

Procedura di aggiornamento di FireAMP Private Cloud 3.0.1

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Requisiti hardware](#)

[Componenti usati](#)

[Processo di aggiornamento](#)

[1. Download e installazione degli aggiornamenti](#)

[2. Raccolta e chiusura di backup](#)

[3. Installazione della nuova versione](#)

[4. Ripristino backup](#)

[5. Autorità di certificazione](#)

[6. Servizio di autenticazione](#)

[7. Installazione](#)

[8. Controlli successivi all'aggiornamento](#)

[Modifiche in Virtual Private Cloud 3.0.1](#)

[1. Windows Connector versione 6.1.7](#)

[2. Servizio Autorità di certificazione e autenticazione](#)

Introduzione

In questo documento viene descritto come aggiornare FireAMP Private Cloud (vPC) versione 2.4.4 alla versione 3.0.1. La procedura di aggiornamento richiede una nuova istanza della macchina virtuale per la versione 3.0.1.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Installazione di un modello di Open Virtual Appliance (OVA) in VMWare ESXi
- Conoscenze base del funzionamento e del funzionamento di Virtual AMP Cloud

Requisiti hardware

Di seguito sono riportati i requisiti hardware minimi per FireAMP Private Cloud:

- vSphere ESX 5 o superiore

- 8 CPU
- 64 GB RAM
- 1 TB di spazio libero su disco nell'archivio dati VMWare
- Tipo di unità: SSD necessaria
- Tipo RAID: Un gruppo RAID 10 (striping dei mirror)
- Dimensioni minime archivio dati VMware: 1 TB
- Numero minimo di letture casuali dell'archivio dati per il gruppo RAID 10 (4K): 60.000 IOPS
- Numero minimo di scritture casuali dell'archivio dati per il gruppo RAID 10 (4K): 30.000 IOPS

Attenzione: Private Cloud OVA crea le partizioni di unità, quindi non è necessario specificarle in VMWare.

Nota: Per ulteriori informazioni sui requisiti hardware, consultare la [guida per l'utente di FireAMP Private Cloud](#).

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

- FireAMP Private Cloud 2.4.4
- FireAMP Private Cloud 3.0.1
- VMware ESXi 5.0 o versione successiva

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Processo di aggiornamento

In questa sezione vengono fornite istruzioni dettagliate su come raccogliere il backup dalla versione FireAMP Private Cloud 2.4.4 e su come ripristinarlo correttamente nella versione FireAMP Private Cloud 3.0.1.

Attenzione: Il processo di aggiornamento può introdurre tempi di inattività nell'ambiente. I connettori (incluso AMP for Networks connected to your Virtual Private Cloud) che utilizzano il cloud privato possono perdere la connettività al cloud virtuale e possono avere funzionalità compromesse a causa di ciò.

1. Download e installazione degli aggiornamenti

Verificare che FireAMP Virtual Private Cloud 2.4.4 sia aggiornato.

Passaggio 1. Passare a **Operations** -> **Update Device** in Administrator Portal.

Passaggio 2. Fare clic sul pulsante **Check/Download Updates** (Controlla/Scarica aggiornamenti), come mostrato nell'immagine, per essere certi che FireAMP Virtual Private Cloud, da cui ha luogo la raccolta di backup, sia aggiornato (per contenuti e 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.

Passaggio 3. Dopo l'installazione degli aggiornamenti software e del contenuto, la pagina di aggiornamento mostra le informazioni sull'aggiornamento del dispositivo, come mostrato nell'immagine.

