

Upgrade-Verfahren für FireAMP Private Cloud 3.0.1

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Hardware-Anforderungen](#)

[Verwendete Komponenten](#)

[Upgrade-Prozess](#)

[1. Herunterladen und Installieren aktualisieren](#)

[2. Backup-Erfassung und -Herunterfahren](#)

[3. Installation neuer Versionen](#)

[4. Backup-Wiederherstellung](#)

[5. Zertifizierungsstellen](#)

[6. Authentifizierungsdienst](#)

[7. Installation](#)

[8. Prüfungen nach dem Upgrade](#)

[Änderungen bei Virtual Private Cloud 3.0.1](#)

[1. Windows Connector Version 6.1.7](#)

[2. Zertifizierungsstellen und Authentifizierungsdienst](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie ein Upgrade von FireAMP Private Cloud (vPC) Version 2.4.4 auf Version 3.0.1 durchführen. Beachten Sie, dass für die Aktualisierung eine neue Virtual Machine-Instanz für die Version 3.0.1 erforderlich ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Installation einer OVA-Vorlage (Open Virtual Appliance) im VMWare ESXi
- Grundkenntnisse der Funktionsweise und des Betriebs der Virtual AMP Cloud

Hardware-Anforderungen

Nachstehend finden Sie die Hardware-Mindestanforderungen für die FireAMP Private Cloud:

- vSphere ESX 5 oder höher

- 8 CPUs
- 64 GB RAM
- 1 TB freier Festplattenspeicher im VMWare-Datenspeicher
- Laufwerkstyp: SSD erforderlich
- RAID-Typ: Eine RAID 10-Gruppe (Stripe aus Spiegeln)
- Mindestgröße des VMware-Datenspeichers: 1 TB
- Minimum Data Store Random Reads für die RAID 10-Gruppe (4.000): 60.000 IOPS
- Minimum Data Store Random Writes for the RAID 10 Group (4K): 30.000 IOPS

Vorsicht: Die Private Cloud OVA erstellt die Festplattenpartitionen, sodass sie nicht in VMWare angegeben werden müssen.

Hinweis: Weitere Informationen zu den Hardwareanforderungen finden Sie im [FireAMP Private Cloud-Benutzerhandbuch](#).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- FireAMP Private Cloud 2.4.4
- FireAMP Private Cloud 3.0.1
- VMWare ESXi 5.0 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Upgrade-Prozess

Dieser Abschnitt enthält schrittweise Anweisungen zum Erfassen der Sicherung von der FireAMP Private Cloud 2.4.4-Version und zum ordnungsgemäßen Wiederherstellen der Sicherung in der FireAMP Private Cloud 3.0.1-Version.

Vorsicht: Upgrades können Ausfallzeiten in Ihrer Umgebung verursachen. Connectors (einschließlich AMP für Netzwerke, die mit Ihrer Virtual Private Cloud verbunden sind), die die Private Cloud verwenden, können die Verbindung zur Virtual Cloud verlieren und ihre Funktionalität kann dadurch eingeschränkt werden.

1. Herunterladen und Installieren aktualisieren

Stellen Sie sicher, dass Ihre FireAMP Virtual Private Cloud 2.4.4 auf dem neuesten Stand ist.

Schritt 1: Navigieren Sie zu **Operations** -> **Update Device** im Administratorportal.

Schritt 2: Klicken Sie auf die Schaltfläche **Check/Download Updates** (wie im Bild gezeigt), um sicherzustellen, dass Ihre FireAMP Virtual Private Cloud, von der aus die Sicherung erfolgt, auf dem neuesten Stand ist (im Hinblick auf Inhalte und Software).

Updates keep your Private Cloud device up to date.

Check/Download Updates

Content

2.4.4_1528990794
Client Definitions, DFC, Tetra Content Version

Update Content

Software

✓ 2.4.4_1528991036
Private Cloud Software Version

Update Software

Checked 43 minutes ago; software is up to date.

Schritt 3: Nach der Installation von Content- und Software-Updates zeigt die Aktualisierungsseite die Informationen an, die das Gerät auf dem neuesten Stand hat, wie im Bild gezeigt.

Updates keep your Private Cloud device up to date.

Check/Download Updates

Content

✓ 2.4.4.20190424060125
Client Definitions, DFC, Tetra Content Version

Update Content

Checked 1 minute ago; content is up to date.

Software

✓ 2.4.4_1528991036
Private Cloud Software Version

Update Software

Checked 35 minutes ago; software is up to date.

2. Backup-Erfassung und -Herunterfahren

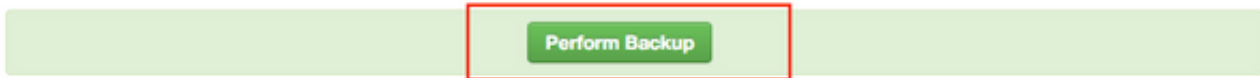
Schritt 1: Navigieren Sie zu **Operations -> Backups**.

Schritt 2: Klicken Sie im Abschnitt Manuelle Sicherung auf die Schaltfläche **Sicherung durchführen**. Die Prozedur startet eine Sicherungserstellung.



Backups create a copy of your FireAMP Private Cloud databases in /data/backups named amp-backup-YYYYMMDD-hhmm.ss.bak, where YYYY is the year, MM is the month, DD is the day, hh is the hour, mm the minute, and ss the second the backup was run.

Manage Schedule Notifications

Manual Backup



Previous Backups

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20190424-0000.01.bak	359 MB	2019-04-24 00:00:37 +0000 about 7 hours ago	 

Schritt 3: Wenn der Vorgang erfolgreich abgeschlossen wurde, wird die erfolgreiche Benachrichtigung angezeigt, wie im Bild gezeigt.

