Private Cloud Administration Portal User Guide

Version 3.0

Last Updated: May 3, 2019

Chapter 1
Set up Virtual

This section will walk you through the steps to install a FireAMP Private Cloud device. Before installing the Private Cloud device familiarize yourself with the system requirements and other prerequisites.

Requirements

A full installation of FireAMP Private Cloud in Proxy Mode requires vSphere ESX.

IMPORTANT! Private Cloud device snapshots can be very large, and in some cases can fill up the datastore being used by the device. This will result in the Private Cloud virtual machine being paused and a disruption in service.

Hardware Requirements

vSphere ESX 5 or higher

- 8 CPUs
- 64 GB RAM
- 1 TB free disk space on the VMWare datastore
  - Type of drives: SSD required
  - RAID Type: One RAID 10 group (striped mirror)
  - Minimum VMware data store size: 1TB

- Minimum Data Store Random Reads for the RAID 10 Group (4K): 60K IOPS
- Minimum Data Store Random Writes for the RAID 10 Group (4K): 30K IOPS

IMPORTANT! The Private Cloud OVA will create the drive partitions so there is no need to specify them in VMWare.

Browser requirements

To access the FireAMP portal and FireAMP Console your browser must support WebSockets and JavaScript. The following browsers are supported:

- Microsoft Internet Explorer 10 or higher
- Mozilla Firefox 14 or higher
- Apple Safari 6 or higher
- Google Chrome 20 or higher

Install Procedure

A FireAMP Private Cloud install can only be performed on a VMware ESXi server using vSphere. You will need to configure your VM to use 8 CPU cores, 64 GB of RAM, and 1 TB of disk space to install the OVA. This section will guide you through installing FireAMP Private Cloud.

Before you begin

FireAMP Private Cloud requires certain infrastructure to be in place before beginning the installation.

- Static IP addresses

  The FireAMP device requires two static IP addresses for its network interfaces. Alternatively, you can reserve IP addresses in DHCP for the MAC addresses of the interfaces.
- Hostnames and trusted certificates

  You will need hostname and trusted certificate pairs for each of the following services:
  - Authentication
  - FireAMP Console
  - Disposition Server
  - Disposition Server – Extended Protocol
  - Disposition Update Service
  - Firepower Management Center Link

IMPORTANT! Hostnames cannot be changed once the device has finished installation.

- SMTP

  If you plan to set up notifications to use an email relay you will need to have the information for the SMTP server you plan to use including authentication information if required.
- NTP server

  You will need to allow your FireAMP device to access a Network Time Protocol (NTP) server. The NTP server can be external or within your network.
- Firewall and Proxy configuration

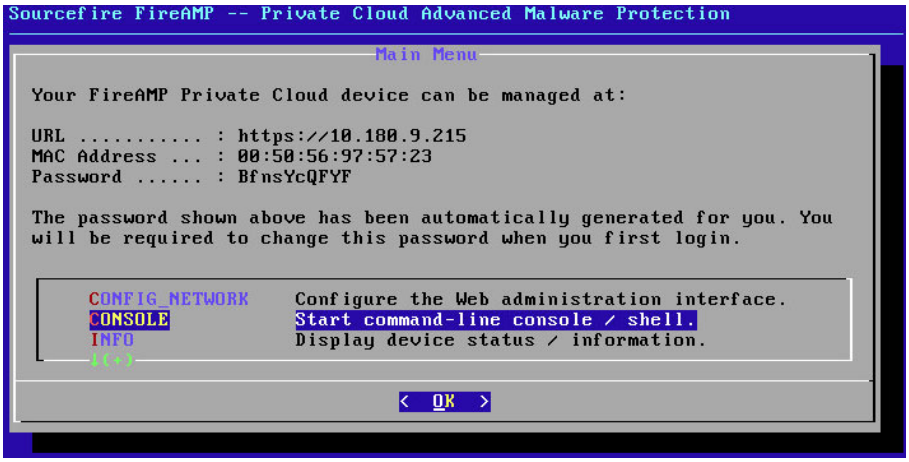
  In addition to access to any of the above services that you configure (NTP, DNS, SMTP), you will need to allow access from the Private Cloud device to the upstream server on TCP port 443. You will also need to allow access from the computers you plan to deploy the FireAMP Connectors on to the Private Cloud device on either TCP port 443. If you use a proxy server you will need to have the proxy hostname, port, and authentication information available.