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

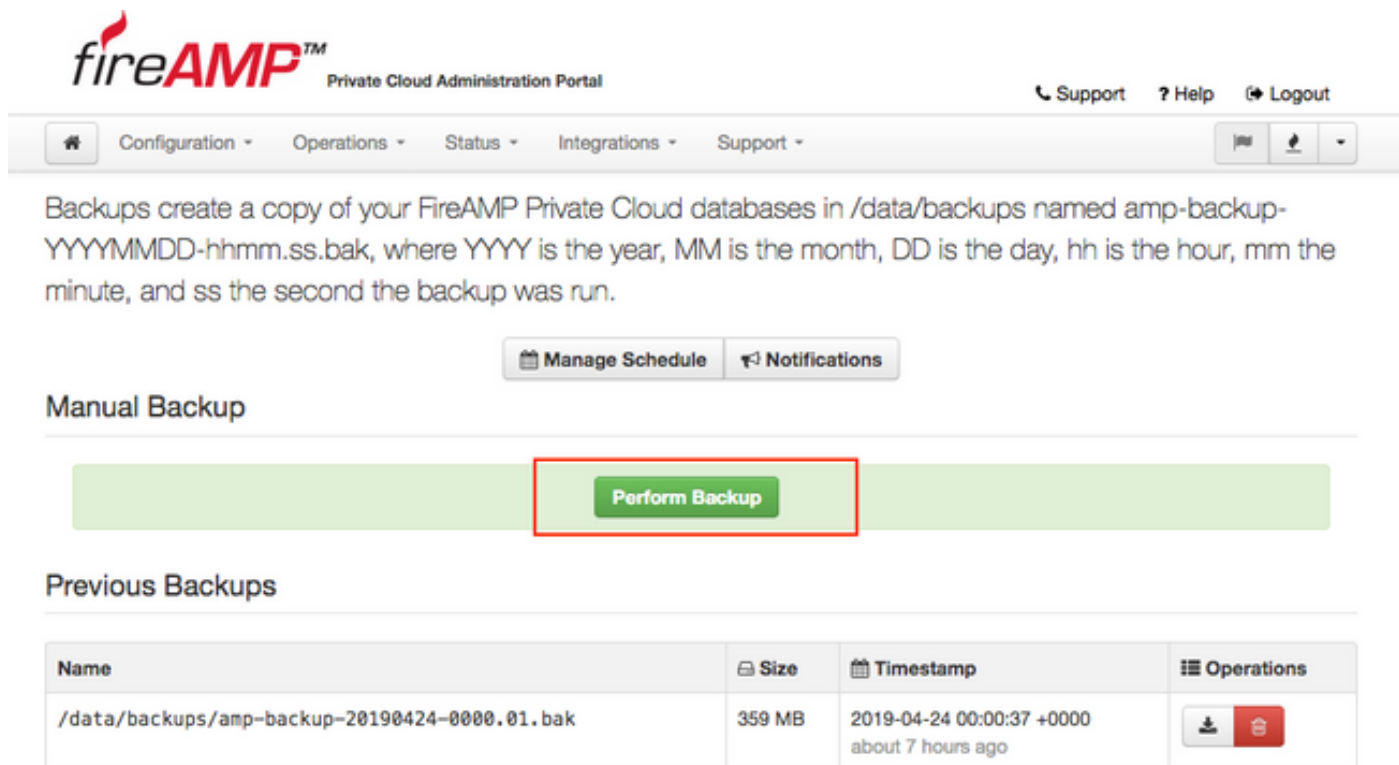
Checked 35 minutes ago; software is up to date.

2. Raccolta e chiusura di backup

Passaggio 1. Passare a **Operazioni** -> **Backup**.

Passaggio 2. Nella sezione Backup manuale, fare clic su **Esegui backup** pulsante. La procedura

avvia la creazione di un backup.



fireAMP™ Private Cloud Administration Portal

Support ? Help Logout

Configuration - Operations - Status - Integrations - Support -



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

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	 

Passaggio 3. Al termine del processo, viene visualizzata la notifica di esito positivo, come illustrato nell'immagine.

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-20190424-0000.01.bak	359 MB	2019-04-24 00:00:37 +0000 about 8 hours ago	 

Passaggio 4. Fare clic su  pulsante. Verificare che il backup sia stato scaricato correttamente e salvato in un luogo sicuro.