The backup was successful.

Backups create a copy of your FireAMP Private Cloud databases in /data/backups named amp-backup-YYYYMMDD-hhmm.ss.bak, where YYYY is the year, MM is the month, DD is the day, hh is the hour, mm the minute, and ss the second the backup was run.

Manage Schedule Notifications





Manual Backup


Perform Backup

Last Manual Backup Successful

Backup Job Details

Previous Backups

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20190424-0825.43.bak	352 MB	2019-04-24 08:26:18 +0000 less than a minute ago	 
/data/backups/amp-backup-20190424-0800.01.bak	359 MB	2019-04-24 00:00:37 +0000 about 8 hours ago	 

Schritt 4: Klicken -Taste. Stellen Sie sicher, dass die Sicherung ordnungsgemäß heruntergeladen und an einem sicheren Ort gespeichert wurde.

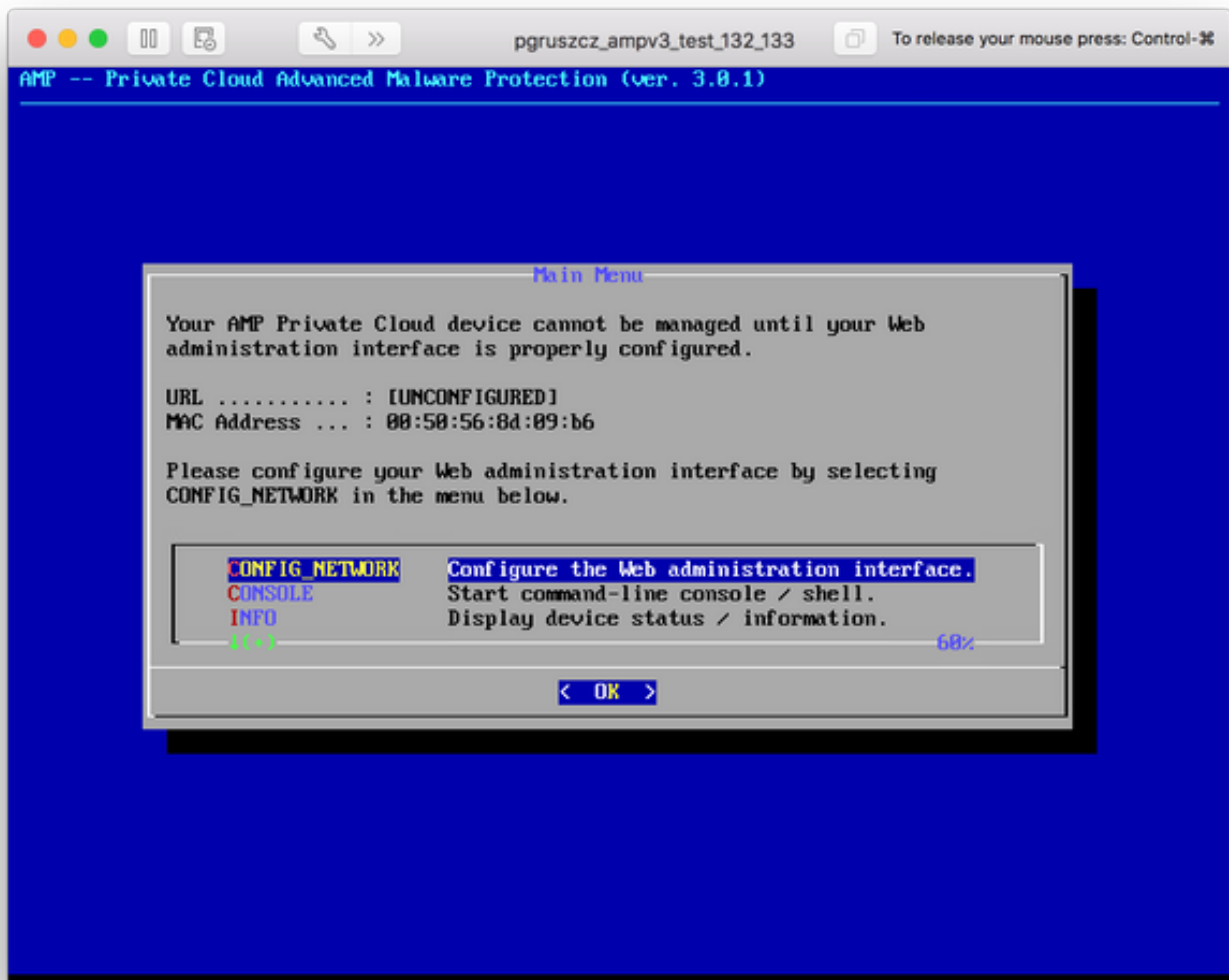
3. Installation neuer Versionen

In diesem Abschnitt wird davon ausgegangen, dass Virtual Machine für 3.0.1 FireAMP Virtual Private Cloud bereits bereitgestellt ist. Installationsverfahren für Virtual Machine für 3.0.1 OVA auf VMWare ESXi finden Sie unter dem Link: [Bereitstellen einer OVA-Datei auf einem ESX-Server.](#)