OVA Import

1. From vSphere select File > Deploy OVF Template.
2. Browse for the location of your FireAMP OVA then click Next.
3. Verify that the OVA has a valid signature from Cisco and click Next.
4. Supply the name for your device and specify the install location in your inventory and click Next.
5. Select the host or cluster where you want to install your device.
6. For the disk format choose Thick Provision Lazy Zeroed.
7. Choose the appropriate network mapping for your device and click Next.
8. Review your configuration options and click Finish.
9. You can increase drive space for your device after the virtual machine has been imported. Right-click the device in vSphere and click Edit Settings. Consult your virtual machine software manual for details on adding additional hard disks.

Configuration

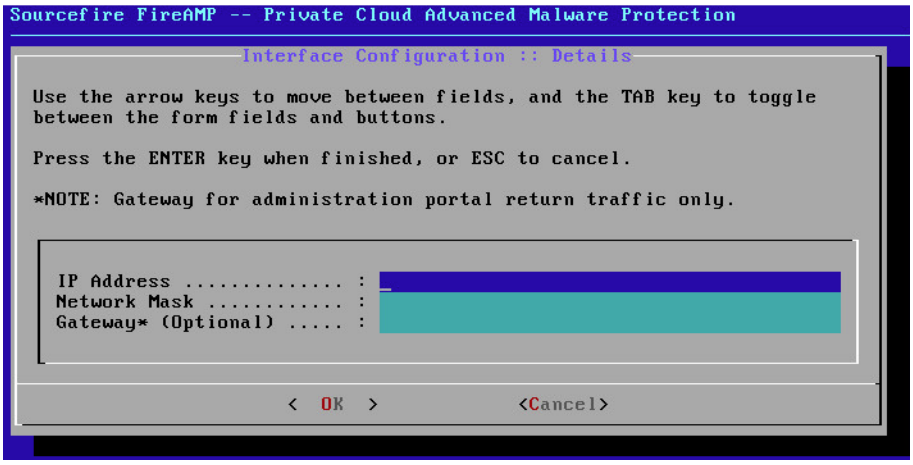
10. Once your installation is complete open your device console from vSphere and power it on.



11. Select Config Network from the console menu. You will be asked if you want to configure your interface through DHCP.

If you are using a reserved address through DHCP select Yes. When you are asked to reconfigure the interface with DHCP select Yes.

If you have assigned a static IP address to the device select No. You will then have to enter the IP address, network mask, and default gateway information for the device. Select Ok when you have entered the correct information. You will then be prompted to reconfigure the administration interface with these settings.

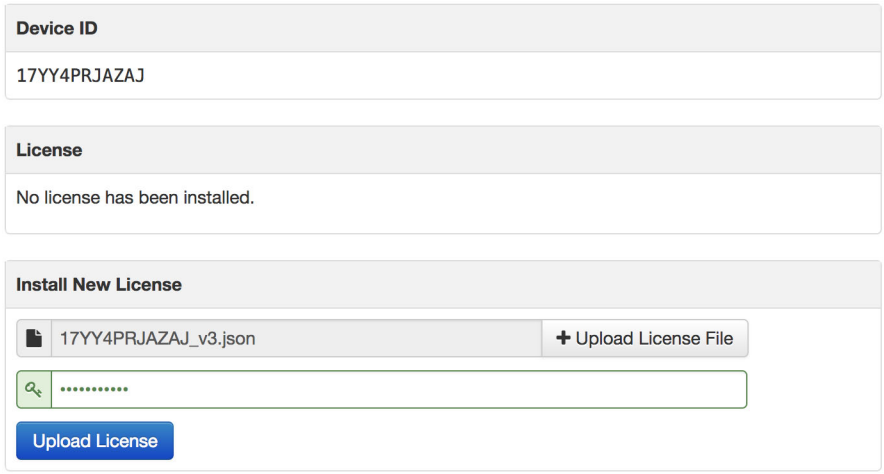


IMPORTANT! It is highly recommended that the FireAMP administration interface be placed on a separate, secure network that is not publicly accessible.

12. Open a browser and navigate to the IP address displayed on the device console that you set in step 11. If you have assigned a DNS name to that interface, you can also navigate to it using that name.