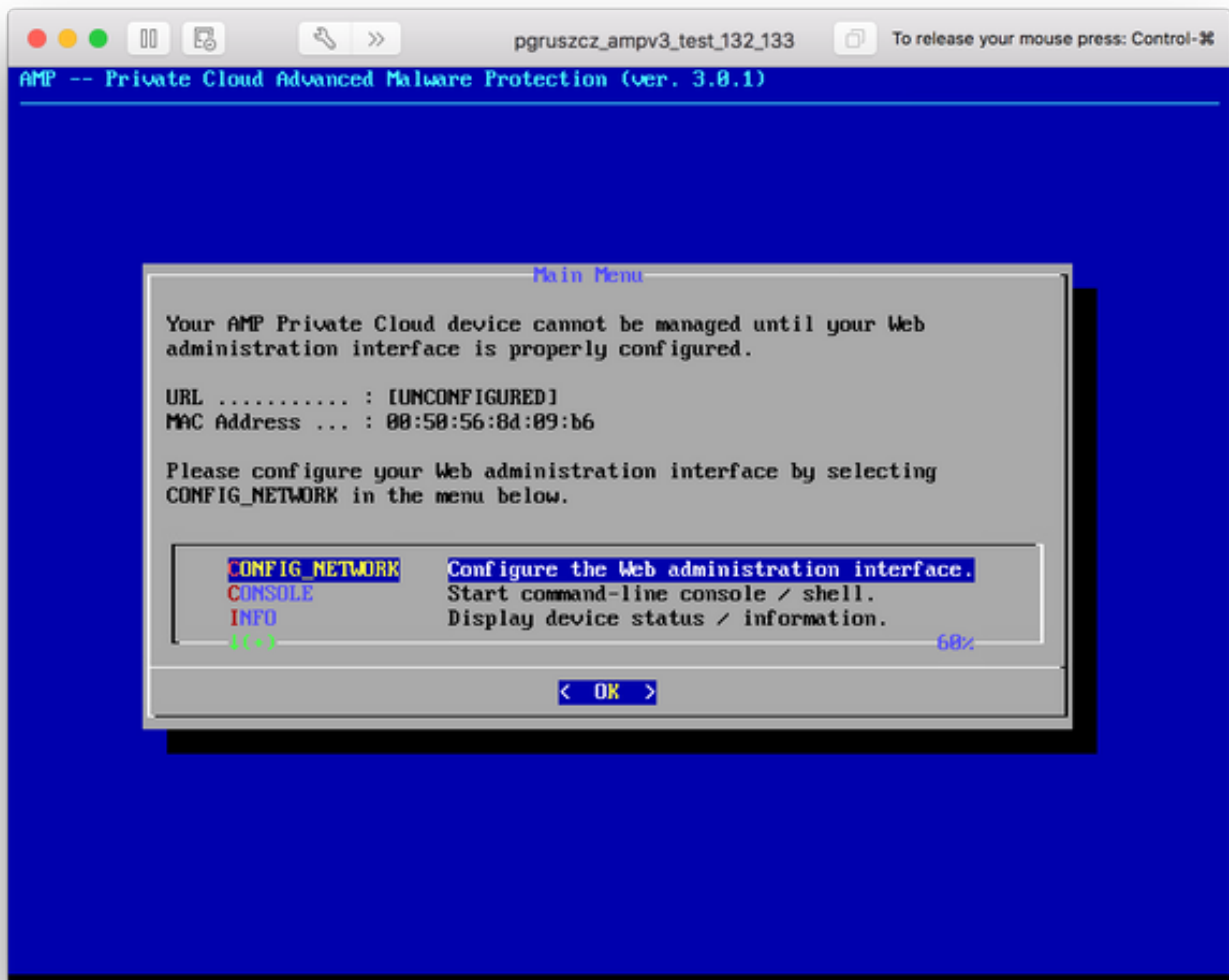
3. Installazione della nuova versione

In questa sezione si presume che la macchina virtuale per il cloud privato virtuale FireAMP 3.0.1 sia già distribuita. Procedura di installazione per quanto riguarda di Virtual Machine per 3.0.1 OVA su VMWare ESXi può essere trovato sotto il collegamento: [Distribuire un file OVA su un server ESX.](#)

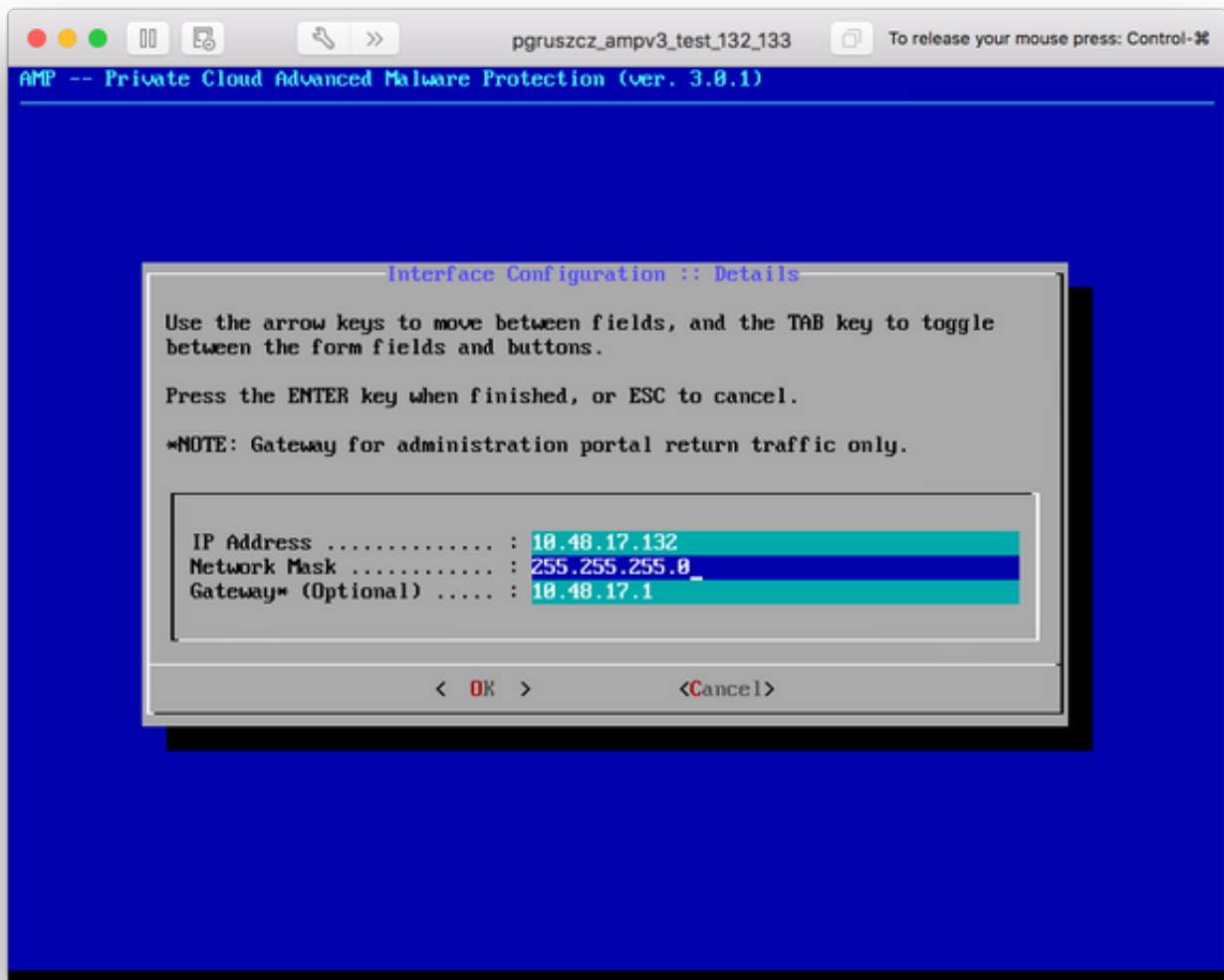
Nota: La procedura descritta nell'articolo utilizza esattamente gli stessi nomi host e indirizzi IP per FireAMP Virtual Private Cloud 2.4.4 e 3.0.1. Quando si segue questa guida, è necessario arrestare FireAMP Virtual Private Cloud 2.4.4 dopo la raccolta dei dati di backup.