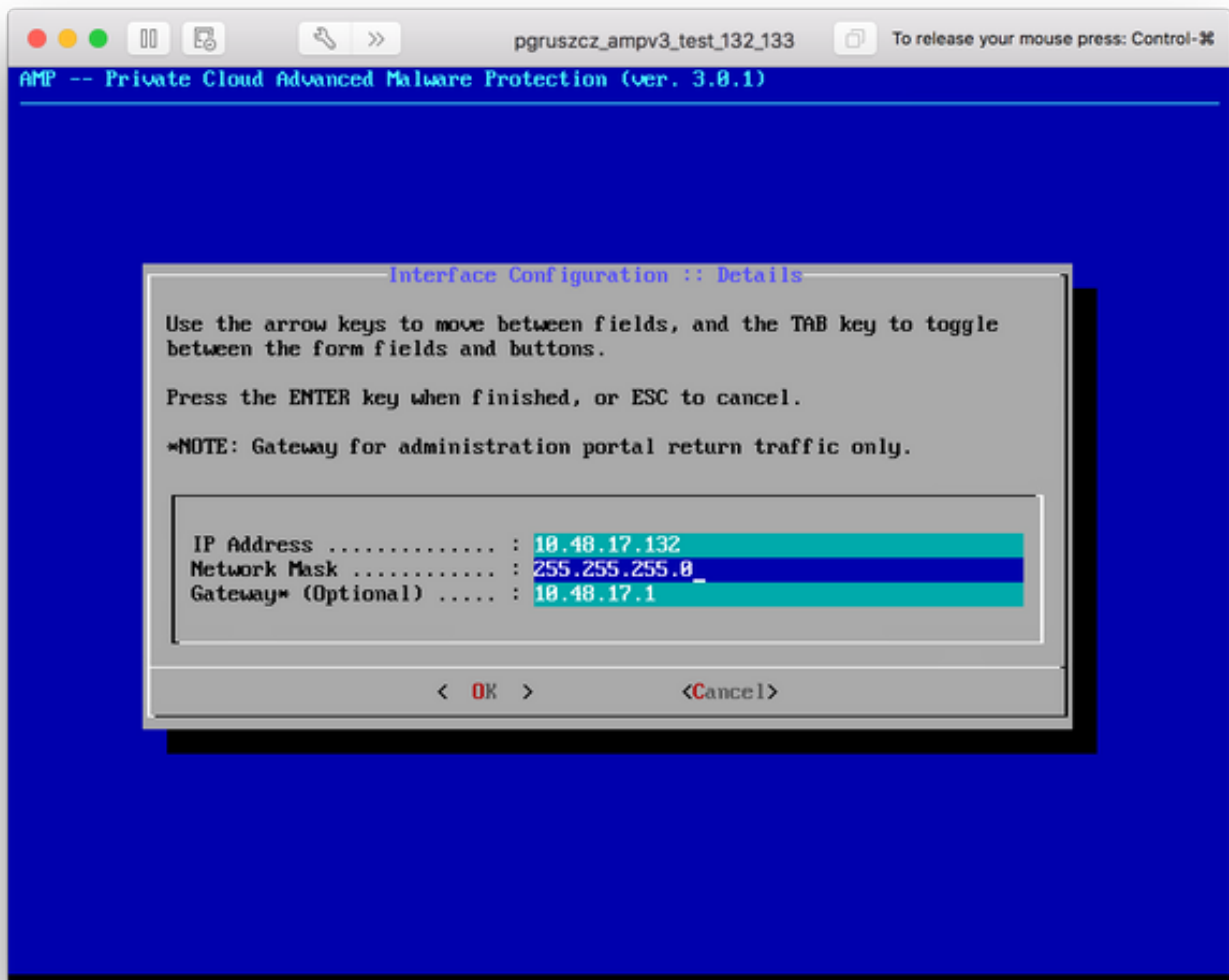
Hinweis: Das im Artikel beschriebene Verfahren verwendet exakt dieselben Hostnamen und IP-Adressen für FireAMP Virtual Private Cloud 2.4.4 und 3.0.1. Wenn Sie diesem Leitfaden folgen, müssen Sie FireAMP Virtual Private Cloud 2.4.4 nach der Sicherung beenden.

Schritt 1: Öffnen Sie das Konsolenterminal für die neu erstellte Virtual Machine-Instanz, bei der die Version 3.0.1 installiert ist. Sie können durch **Tab**, **Enter** und **Pfeil** Tasten navigieren.