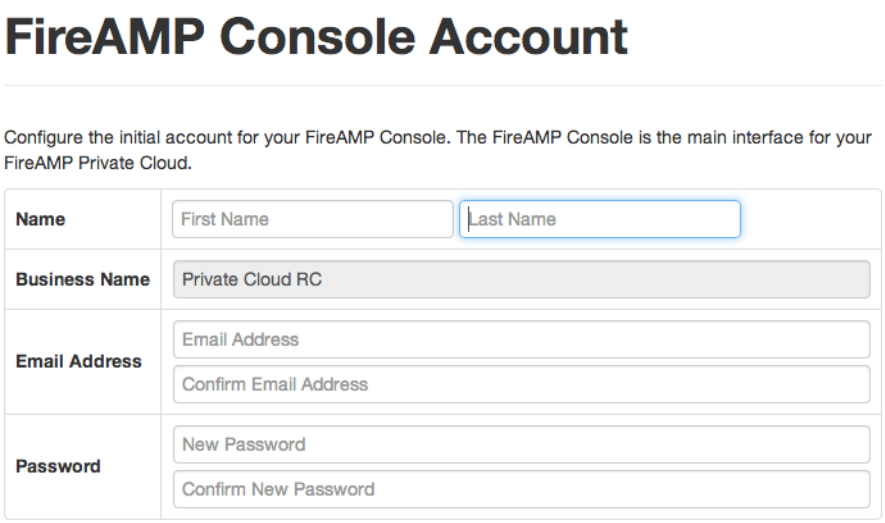
13. You will be prompted to enter a password to login. Enter the temporary password displayed in the device console and click the **Login** button.
14. You will then be prompted to change the password for the Administration Portal. Enter your new password then click **Change Password**.
15. Read and accept the end-user license agreement to continue with the configuration.
16. Next you can choose whether to perform a new installation of FireAMP Private Cloud or restore your device from backup. Choose Clean Installation by clicking the **Start** button below it.

    If you are restoring the device see Restoring from Backup for the necessary steps.
17. On the License page, upload the license file you received for your device and enter the accompanying passphrase. Click **Next** to continue.



18. Verify that your license details are correct then click **Next**.
19. Verify that you have all the network and infrastructure requirements listed on the Welcome screen in place before continuing. Click **Next** when you have completed the requirements.

20. On the FireAMP Console Account page you must enter information for the first user account on your FireAMP Console. The Business Name is populated from your license file. This will be the account used to log into the FireAMP Console once the FireAMP Private Cloud installation is complete.



21. The hardware requirements check lets you know if your VM meets the minimum requirements for FireAMP Private Cloud. If the requirements are not met, you can shut down the VM and reconfigure or continue. If you choose to continue without meeting the minimum requirements your Private Cloud device may experience performance issues and instability.
22. Configure your Network interface by selecting whether to use DHCP or Static addresses. If you select Static you will have to enter the IP address, subnet mask, gateway, and DNS servers in the appropriate fields.

IMPORTANT! You should never configure your device to use DHCP unless you have created MAC address reservations for the interfaces. If the IP addresses of your interfaces change this can cause serious problems with your deployed FireAMP Connectors.

23. Enter the addresses of one or more NTP servers you want to use for Date and Time synchronization. You can use internal or external NTP servers and specify more than one using a comma or space delimited list. Synchronize the time with your browser or run `amp-ctl ntpdate` from the device console to force an immediate time synchronization with your NTP servers.
24. Click the **Add Certificate Authority** button to add your certificate root. Click **+Add Certificate Root** and select your root certificate. Click the **Upload** button once you have selected the correct certificate. Click **Next** once you have uploaded your certificate authority.
25. Select the appropriate Cisco Cloud region. Expand **View Hostnames** if you need to create firewall exceptions for your FireAMP Private Cloud device to communicate with the Cisco Cloud for file lookups and device updates.