Passaggio 1. Aprire il terminale della console per l'istanza della macchina virtuale appena creata con la versione 3.0.1 installata. È possibile spostarsi tra i tasti **Tab**, **Enter** e **freccia**.

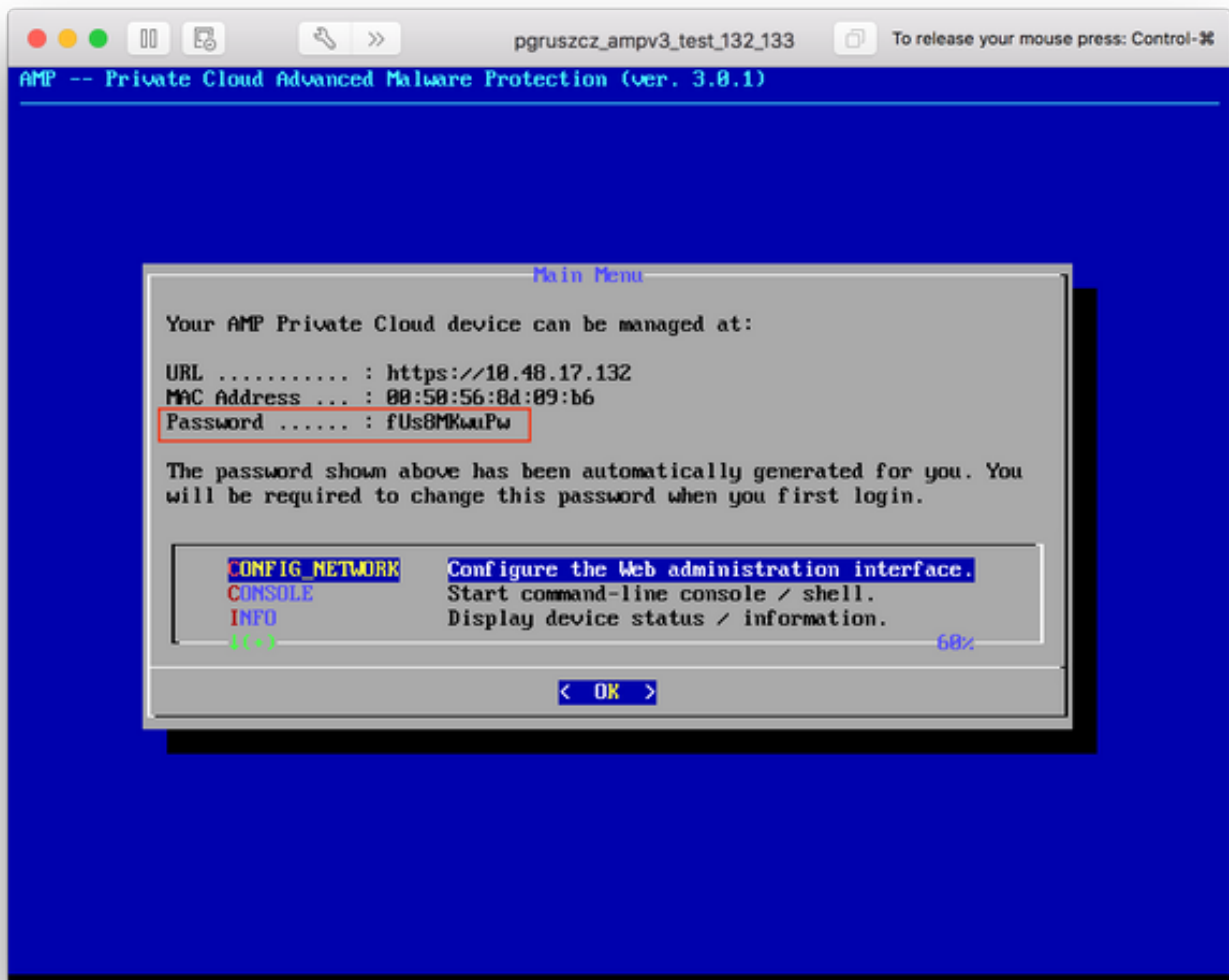
Passaggio 2. Passare a **CONFIG_NETWORK** e fare clic sul tasto **Enter** sulla tastiera per iniziare la configurazione dell'indirizzo IP di gestione per il cloud privato FireAMP. Se non si desidera utilizzare DHCP, selezionare **No** e premere **Invio**.