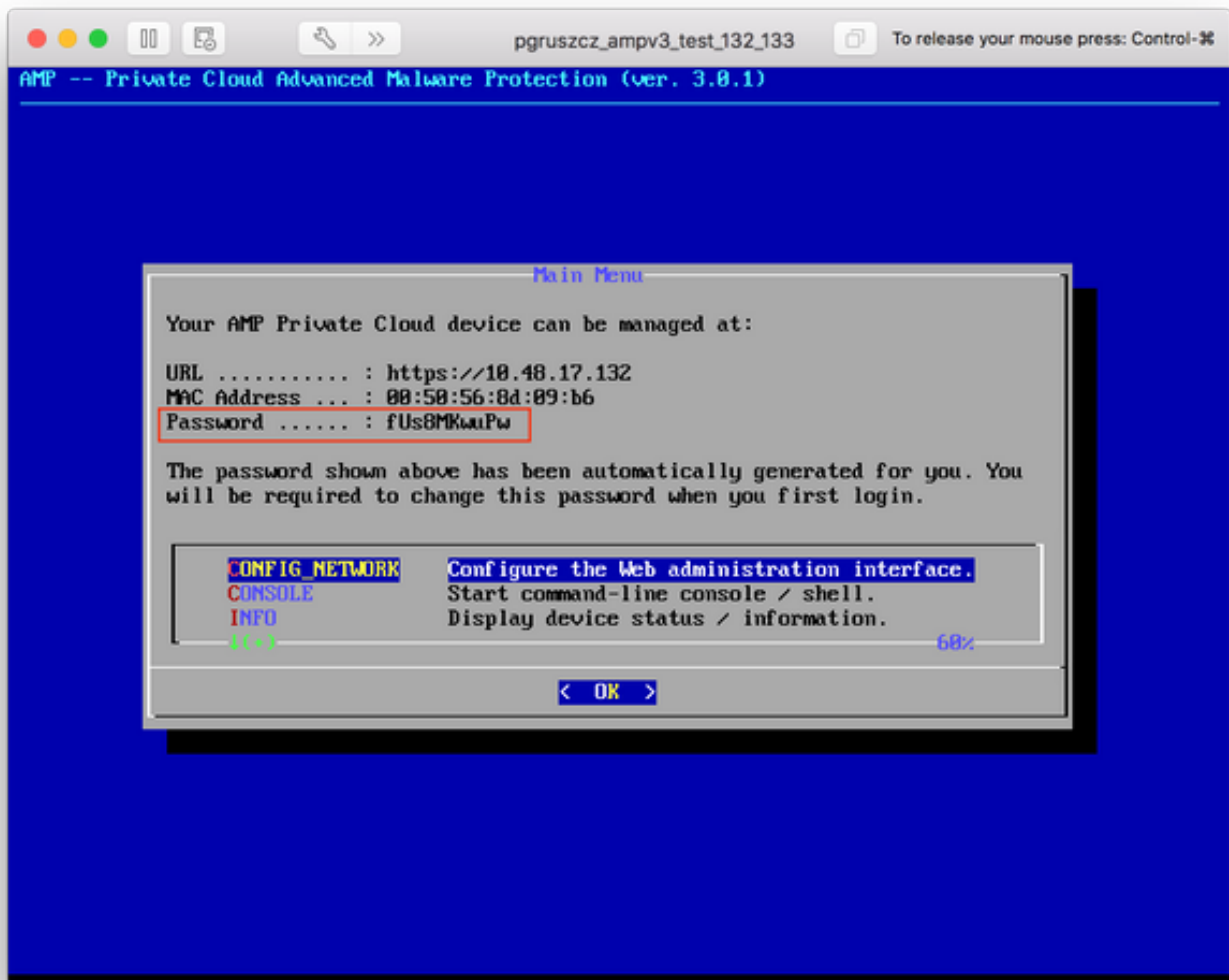
Schritt 2: Navigieren Sie zu **CONFIG_NETWORK** und klicken Sie auf die **Eingabetaste** auf Ihrer Tastatur, um die Konfiguration der Management-IP-Adresse für die FireAMP Private Cloud zu starten. Wenn Sie DHCP nicht verwenden möchten, wählen Sie **Nein** und drücken Sie die **Eingabetaste**.



Schritt 3: Geben Sie die **IP-Adresse**, die **Netzwerkmaske** und das **Standard-Gateway** ein. Navigieren Sie zu **OK**, wie im Bild gezeigt. Drücken Sie die Eingabetaste.



Schritt 4: Die Änderung der Netzwerkkonfiguration erfordert einen Neustart der Schnittstelle. Nach dem Neustart wird das Hauptkonsolenmenü erneut angezeigt, wie im Bild gezeigt. Diesmal sehen Sie eine IP-Adresse in der URL-Zeile. Beachten Sie außerdem, dass das ursprüngliche **Kennwort** angezeigt wird. Dies ist ein einmaliges Kennwort (später als **erstes Kennwort** bezeichnet), das in der webbasierten Einrichtung verwendet wird.



Schritt 5: Öffnen Sie einen Webbrowser, und navigieren Sie zur Management-IP-Adresse der Appliance. Sie erhalten einen Zertifikatsfehler, da die FireAMP Private Cloud zunächst ein eigenes HTTPS-Zertifikat generiert. Konfigurieren Sie Ihren Browser so, dass das selbstsignierte Zertifikat der FireAMP Private Cloud temporär als vertrauenswürdig gilt.

Schritt 6: Sie erhalten einen Bildschirm zur Eingabe eines Kennworts, wie im Bild gezeigt. Verwenden Sie das **ursprüngliche Kennwort** über die Konsole. Klicken Sie auf **Anmelden**.



Password Required

Authentication is required to administer your FireAMP Private Cloud device. The password can be found on the device console of your Private Cloud device.

Login

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

Support

Schritt 7: Nach erfolgreicher Anmeldung müssen Sie das Kennwort ändern. Verwenden Sie das **ursprüngliche Kennwort** in der Konsole im Feld **Altes Kennwort**. Verwenden Sie Ihr neues Kennwort zweimal in den Feldern **Neues Kennwort**. Klicken Sie auf **Kennwort ändern**.



Private Cloud Administration Portal

Support ? Help Logout

Configuration Operations Status Integrations Support

Password Expired

Change the password used to access the FireAMP Private Cloud Administration Portal and the device console. Note that this is also the root password for your device.

Warning

Your device password is used to authenticate to the Administration Portal as well as the device console. It may not be possible to paste complex passwords or passwords with non-keyboard characters into the device console.