26. Select the frequency for critical and regular Notifications. Enter the email addresses you want to receive alert notifications for the FireAMP device. You can use email aliases or specify multiple addresses using a comma separated list. You can also specify the sender name and email address used by the device. These notifications are not the same as FireAMP Console subscriptions. You can also specify a unique Device Name if you have multiple FireAMP Private Cloud devices. Click **Next**.
27. Click **Add SSH Key** to enter any public keys you want to add to the device. SSH keys allow you to access the device via remote shell with root privileges. Only trusted users should be granted access. Your Private Cloud device requires an OpenSSH formatted RSA key. You can add more SSH keys later by navigating to **Configuration >** SSH in your Administration Portal.
28. On the following pages you will assign hostnames and upload matching certificate and key pairs for the device services:
    - Authentication
    - FireAMP Console
    - Disposition Server
    - Disposition Server - Extended Protocol
    - Disposition Update Service
    - Firepower Management Center

    On the page for each service, enter the fully qualified domain name of the host, then click **Replace Certificate**. Click **+Choose Certificate** and **+Choose Key** to upload your matching certificate and key pair for each host. Click **Next** to continue.
29. You must download and verify a backup of your configuration before proceeding with the install. Click **Download** to save the backup to your local computer. Once the file has been downloaded, click **Choose File** to upload the backup file and verify that it is not corrupt. Click **Next** to verify the file and proceed.
30. Review your FireAMP settings before beginning the installation. You can go back to previous steps to change settings using the navigation bar on the left. If you edit any settings you will have to download a new backup file with the new settings and verify it. Once you are satisfied with your configuration settings click **Start Installation**.
31. When the installation has completed you will receive a message to reboot the FireAMP device. Click **Reboot**. When the device has finished rebooting you will be taken to the FireAMP Administration Portal landing page.

Now that the configuration and installation of the device is complete you can launch the FireAMP Console from the Administration Portal. Use the account you created in step 20 to log into the FireAMP Console.

Restoring from Backup

To restore your Private Cloud device from a backup, you must have successfully generated and downloaded a backup file from your Private Cloud device. See Backups to configure your backup schedule.

Restore from Local File

1. Follow the steps in Install Procedure up to step 10 and note the IP address of your new device from the URL field.
2. To transfer the backup file via scp:
   - On the device where your backup file is stored, run the following command:

     ```
     scp /backup/filepath/backupfile.bak
     root@<IP_address_of_new_device>:/data/
     ```
   - If you are prompted with a message stating “The authenticity of host ‘ip_address’ can't be established. Are you sure you want to continue connecting (yes/no)?” reply “yes”.
   - If you are prompted for a password, enter the password from Install Procedure step 10.
   - Proceed to step 4.
3. To transfer the backup file via sftp:
   - On the device where your backup file is stored, run the following command:

     ```
     sftp root@<IP_address_of_new_device>
     ```
   - If you are prompted with a message stating “The authenticity of host ‘ip_address’ can't be established. Are you sure you want to continue connecting (yes/no)?” reply “yes”.
   - If you are prompted for a password, enter the password from Install Procedure step 10.
   - Navigate to the /data directory on the destination server using the following command:

     ```
     sftp> cd /data
     ```
   - Transfer the backup file using the following command:

     ```
     sftp> put /backup/filepath/backupfile.bak
     ```
   - Close the sftp session using the following command:

     ```
     sftp> exit
     ```
   - Proceed to step 4.
4. Continue to follow the steps in Install Procedure up to step 16.
5. Select **Local** in the Restore box and specify the path where you transferred your backup file in step 2 or 3 then click **Start**.
6. When prompted click **Reconfigure Administration Portal Now**.
7. Once reconfiguration is complete login to the Administration Portal using the password from the Administration Portal you restored.
8. After a successful restore you can safely delete the backup file you copied to the server to free up disk space.

Restore from Remote File

1. Follow the steps in Install Procedure up to step 16.
2. Select **Remote** in the Restore box and specify the path to the remote server where your backup file is located then click Start.
3. When prompted click **Reconfigure Administration Portal Now**.
4. After reconfiguration is complete login to the Administration Portal using the password from the Administration Portal you restored.

Restore via Upload

1. Follow the steps in Install Procedure up to step 16.
2. Select **Upload** in the Restore box.
3. Click **Choose File** and navigate to the backup file on your local computer then click **Start**.
4. When prompted click **Reconfigure Administration Portal Now**.
5. After reconfiguration is complete login to the Administration Portal using the password from the Administration Portal you restored.

Chapter 2
Set up Appliance

This section will walk you through the steps to install FireAMP Private Cloud on your AMP PC3000 appliance. Before installing the Private Cloud device familiarize yourself with the requirements and prerequisites.

Requirements

The AMP PC3000 appliance includes all hardware necessary to support 100,000 Connectors.