Passaggio 3. Inserire l'indirizzo IP, la maschera di rete e il gateway predefinito. Passare a OK, come mostrato nell'immagine. Premere Invio.



Passaggio 4. La modifica della configurazione della rete richiede il riavvio dell'interfaccia. Dopo il riavvio, viene nuovamente visualizzato il menu della console principale, come mostrato nell'immagine. Questa volta viene visualizzato un indirizzo IP sulla riga dell'URL. Si noti inoltre che viene visualizzata la **password** iniziale. Si tratta di una password temporanea (in seguito denominata **password iniziale**) utilizzata nell'installazione basata sul Web.



Passaggio 5. Aprire un browser Web e individuare l'indirizzo IP di gestione dell'accessorio. Si riceve un errore di certificato poiché il cloud privato FireAMP genera inizialmente il proprio certificato HTTPS. Configurare il browser per considerare temporaneamente attendibile il certificato autofirmato del cloud privato FireAMP.

Passaggio 6. Viene visualizzata una schermata per immettere una password, come mostrato nell'immagine. Utilizzare la **password iniziale** della console. Fare clic su **Login**.



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

Passaggio 7. Dopo aver eseguito correttamente l'accesso, è necessario modificare la password. Utilizzare la **password iniziale** della console nel campo **Vecchia password**. Utilizzare la nuova password due volte nei campi **Nuova password**. Fare clic su **Cambia password**.



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. Ripristino backup

Passaggio 1. La pagina di benvenuto del portale di amministrazione presenta due modalità di installazione di FireAMP Virtual Cloud 3.0.1, come mostrato nell'immagine.

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 >

Passaggio 2. È possibile scegliere uno dei tre metodi per caricare il file di backup nell'istanza di FireAMP Virtual Private Cloud appena creata:

Locale: ripristina la configurazione da un file di backup già presentato sul dispositivo (è necessario salvare il file sull'accessorio tramite SFTP o SCP). Una volta avviato il processo di ripristino, i file vengono estratti nella directory corretta. Per questo motivo, è consigliabile utilizzare la directory /data.

Remoto - Ripristina da un file in un server HTTP accessibile in remoto.

Upload - Ripristina dal file caricato dal browser. Funziona solo se le dimensioni del file di backup sono inferiori a 20 MB.

In questo esempio è stata scelta l'opzione remote.

Nota: È necessario consentire la corretta connettività per il server HTTP. I file di backup devono essere accessibili dal punto di vista del cloud privato.

Fare clic sul pulsante **Start** per procedere con il ripristino, come mostrato nell'immagine.

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 >

Passaggio 3. La procedura di ripristino da un backup sostituisce la configurazione corrente. Le chiavi host SSH e la password del portale di amministrazione del dispositivo vengono sostituite. È possibile esaminare parti della configurazione per quanto riguarda l'installazione.

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 >

Passaggio 4. Dopo aver completato una copia del file di backup, la pagina di ripristino presenta un messaggio popup come mostrato nell'immagine. Fare clic sul pulsante **Riconfigura portale di amministrazione adesso** per completare la procedura di ripristino.

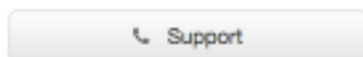
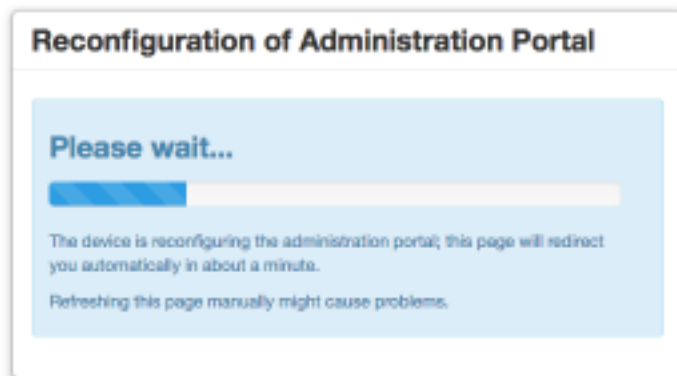


Reconfiguration of Administration Portal

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

Reconfigure Administration Portal Now

Support



Passaggio 5. Al termine della riconfigurazione, viene visualizzata nuovamente la pagina del portale di amministrazione, come illustrato nell'immagine. Da ora in poi, per effettuare il login è necessario usare la password del backup 2.4.4 FireAMP Virtual Private Cloud.