Change Password

4. Backup-Wiederherstellung

Schritt 1: Die Willkommenseite des Admin-Portals bietet zwei Möglichkeiten zur 3.0.1-Installation von FireAMP Virtual Cloud, wie im Bild gezeigt.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Clean Installation

Start >

Restore

Local Remote Upload

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

+ Choose Restore File

/data

Start >

Schritt 2: Sie können eine von drei verschiedenen Methoden auswählen, um die Sicherungsdatei in die neu erstellte FireAMP Virtual Private Cloud-Instanz hochzuladen:

Lokal - Stellt die Konfiguration aus einer Sicherungsdatei wieder her, die bereits auf dem Gerät angezeigt wird (Sie müssen die Datei über SFTP oder SCP auf der Appliance speichern). Dateien werden nach Beginn des Wiederherstellungsprozesses in das richtige Verzeichnis extrahiert. Aus diesem Grund wird empfohlen ist /data directory.

Remote - Wiederherstellen von einer Datei auf einem HTTP-Server, auf den remote zugegriffen werden kann.

Hochladen - Wiederherstellen aus der von Ihrem Browser hochgeladenen Datei. Funktioniert nur, wenn die Sicherungsdatei kleiner als 20 MB ist.

In diesem Beispiel wurde die Remote-Option gewählt.

Hinweis: Der HTTP-Server muss über eine geeignete Verbindung verfügen. Die Sicherungsdatei muss aus Sicht der Private Cloud zugänglich sein.

Klicken Sie auf **Start**, um mit der Wiederherstellung fortzufahren, wie im Bild gezeigt.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Clean Installation

Start >

Restore

Local Remote Upload

Restore from a file on a remotely accessible server.

http://10.48.26.106/amp-backup-20190424-1044.11.bak

/data

Start >

Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Clean Installation

Start >

Restore

Local Remote Upload

Restore from a file on a remotely accessible server.

http://10.48.26.106/amp-backup-20190424-1044.11.bak

/data

Start >

Schritt 3: Durch das Wiederherstellen der Prozedur aus einer Sicherung wird die aktuelle Konfiguration ersetzt. Die SSH-Hostschlüssel des Geräts und das Administratorportal-Kennwort werden ersetzt. Sie können Teile Ihrer Konfiguration im Hinblick auf die Installation überprüfen.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Preparing Restore

Your restore file is being processed, please wait.

```
portal/fireAMP/linux/1.7.0.545/rhel/7/CURRENT_REVISION
portal/fireAMP/linux/1.7.0.545/rhel/6
portal/fireAMP/linux/1.7.0.545/rhel/6/ciscoampconnector-1.7.0.545-1.el6.x86_64.rpm
portal/fireAMP/linux/1.7.0.545/rhel/6/fireamp-linux.tar.gz
portal/fireAMP/linux/1.7.0.545/rhel/6/CURRENT_REVISION
portal/fireAMP/linux/1.7.0.545/update.xml
portal/fireAMP/protectent
portal/fireAMP/protectent/REVISION
portal/fireAMP/protectent/5.1.15.10683
portal/fireAMP/protectent/5.1.15.10683/installer-32-tcp.exe
```

Clean Installation

Start >

Restore

Local Remote Upload

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

+ Choose Restore File

Start >

Schritt 4: Nach einer erfolgreichen Kopie der Sicherungsdatei wird auf der Wiederherstellungsseite die im Bild dargestellte Popup-Meldung angezeigt. Klicken Sie auf die Schaltfläche "Verwaltungsportal jetzt neu konfigurieren", um den Wiederherstellungsvorgang abzuschließen.

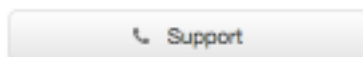
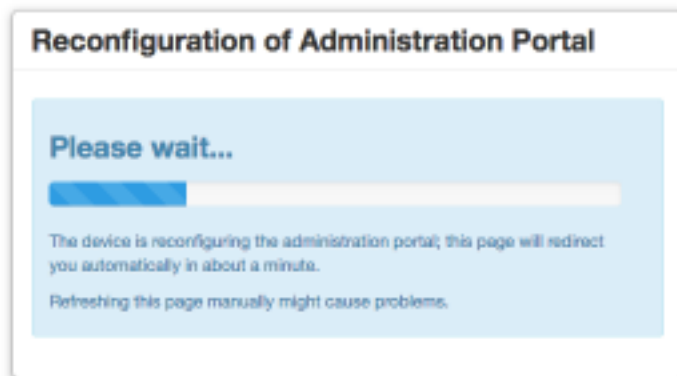


Reconfiguration of Administration Portal

Reconfiguration of the Administration Portal must be performed to update authentication configuration and certificates.

Reconfigure Administration Portal Now

Support



Schritt 5: Nach Abschluss der Neukonfiguration wird die Seite für das Administrationsportal erneut angezeigt, wie im Bild gezeigt. Um sich jetzt anzumelden, müssen Sie das Kennwort des 2.4.4 FireAMP Virtual Private Cloud-Backups verwenden.

Bild zeigt die meiste Arbeit für die richtige Installation wie bereits getan (Kontrollfelder). Es wird erwartet, dass die Konfiguration durch Backup über FireAMP Virtual Private Cloud 2.4.4 wiederhergestellt wird.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Review and Install

▶ Start Installation

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Restore Ready

Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.

Clean Installation

Start >

Restore

Local Remote **Upload**

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

+ Choose Restore File

Start >

5. Zertifizierungsstellen

Die Version 3.0.1 der FireAMP Virtual Private Cloud bietet neue Funktionen und Verhaltensweisen für den Systembetrieb. Diese müssen konfiguriert und abgeschlossen werden, bevor Sie mit der Installation beginnen können.

Die erste Komponente, die neu ist und in der früheren Version nicht enthalten war, sind **Zertifizierungsstellen**.