Browser requirements

To access the FireAMP portal and FireAMP Console your browser must support WebSockets and JavaScript. The following browsers are supported:

- Microsoft Internet Explorer 10 or higher
- Mozilla Firefox 14 or higher
- Apple Safari 6 or higher
- Google Chrome 20 or higher

Install Procedure

This section will guide you through configuring FireAMP Private Cloud on your AMP PC3000 appliance. This guide assumes you have already rack mounted your chassis, connected cables, and followed the initial configuration found in the Cisco AMP PC3000 Hardware Installation Guide.

Deployment modes

The AMP PC3000 appliance offers three different modes that it can be configured to run.

Cloud Proxy

In cloud proxy mode the Connectors send queries to the appliance and the appliance acts as a proxy to the Cisco Cloud.

- Requires an Internet connection and communication with 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.

Standalone Connected

In standalone connected mode the Connectors send queries to the appliance but the appliance has a local copy of file dispositions and other updates. The appliance automatically downloads content and updates through an Internet connection.

- Requires an Internet connection.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates can be automatically downloaded and applied to this Private Cloud device.

Standalone Air Gap

In standalone air gap mode the Connectors send queries to the appliance but the appliance has a local copy of file dispositions and other updates. You must manually download content and updates with a separate computer and physically transfer them to the device.

- Does not require an Internet connection.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates must be downloaded separately and applied to this Private Cloud device.

Before you begin

FireAMP Private Cloud requires certain infrastructure to be in place before beginning the installation.

- Static IP addresses

  The FireAMP device requires two static IP addresses for its network interfaces. Alternatively, you can reserve IP addresses in DHCP for the MAC addresses of the interfaces.

- Hostnames and trusted certificates

  You will need hostname and trusted certificate pairs for each of the following services:

  - Authentication
  - FireAMP Console
  - Disposition Server
  - Disposition Server – Extended Protocol
  - Disposition Update Service
  - Firepower Management Center Link

  IMPORTANT! Hostnames cannot be changed once the device has finished installation.

- SMTP

  If you plan to set up notifications to use an email relay you will need to have the information for the SMTP server you plan to use including authentication information if required.

- NTP server

  You will need to allow your FireAMP device to access a Network Time Protocol (NTP) server. The NTP server can be external or within your network.

- Firewall and Proxy configuration

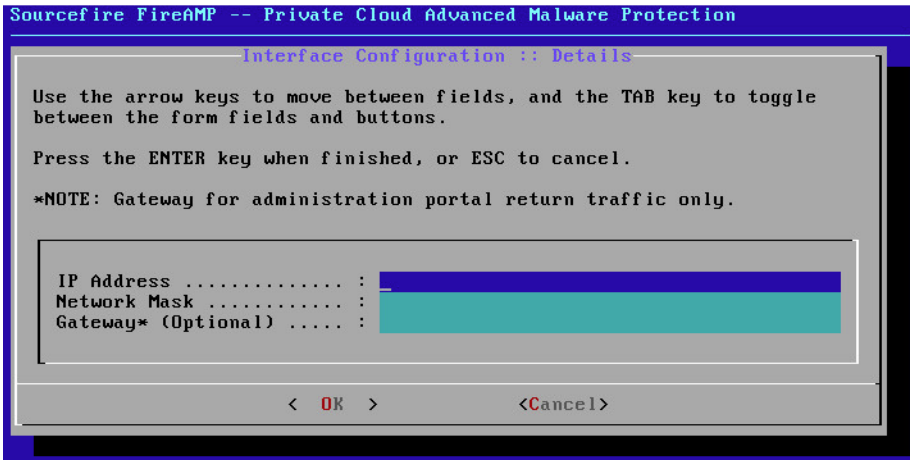
  In addition to access to any of the above services that you configure (NTP, DNS, SMTP), you will need to allow access from the Private Cloud device to the upstream server on TCP port 443. You will also need to allow access from the computers you plan to deploy the FireAMP Connectors on to the Private Cloud device on either TCP port 443. If you use a proxy server you will need to have the proxy hostname, port, and authentication information available.

Configuration

1. After you have completed step 10 from the Cisco AMP PC3000 Hardware Installation Guide select Config Network from the console menu. You will be asked if you want to configure your interface through DHCP.

   If you are using a reserved address through DHCP select Yes. When you are asked to reconfigure the interface with DHCP select Yes.