Nell'immagine è illustrata la maggior parte del lavoro già svolto per la corretta installazione (segni di spunta). È previsto poiché il backup ripristina la configurazione da FireAMP Virtual Private Cloud 2.4.4.

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

/data

Start >

5. Autorità di certificazione

La versione 3.0.1 di FireAMP Virtual Private Cloud introduce nuove funzionalità e comportamenti in termini di funzionamento del sistema. Per poter iniziare l'installazione, è necessario configurarli e completarli.

Il primo componente nuovo e non presente nella versione precedente è **Autorità di certificazione**.

La pagina **Autorità di certificazione** consente di gestire i certificati radice per i servizi se si desidera utilizzare un'autorità di certificazione personalizzata. Se necessario, è possibile scaricare o eliminare il certificato radice.

Nota: L'archivio attendibile Autorità di certificazione viene utilizzato solo per i servizi del cloud virtuale (per compilare e convalidare la catena di certificati appropriata). Non viene utilizzato per varie integrazioni di vPC, come ThreatGrid.

Passaggio 1. Passare alla sezione **Configurazione** -> **Autorità di certificazione** nel pannello **Opzioni di installazione**. Fare clic sul pulsante **Aggiungi autorità di certificazione**, come mostrato

nell'immagine.

The screenshot shows the fireAMP Private Cloud Administration Portal interface. At the top left is the fireAMP logo and the text "Private Cloud Administration Portal". On the top right, there are links for "Support", "Help", and "Logout". Below the header is a navigation bar with tabs for "Configuration", "Operations", "Status", "Integrations", and "Support". A sidebar on the left lists "Installation Options" and "Configuration" sections, each with a list of sub-items and checkmarks. The main content area is titled "Certificate Authorities" and features a button labeled "Add Certificate Authority" which is highlighted with a red rectangle. Below the button is a light blue message box stating "No certificate authorities have been uploaded to this device." and a green "Next >" button.

Passaggio 2. Per caricare il certificato, fare clic su **Add Certificate Root** (Aggiungi radice certificato), come mostrato nell'immagine. Affinché il cloud privato virtuale accetti il certificato, è necessario soddisfare tutti i requisiti elencati.

Nota: Durante la procedura di aggiornamento, è necessario aggiungere il **certificato radice** utilizzato per firmare il certificato del servizio di **autenticazione**, descritto nella sezione successiva.

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 ✓

Add Certificate Authority

● Certificate Root (PEM .crt)

<input checked="" type="checkbox"/>	Certificate file has been uploaded.
<input checked="" type="checkbox"/>	Certificate is in a readable format.
<input checked="" type="checkbox"/>	Certificate start and end dates are valid.
<input checked="" type="checkbox"/>	Certificate end date is later than 20 months from today.
<input checked="" type="checkbox"/>	Certificate file only contains one certificate.

certnew.cer + Add Certificate Root

Cancel Upload

Passaggio 3. Dopo aver aggiornato il certificato, fare clic sul pulsante **Upload** (Carica), come mostrato nell'immagine, per caricarlo.

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 ✓

Add Certificate Authority

● Certificate Root (PEM .crt)

<input checked="" type="checkbox"/>	Certificate file has been uploaded.
<input checked="" type="checkbox"/>	Certificate is in a readable format.
<input checked="" type="checkbox"/>	Certificate start and end dates are valid.
<input checked="" type="checkbox"/>	Certificate end date is later than 20 months from today.
<input checked="" type="checkbox"/>	Certificate file only contains one certificate.

certnew.cer + Add Certificate Root

Cancel **Upload**

Se si utilizza un'autorità di certificazione subordinata per firmare i certificati di servizio, caricarli anche in questa sezione.

Attenzione: Anche se si genera un certificato autofirmato per il servizio di autenticazione,