Auf der Seite **Zertifizierungsstellen** können Sie Stammzertifikate für Ihre Dienste verwalten, wenn Sie eine benutzerdefinierte Zertifizierungsstelle verwenden möchten. Sie können Ihr Stammzertifikat bei Bedarf herunterladen oder löschen.

Hinweis: Der vertrauenswürdige Speicher der Zertifizierungsstellen wird nur für virtuelle Cloud-Services verwendet (zum Erstellen und Validieren der richtigen Zertifikatkette). Sie wird nicht für verschiedene vPC-Integrationen wie ThreatGrid verwendet.

Schritt 1: Navigieren Sie im Bereich **Installationsoptionen** zum Abschnitt **Konfiguration** ->

Zertifizierungsstellen. Klicken Sie auf die Schaltfläche **Zertifizierungsstelle hinzufügen**, wie im Bild gezeigt.

The screenshot shows the 'Certificate Authorities' page in the fireAMP Private Cloud Administration Portal. The page title is 'Certificate Authorities'. A button labeled 'Add Certificate Authority' is highlighted with a red rectangle. Below the button, a light blue message box states: 'No certificate authorities have been uploaded to this device.' A green 'Next >' button is located at the bottom right. On the left side, there is a navigation menu with sections 'Installation Options' and 'Configuration'. Under 'Installation Options', items include 'Install or Restore', 'License', 'Welcome', 'Deployment Mode', 'FireAMP Console Account', and 'Hardware Requirements'. Under 'Configuration', items include 'Network', 'Date and Time', 'Certificate Authorities', 'Upstream Proxy Server', 'Cisco Cloud', 'Email', 'Notifications', 'Backups', 'SSH', 'Syslog', and 'Updates'. All items in the menu have a checkmark icon to their right. The top navigation bar includes 'Support', 'Help', and 'Logout' links.

Schritt 2: Klicken Sie auf **Zertifikatsstamm hinzufügen**, wie im Bild gezeigt, um das Zertifikat hochzuladen. Alle aufgeführten Anforderungen müssen erfüllt sein, damit das Zertifikat für die Virtual Private Cloud akzeptiert werden kann.

Hinweis: Während des Aktualisierungsvorgangs müssen Sie das **Stammzertifikat** hinzufügen, das zum Signieren des **Authentifizierungsdienstzertifikats** verwendet wird, wie im nächsten Abschnitt erläutert.

Configuration Operations Status Integrations Support

Add Certificate Authority

● Certificate Root (PEM .crt)

- Certificate file has been uploaded.
- Certificate is in a readable format.
- Certificate start and end dates are valid.
- Certificate end date is later than 20 months from today.
- Certificate file only contains one certificate.

certnew.cer + Add Certificate Root

Cancel Upload

Schritt 3: Wenn das Zertifikat aktualisiert ist, klicken Sie auf die Schaltfläche **Hochladen**, wie im Bild gezeigt, um das Zertifikat hochzuladen.

fireAMP™ Private Cloud Administration Portal

Support Help Logout

Configuration Operations Status Integrations Support

Add Certificate Authority

● Certificate Root (PEM .crt)

- Certificate file has been uploaded.
- Certificate is in a readable format.
- Certificate start and end dates are valid.
- Certificate end date is later than 20 months from today.
- Certificate file only contains one certificate.

certnew.cer + Add Certificate Root

Cancel Upload

Wenn Sie eine untergeordnete Zertifizierungsstelle zum Signieren von Service-Zertifikaten verwenden, laden Sie diese ebenfalls in diesen Abschnitt hoch.

Vorsicht: Auch wenn Sie ein selbstsigniertes Zertifikat für den Authentifizierungsdienst

generieren, stellen Sie sicher, dass es im Abschnitt Zertifizierungsstelle hochgeladen wird, bevor Sie mit den nächsten Schritten fortfahren.

6. Authentifizierungsdienst

Die zweite Komponente, die in Version 3.0.1 hinzugefügt und nicht aus der Sicherung importiert wird, ist die **Authentifizierung** im Abschnitt Dienste.

Der **Authentifizierungsdienst** wird in zukünftigen Versionen der Private Cloud verwendet, um Benutzerauthentifizierungsanforderungen zu bearbeiten. Sie wird in Version 3.0.1 zur zukünftigen Kompatibilität hinzugefügt.

Schritt 1: Navigieren Sie im Bereich **Installationsoptionen** zum Abschnitt **Services** -> **Authentifizierung**. Geben Sie einen eindeutigen **Authentifizierungs-Hostnamen** ein, der im Hostnamenabschnitt angegebene DNS-Eintrag muss auf dem DNS-Server korrekt konfiguriert sein und verweist auf die IP-Adresse der Virtual Private Cloud Console.

The screenshot shows the FireAMP Private Cloud Administration Portal interface. The top navigation bar includes the FireAMP logo, the text 'Private Cloud Administration Portal', and links for Support, Help, and Logout. Below this is a secondary navigation bar with tabs for Configuration, Operations, Status, Integrations, and Support. The left sidebar is divided into three sections: 'Installation Options' (with a note that only the License section can be altered after installation), 'Configuration' (listing various system settings like Network, Date and Time, Certificate Authorities, etc.), and 'Services' (listing various services like Authentication, FireAMP Console, Disposition Server, etc.). The main content area is titled 'Authentication Configuration'. It features a red-bordered box around the 'Authentication Hostname' section, which includes a text input field containing 'authentication.amptest.pgruszczy.com' and a checked 'Validate DNS Name' checkbox. Below this is the 'Authentication Certificate' section, which contains a blue message box stating 'No certificate has been provided for this service.' and a 'Replace Certificate' button. At the bottom right of the main content area, there is a green 'Next >' button.