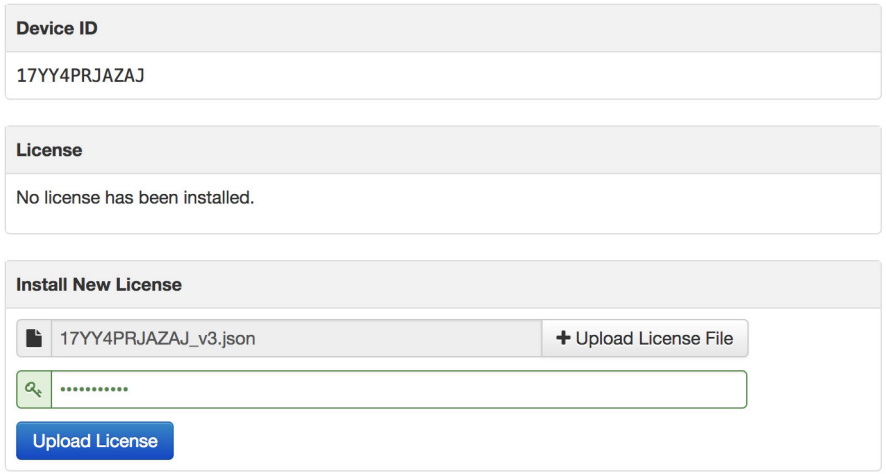
   If you have assigned a static IP address to the device select No. You will then have to enter the IP address, network mask, and default gateway information for the device. Select Ok when you have entered the correct information. You will then be prompted to reconfigure the administration interface with these settings.



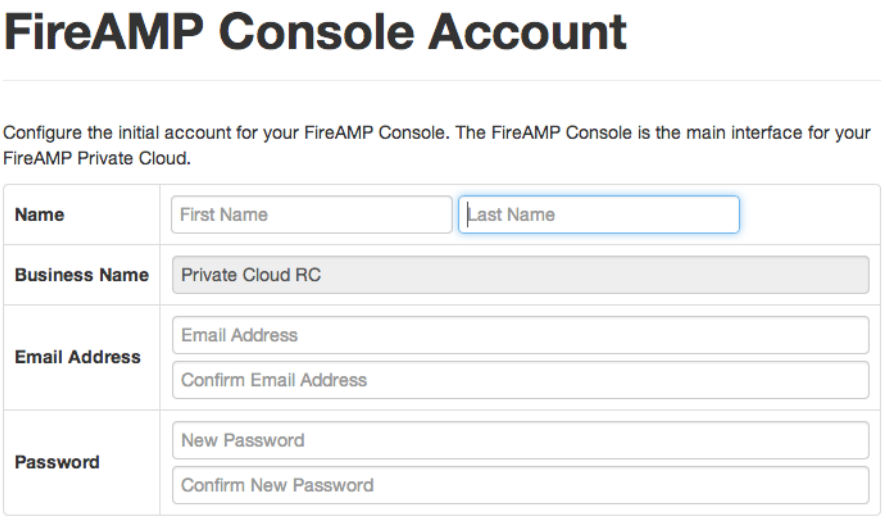
IMPORTANT! It is highly recommended that the FireAMP administration interface be placed on a separate, secure network that is not publicly accessible.

2. Open a browser and navigate to the IP address displayed on the device console that you set in step 1. If you have assigned a DNS name to that interface, you can also navigate to it using that name.
3. You will be prompted to enter a password to login. Enter the temporary password displayed in the device console and click the **Login** button.
4. You will then be prompted to change the password for the Administration Portal. Enter your new password then click **Change Password**.
5. Read and accept the end-user license agreement to continue with the configuration.
6. Next you can choose whether to perform a new installation of FireAMP Private Cloud or restore your device from backup. Choose Clean Installation by clicking the **Start** button below it.

7. On the License page, upload the license file you received for your device and enter the accompanying passphrase. Click **Next** to continue.



8. Verify that your license details are correct then click **Next**.
9. Verify that you have all the network and infrastructure requirements listed on the Welcome screen in place before continuing. Click **Next** when you have completed the requirements.
10. On the Deployment Mode page you can select Cloud Proxy or Standalone mode. If you choose Standalone then you must select Standalone Connected or Standalone Air Gap on the Standalone Operation page.
11. On the FireAMP Console Account page you must enter information for the first user account on your FireAMP Console. The Business Name is populated from your license file. This will be the account used to log into the FireAMP Console once the FireAMP Private Cloud installation is complete.