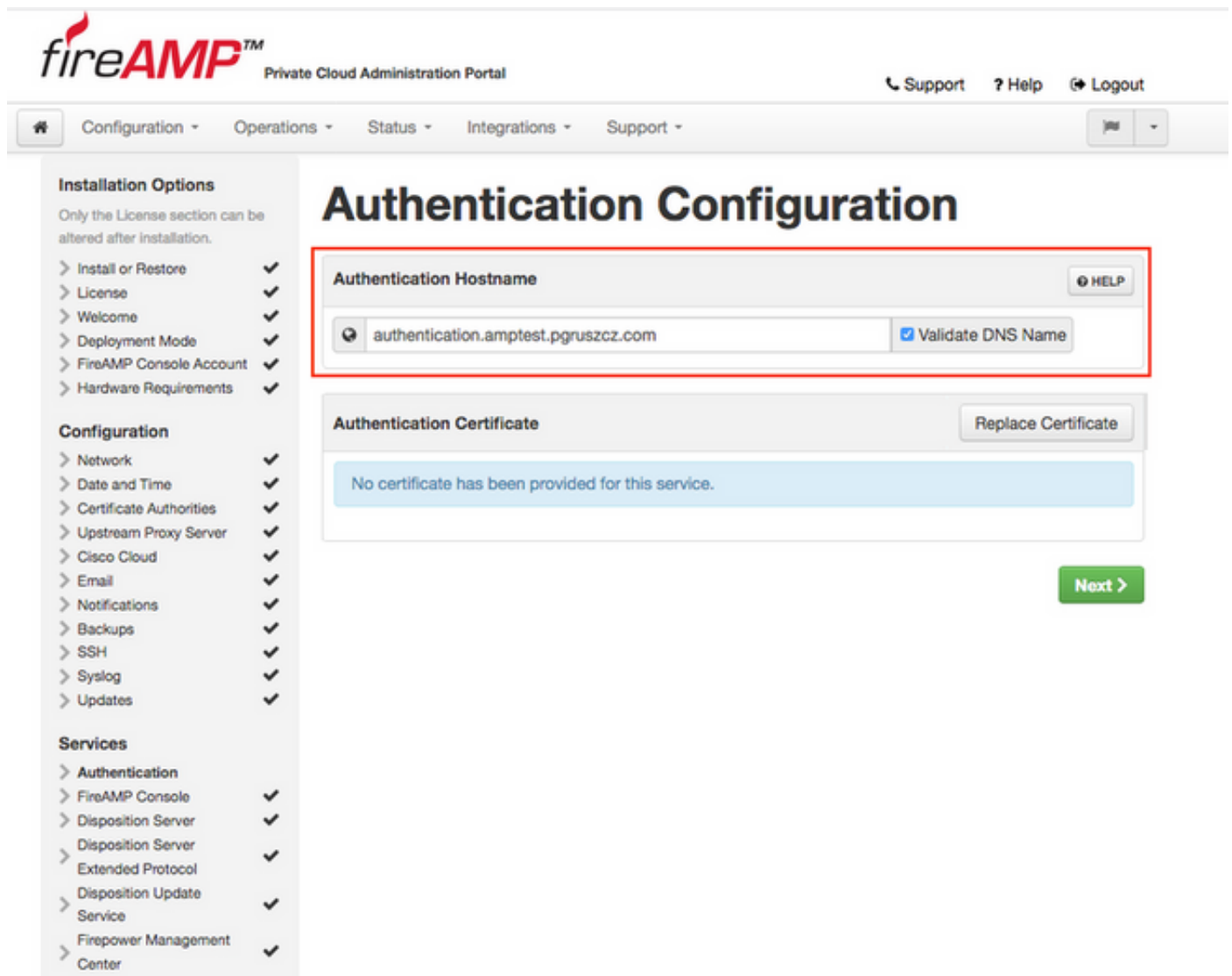
assicurarsi che venga caricato nella sezione Autorità di certificazione prima di procedere con i passaggi successivi.

6. Servizio di autenticazione

Il secondo componente aggiunto nella versione 3.0.1 e non importato dal backup è **Authentication** nella sezione Services.

Nelle versioni future di Cloud privato verrà utilizzato il servizio di **autenticazione** per gestire le richieste di autenticazione degli utenti. È stato aggiunto nella versione 3.0.1 per una futura compatibilità.

Passaggio 1. Passare alla sezione **Servizi -> Autenticazione** nel pannello **Opzioni di installazione**. Immettere un **nome host di autenticazione** univoco. La voce DNS specificata nella sezione hostname deve essere configurata correttamente nel server DNS e puntare all'indirizzo IP dell'interfaccia della console Virtual Private Cloud.



The screenshot displays 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 main content area is titled "Authentication Configuration". On the left, a sidebar menu lists "Installation Options" (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), and "Services" (Authentication, FireAMP Console, Disposition Server, Extended Protocol, Disposition Update, Service, Firepower Management Center). The "Authentication Hostname" section is highlighted with a red box and contains a text input field with the value "authentication.amptest.pgruszczy.com", a "Validate DNS Name" checkbox, and a "HELP" button. Below this is the "Authentication Certificate" section, which includes a "Replace Certificate" button and a message: "No certificate has been provided for this service." A green "Next >" button is located at the bottom right of the main content area.

Passaggio 2. Dopo aver specificato il nome host e averlo risolto correttamente, fare clic sul pulsante **Sostituisci certificato**, come mostrato nell'immagine.

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

Validate DNS Name

Authentication Certificate Replace Certificate

No certificate has been provided for this service.

Next >

Nota: Per informazioni sulla generazione dei certificati, visitare l'articolo: [Come generare e aggiungere i certificati necessari per l'installazione di AMP VPC 3.x in avanti](#) per ulteriori informazioni sui requisiti hardware.