Schritt 2: Wenn der Hostname angegeben und ordnungsgemäß auflösbar ist, klicken Sie auf die Schaltfläche **Zertifikat ersetzen**, wie im Bild gezeigt.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Authentication Configuration

Authentication Hostname

HELP

authentication.amptest.pgruszczy.com

Validate DNS Name

Authentication Certificate

Replace Certificate

No certificate has been provided for this service.

Next >

Hinweis: Wenn Sie Hilfe bei der Generierung von Zertifikaten benötigen, lesen Sie den folgenden Artikel: [Generieren und Hinzufügen von Zertifikaten, die für die Installation von AMP VPC 3.x ab erforderlich sind](#), um weitere Informationen zu Hardwareanforderungen zu erhalten.

Schritt 3: Klicken Sie auf die Schaltfläche **Zertifikat auswählen**, um das Zertifikat des Authentifizierungsdiensts hochzuladen, wie im Bild gezeigt.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management ✓
- > Center ✓

Other

- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname

HELP

authentication.amptest.pgruszc.com

Validate DNS Name

Authentication Certificate

Undo

Replace Certificate

● Certificate (PEM .crt)

- Certificate file has been uploaded.
- Certificate is in a readable format.
- Certificate start and end dates are valid.
- Certificate contains a subject.
- Certificate contains a common name.
- Certificate contains a public key matching the uploaded key.
- Certificate matches hostname.
- Certificate is signed by a trusted root authority.

🔑 Key (PEM .key)

- Key file has been uploaded.
- Key contains a supported key type.
- Key contains public key material.
- Key contains private key material.
- Key contains a public key matching the uploaded certificate.

private.key

+ Choose Key

authentication_serv

+ Choose Certificate

Next >

Schritt 4: Als Nächstes laden Sie die private Schlüsseldatei für das Zertifikat hoch. Klicken Sie zum Hinzufügen auf die Schaltfläche **Schlüssel auswählen**.

Installation Options
Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Review and Install

[▶ Start Installation](#)

Authentication Configuration

Authentication Hostname HELP

authentication.amptest.pgruszczy.com Validate DNS Name

Authentication Certificate Undo Replace Certificate

● Certificate (PEM .crt)	🔍 Key (PEM .key)
<input checked="" type="checkbox"/> Certificate file has been uploaded.	<input checked="" type="checkbox"/> Key file has been uploaded.
<input checked="" type="checkbox"/> Certificate is in a readable format.	<input checked="" type="checkbox"/> Key contains a supported key type.
<input checked="" type="checkbox"/> Certificate start and end dates are valid.	<input checked="" type="checkbox"/> Key contains public key material.
<input checked="" type="checkbox"/> Certificate contains a subject.	<input checked="" type="checkbox"/> Key contains private key material.
<input checked="" type="checkbox"/> Certificate contains a common name.	<input checked="" type="checkbox"/> Key contains a public key matching the uploaded certificate.
<input checked="" type="checkbox"/> Certificate contains a public key matching the uploaded key.	
<input checked="" type="checkbox"/> Certificate matches hostname.	
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	

private.key + Choose Key

authentication_serv + Choose Certificate

[Next >](#)

Schritt 5: Sie müssen sicherstellen, dass alle Anforderungen erfüllt sind, bevor Sie mit dem nächsten Schritt fortfahren können. Hervorgehobene Anforderungen sind erfüllt, wenn das Stammzertifikat, das zum Signieren des **Authentifizierungsdiensts** verwendet wird, korrekt im Speicher der **Zertifizierungsstellen** platziert wird.

Vorsicht: Sie können die Hostnamen für alle anderen Dienste nur zu diesem Zeitpunkt ändern. Nach Abschluss der Installation kann der Hostname für die Dienste nicht mehr geändert werden. Später können Sie nur Zertifikate ändern. Sie müssen sicherstellen, dass Sie das Risiko einer solchen Operation verstehen. Wenn Sie die Hostnamen der von den Connectors oder AMP für Netzwerkgeräte verwendeten Services ändern, können diese Probleme mit der Cloud-Kommunikation haben, sobald das Upgrade abgeschlossen ist.

7. Installation

Schritt 1: Sobald alle Abschnitte abgeschlossen und als gültig gekennzeichnet sind, beginnen Sie

mit der Installation. Navigieren Sie zum Abschnitt **Prüfen und Installieren**, und klicken Sie auf **Installation starten**, wie im Bild gezeigt.

fireAMP™ Private Cloud Administration Portal

Support ? Help Logout

Configuration Operations Status Integrations Support

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Review and Install

[▶ Start Installation](#)

Review and Install

Review the following information and, once you are satisfied with your configuration settings, begin the installation. Note that the configuration shown below cannot be altered after installation.

Restore Ready

Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.

Installation Type [Edit](#)

Cloud Proxy

- Requires an Internet connection and communication with FireAMP Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

FireAMP Console Account [Edit](#)

Name	Piotr Gruszczynski
Email Address	pgruszcz@cisco.com
Business Name	Cisco - pgruszcz

Recovery

When restoring from a backup, a recovery image is not required.

[▶ Start Installation](#)

Schritt 2: Das Administratorportal zeigt Ihnen den aktuellen Status, das Startdatum und die Protokolle. Wenn Fehler oder Probleme auftreten, die Support-Aufmerksamkeit erfordern, sammeln Sie die Protokolle, indem Sie auf die Schaltfläche **Ausgabe herunterladen** klicken, wie im Bild gezeigt, und fügen Sie sie dem TAC-Fall hinzu.