12. The Hardware Configuration page shows your CPU and memory configuration so you can verify this matches your appliance specifications.
13. Configure your Network interface by selecting whether to use DHCP or Static addresses. If you select Static you will have to enter the IP address, subnet mask, gateway, and DNS servers in the appropriate fields.

    IMPORTANT! You should never configure your device to use DHCP unless you have created MAC address reservations for the interfaces. If the IP addresses of your interfaces change this can cause serious problems with your deployed FireAMP Connectors.

14. Enter the addresses of one or more NTP servers you want to use for Date and Time synchronization. You can use internal or external NTP servers and specify more than one using a comma or space delimited list. Synchronize the time with your browser or run `amp-ctl ntpdate` from the device console to force an immediate time synchronization with your NTP servers.
15. Click the **Add Certificate Authority** button to add your certificate root. Click **+Add Certificate Root** and select your root certificate. Click the **Upload** button once you have selected the correct certificate. Click **Next** once you have uploaded your certificate authority.
16. **[Cloud Proxy mode only]** Select the appropriate Cisco Cloud region. Expand **View Hostnames** if you need to create firewall exceptions for your FireAMP Private Cloud device to communicate with the Cisco Cloud for file lookups and device updates.
17. **[Air Gap mode only]** Download the amp-sync tool and copy it to an Internet-connected computer. This script allows you to download updates and build an ISO file that can be transferred to your Private Cloud appliance. See amp-sync for details on using this utility.
18. Select the frequency for critical and regular Notifications. Enter the email addresses you want to receive alert notifications for the FireAMP device. You can use email aliases or specify multiple addresses using a comma separated list. You can also specify the sender name and email address used by the device. These notifications are not the same as FireAMP Console subscriptions. You can also specify a unique Device Name if you have multiple FireAMP Private Cloud devices. Click **Next**.
19. Click **Add SSH Key** to enter any public keys you want to add to the device. SSH keys allow you to access the device via remote shell with root privileges. Only trusted users should be granted access. Your Private Cloud device requires an OpenSSH formatted RSA key. You can add more SSH keys later by navigating to **Configuration >** SSH in your Administration Portal.
20. On the following pages you will assign hostnames and upload matching certificate and key pairs for the device services:
    - Authentication
    - FireAMP Console
    - Disposition Server
    - Disposition Server - Extended Protocol
    - Disposition Update Service

- Firepower Management Center

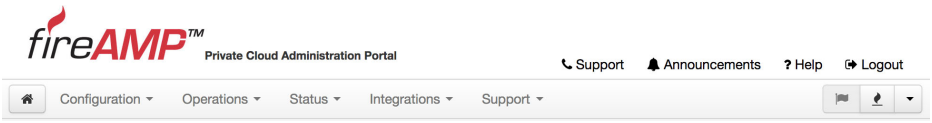
On the page for each service, enter the fully qualified domain name of the host, then click **Replace Certificate**. Click **+Choose Certificate** and **+Choose Key** to upload your matching certificate and key pair for each host. Click **Next** to continue.

21. You must download and verify a backup of your configuration before proceeding with the install. Click **Download** to save the backup to your local computer. Once the file has been downloaded, click **Choose File** to upload the backup file and verify that it is not corrupt. Click **Next** to verify the file and proceed.
22. Review your FireAMP settings before beginning the installation. You can go back to previous steps to change settings using the navigation bar on the left. If you edit any settings you will have to download a new backup file with the new settings and verify it. Once you are satisfied with your configuration settings click **Start Installation**.
23. When the installation has completed you will receive a message to reboot the FireAMP device. Click **Reboot**. When the device has finished rebooting you will be taken to the FireAMP Administration Portal landing page.

Now that the configuration and installation of the device is complete you can launch the FireAMP Console from the Administration Portal. Use the account you created in step 11 to log into the FireAMP Console.

Chapter 3
Administration Portal

The Administration Portal allows you to manage the operation of your FireAMP Private Cloud device. You can change configuration settings, update the device, integrate other Cisco devices and services, or launch support sessions.



There is a link to open a ticket with Cisco Support and a link to view current and past system announcements. There are also links to the Help system and clicking Logout will end your current session.

There are three buttons to the right of the menus. The first shows you if there are any available device updates and takes you to the Update Device page. The second launches the FireAMP Console, and the third allows you to reboot or shut down your Private Cloud device.

