert
whitelist profile Sig-white-list
policy utd-policy-vrf-1
vrf 511
all-interfaces
threat-inspection profile IPS-POLICY
fail close
app-hosting appid utd
app-vnic gateway0 virtualportgroup 0 guest-interface 0
guest-ipaddress 192.168.1.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 1 guest-interface 1
guest-ipaddress 192.168.2.2 netmask 255.255.255.252
app-resource package-profile urlf-low
start
cedge#

```

## Überprüfung

1. Führen Sie **show logging** aus, und stellen Sie sicher, dass Sie ähnliche Protokolle erhalten, wie als Nächstes gezeigt.

```

*Mar 3 23:17:17.573: %LINK-3-UPDOWN: Interface VirtualPortGroup0, changed state to up *Mar 3
23:17:18.094: %LINK-3-UPDOWN: Interface VirtualPortGroup1, changed state to up *Mar 3
23:17:18.572: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup0, changed state
to up *Mar 3 23:17:19.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup1,
changed state to up *Mar 3 23:17:25.630: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel2000000001, changed state to up *Mar 3 23:19:36.863: %VIRT_SERVICE-5-ACTIVATION_STATE:
Successfully activated virtual service utd *Mar 3 23:19:37.577: %IM-6-START_MSG: R0/0: ioxman:
app-hosting: Start succeeded: utd started successfully Current state is running *Mar 3
23:19:38.318: %ONEP_BASE-6-CONNECT: [Element]: ONEP session Application:utd_snort Host:cedge
ID:6633 User: has connected. *Mar 3 23:19:50.428: %IOSXE_UTD-4-MT_CONFIG_DOWNLOAD: UTD MT
configuration download has started *Mar 3 23:20:06.460: %IOSXE_UTD-4-MT_CONFIG_DOWNLOAD: UTD MT
configuration download has completed *Mar 3 23:20:08.389: %IOSXE-5-PLATFORM: R0/0: cpp_cp:
QFP:0.0 Thread:011 TS:00000780131568867961 %SDVT-5-SDVT_HEALTH_UP: Service node is up for
channel Threat Defense. Current Health: Green, Previous Health: Down

```

**Hinweis:** Der aktuelle Zustand ändert sich von **Nach unten** zu **Grün**, wenn die Konfiguration erfolgreich durchgeführt wurde.

2. Führen Sie diese Befehle aus, um die UTD-Installation zu überprüfen.

```

cedge#show app-hosting list App id State -----
-- utd RUNNING >>> State change from Deployed to Running cedge#show utd engine standard version
UTD Virtual-service Name: utd IOS-XE Recommended UTD Version: 1.0.16_SV2.9.16.1_XE17.3 IOS-XE
Supported UTD Regex: ^1\.0\.[(0-9)+]_SV(.*)_XE17.3$ UTD Installed Version:
1.0.16_SV2.9.16.1_XE17.3 cedge#show virtual-service version name utd running Virtual service utd
running version: Name : UTD-Snort-Feature Version : 1.0.16_SV2.9.16.1_XE17.3 >>>> Changed from
NONE to "1.0.16_SV2.9.16.1_XE17.3" after config. cedge# cedge#show virtual-service Virtual
Service Global State and Virtualization Limits: Infrastructure version : 1.7 Total virtual
services installed : 1 Total virtual services activated : 1 >>>>>>>> Now it is activated

```

## Fehlerbehebung



In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

## Nützliche Befehle

```
show platform software device-mode
show app-hosting list
show virtual-service version name utd running
show utd engine standard version
show utd engine standard status
show virtual-service
```

## Zugehörige Informationen

- [Leitfaden zur Sicherheitskonfiguration: Unified Threat Defense, Cisco IOS XE 17](#)
- [Leitfaden zur Sicherheitskonfiguration: Unified Threat Defense, Cisco IOS XE 16](#)
- [UTD für SDWAN-unterstützte Plattformen und Einschränkungen.](#)
- [Installieren Sie UTD mit vManage.](#)

## 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.