Passaggio 3. Fare clic sul pulsante **Scegli certificato** per caricare il certificato del servizio di autenticazione, come mostrato nell'immagine.

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 >

Passaggio 4. Il passaggio successivo consiste nel caricare il file della chiave privata per il certificato. Per aggiungerlo, fare clic sul pulsante **Scegli tasto**.

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)	🔍 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 >](#)

Passaggio 5. Prima di procedere, è necessario verificare che tutti i requisiti siano soddisfatti. I requisiti evidenziati vengono soddisfatti se il certificato radice utilizzato per firmare il servizio di **autenticazione** viene posizionato correttamente nell'archivio **Autorità di certificazione**.

Attenzione: È possibile modificare i nomi host per tutti gli altri servizi solo in questa fase. Al termine dell'installazione, non sarà possibile modificare il nome host per i servizi. In seguito sarà possibile modificare solo i certificati. Devi accertarti di comprendere il rischio di tale operazione. Se si modificano i nomi host dei servizi utilizzati dai connettori o da AMP per i dispositivi di rete, possono verificarsi problemi di comunicazione con il cloud al termine dell'aggiornamento.

7. Installazione

Passaggio 1. Dopo aver completato tutte le sezioni e averle contrassegnate come valide, si avvia l'installazione. Passare alla sezione **Revisione e installazione** e fare clic sul pulsante **Avvia**

installazione, come mostrato nell'immagine.

The screenshot shows the fireAMP Private Cloud Administration Portal. The main heading is "Review and Install". Below the heading, there is a green box with the text "Restore Ready" and a message: "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." The page is divided into several sections: "Installation Type" (Cloud Proxy), "FireAMP Console Account" (a table with fields for Name, Email Address, and Business Name), and "Recovery". A "Start Installation" button is located at the bottom of the page, highlighted with a red box.

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@ciseco.com
Business Name	Cisco - pgruszcz

Recovery

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

Start Installation

Passaggio 2. Il portale per gli amministratori visualizza lo stato corrente, la data di inizio e i registri. In caso di errori o problemi che richiedono l'attenzione del supporto, raccogliere i registri facendo clic sul pulsante **Scarica output**, come mostrato nell'immagine, e allegarli alla richiesta TAC.

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

Passaggio 3. Quando l'installazione viene completata correttamente, è necessario riavviare il dispositivo per completare il processo. Fare clic sul pulsante **Reboot** (Riavvia) per procedere con la procedura di riavvio, come mostrato nell'immagine.

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

Passaggio 4. Dopo la procedura di riavvio, è possibile accedere al portale **dell'amministratore** e al portale della **console**. La procedura di aggiornamento è terminata.

8. Controlli successivi all'aggiornamento

Una volta riavviato il dispositivo, assicurarsi che il ripristino sia stato completato correttamente:

Passaggio 1. Verificare se i connettori sono in grado di comunicare con l'appliance virtuale 3.0.1 appena installata.

Passaggio 2. Verificare che gli oggetti Events, Device Trajectory e Computers siano ripristinati e presentati correttamente nel portale della console.

Passaggio 3. Se si dispone di AMP per integrazioni di rete come FMC, ESA, WSA assicurarsi che possano comunicare con il file Disposition server.

Passaggio 4. Verificare la presenza di eventuali aggiornamenti di contenuto/software (Operazioni - > Aggiorna dispositivo) e procedere con l'installazione di tali aggiornamenti.

Si consiglia vivamente di eseguire test per garantire un aggiornamento corretto.

Modifiche in Virtual Private Cloud 3.0.1

1. Windows Connector versione 6.1.7

Private Cloud 3.0.1 viene fornito con il supporto per la versione 6.1.7 di Windows Connector. La documentazione relativa è disponibile nel collegamento: [Note di rilascio per la versione 6.1.7](#)

Attenzione: Se sono state apportate modifiche ai certificati, verificare che i certificati utilizzati per i servizi cloud privati siano attendibili nell'endpoint stesso prima di un aggiornamento o di un'installazione alla versione 6.1.7 di Windows Connector. L'attendibilità deve essere a livello di computer, non di utente. Se questa condizione non viene soddisfatta, i connettori non considerano attendibile il certificato presentato dal cloud privato che li mantiene in uno stato disconnesso.

2. Servizio Autorità di certificazione e autenticazione

Le modifiche sono state descritte nel manuale dell'utente della versione 3.0: [Guida per l'utente di Private Cloud](#).

Autorità di certificazione consente di gestire i certificati radice per i servizi se si desidera utilizzare un'autorità di certificazione personalizzata. Se necessario, è possibile scaricare o eliminare il certificato radice.

Nelle versioni future di Cloud privato verrà utilizzato il servizio di **autenticazione** per gestire le richieste di autenticazione degli utenti. È stato aggiunto nella versione 3.0.1 per una futura compatibilità.