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
▶ Running	Fri Apr 26 2019 13:54:03 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 1 minute, 14 seconds ago	⌚ Please wait...	⌚ Please wait...

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2019-04-26T11:55:10+00:00] DEBUG: Current content's checksum:
[2019-04-26T11:55:10+00:00] DEBUG: Rendered content's checksum: 1c2c8f5383551c7c76409b59eec5833923094af0c69d8d967a552c3d47f2a609
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] updated content
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] owner changed to 0
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] group changed to 0
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] mode changed to 644
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] not queuing delayed action run on execute[reset_policy_network_items] (delayed), as it's already been queued
[2019-04-26T11:55:10+00:00] INFO: Processing template[/opt/fire/amp/portal/config/virtual/config_items.chef.yml] action create (fireamp-portal::config_chef line 70)
[2019-04-26T11:55:10+00:00] DEBUG: Current content's checksum:
[2019-04-26T11:55:10+00:00] DEBUG: Rendered content's checksum: 06c8c02083c15cab1270ec1e3e62c593d5627a387793cce53ae290817d555b1c
```

Download Output

Schritt 3: Wenn die Installation erfolgreich ist, müssen Sie das Gerät neu starten, um den Vorgang abzuschließen. Klicken Sie auf die Schaltfläche **Neustart**, um den Neustart durchzuführen, wie im Bild gezeigt.

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
✓ Successful	Fri Apr 26 2019 13:54:03 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 10 minutes, 23 seconds ago	Fri Apr 26 2019 14:03:57 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 0 minute, 28 seconds ago	0 day, 0 hour, 9 minutes, 54 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
un (/opt/fire/chef/cookbooks/daemontools/providers/service.rb line 148)
[2019-04-26T12:03:39+00:00] INFO: execute[/opt/fire/embedded/bin/svc -t /service/fireamp-haproxy] ran successfully
[2019-04-26T12:03:39+00:00] INFO: template[/opt/fire/amp/portal/db/migrate/20190426120103_update_license_summary_2019
0426120051.rb] sending run action to execute[run_migrate_license_summary] (delayed)
[2019-04-26T12:03:39+00:00] INFO: Processing execute[run_migrate_license_summary] action run (fireamp-onprem::license
line 142)
[2019-04-26T12:03:57+00:00] INFO: execute[run_migrate_license_summary] ran successfully
[2019-04-26T12:03:57+00:00] INFO: Chef Run complete in 186.283958188 seconds
[2019-04-26T12:03:57+00:00] INFO: Running report handlers
[2019-04-26T12:03:57+00:00] INFO: Report handlers complete
Sending system notification (this may take some time).
Registration against the FireAMP Disposition Server has previously succeeded.
```

```
=====
Installation has finished successfully! Please reboot!
=====
```

Download Output

Schritt 4: Nach dem Neustart können Sie sich beim **Administrator Portal** und **Console Portal** anmelden. Die Aktualisierung ist abgeschlossen.

8. Prüfungen nach dem Upgrade

Nachdem das Gerät neu gestartet wurde, vergewissern Sie sich, dass die Wiederherstellung erfolgreich abgeschlossen wurde:

Schritt 1: Überprüfen Sie, ob Anschlüsse mit der neu installierten virtuellen Appliance 3.0.1 kommunizieren können.

Schritt 2: Stellen Sie sicher, dass Ereignisse, Device Trajectory und Computer-Objekte ordnungsgemäß wiederhergestellt und im Konsolenportal angezeigt werden.

Schritt 3: Wenn Sie AMP für Netzwerkintegrationen wie FMC, ESA, WSA haben, stellen Sie sicher, dass diese mit dem File Disposition-Server kommunizieren können.

Schritt 4: Suchen Sie nach Inhalt-/Software-Updates (Operations -> Update Device), und fahren Sie mit der Installation dieser Updates fort.

Es wird dringend empfohlen, Tests durchzuführen, um ein erfolgreiches Upgrade sicherzustellen.

Änderungen bei Virtual Private Cloud 3.0.1

1. Windows Connector Version 6.1.7

Private Cloud 3.0.1 wird mit Unterstützung für 6.1.7 Windows Connector ausgeliefert. Die entsprechende Dokumentation finden Sie unter dem Link: [Versionshinweise für 6.1.7](#)

Vorsicht: Wenn Sie Änderungen an Zertifikaten vorgenommen haben, stellen Sie sicher, dass vor einem Upgrade oder einer Installation auf Version 6.1.7 von Windows Connector Zertifikate, die für Private Cloud-Services verwendet werden, auf dem Endpunkt selbst vertrauenswürdig sind. Vertrauen muss auf Computerebene und nicht auf Benutzerebene stattfinden. Wenn diese Bedingung nicht erfüllt wird, vertrauen Connectors nicht dem Zertifikat der Private Cloud, das die Verbindung zum Netzwerk trennt.

2. Zertifizierungsstellen und Authentifizierungsdienst

Die Änderungen wurden im Benutzerhandbuch für 3.0 ausführlich beschrieben: [Private Cloud-Benutzerhandbuch](#).

Zertifizierungsstellen ermöglichen das Verwalten von Stammzertifikaten für Ihre Dienste, wenn Sie eine benutzerdefinierte Zertifizierungsstelle verwenden möchten. Sie können Ihr Stammzertifikat bei Bedarf herunterladen oder löschen.

Der Authentifizierungsdienst wird in zukünftigen Versionen der Private Cloud verwendet, um Benutzerauthentifizierungsanforderungen zu bearbeiten. Sie wird in Version 3.0.1 zur zukünftigen Kompatibilität hinzugefügt.