When you first log into the Administration Portal you will see a dashboard that shows Key performance metrics for the device. Navigate to Status > Metrics or click **Details** on a metric for more detailed metrics.

Chapter 4
Configuration

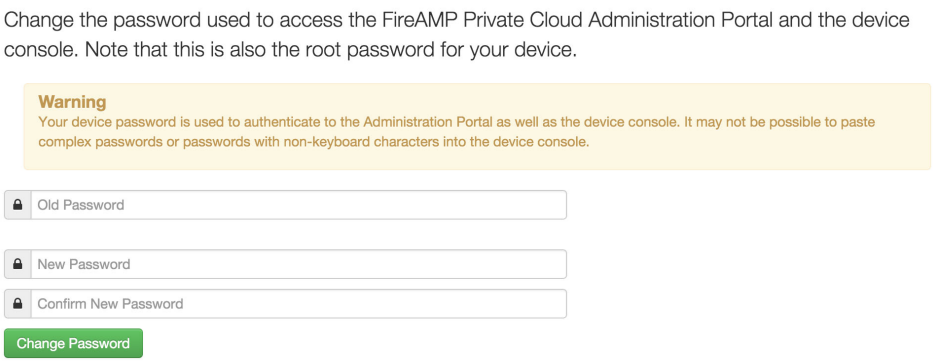
This section describes all the configuration options for the FireAMP Private Cloud device.

Device Summary

The Device Summary shows your current configuration settings. The installation type, initial FireAMP Console account information, storage configuration, and recovery status are displayed. Some of these settings cannot be changed after the device has been configured and are only displayed for informational purposes.

Change Password

The change password screen allows you to change the password required to access the FireAMP Private Cloud Administration Portal and the device console. This is effectively the root password for your FireAMP Private Cloud device.



IMPORTANT! The device console does not support non-keyboard characters. If you set a password using these characters you will not be able to authenticate to the device console.

Cisco Cloud

(Cloud proxy mode only) Cisco Cloud settings allow you to establish communications between your FireAMP Private Cloud device and Cisco cloud servers.

Region is used to specify the server your Private Cloud device will send requests to. You can specify North America or Europe by selecting the appropriate entry in the pulldown. You can also view the hostnames that your Private Cloud device needs to be able to reach so that you can create firewall exceptions if necessary.

The **Client Identity** is displayed in case it is requested by a support engineer. The Client Identity is unique to each Private Cloud device.

Network

The Network page allows you to change the configuration of your device interfaces.

The **Administration Portal** section allows you to view the current interface settings for the administration portal.

Interface Configuration changes the IP address assignment of eth1. Your FireAMP Console and Disposition Server services are running on this interface.

IMPORTANT! If you change the IP address of the interface you must also update the DNS records for your FireAMP Console and Disposition Server to point to the new address.

The **DNS** section allows you to specify the primary and secondary DNS servers that your Private Cloud device will use to perform DNS lookups.

Date and Time

This page allows you to synchronize your current time and specify Network Time Protocol (NTP) servers for your device to synchronize with. Setting the correct date and time on your device is important as time skew can cause problems with your FireAMP deployment.

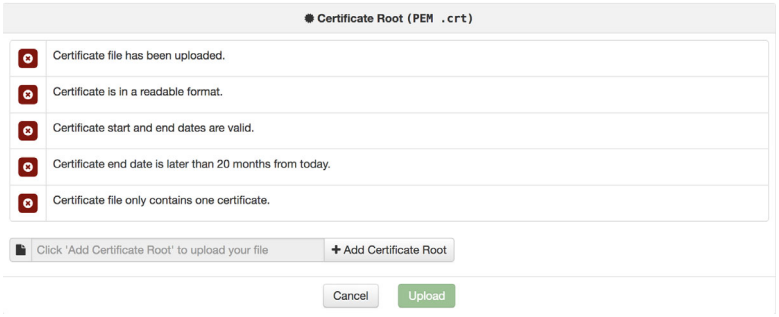
Click **Synchronize with Browser** to synchronize the date and time on your device with the computer you are configuring the device from. This option only appears if you do not have an NTP server specified

Enter one or more NTP servers to synchronize with. These NTP servers can be internal or external, as long as the device can access them on UDP port 123. You can run `amp-ctl ntpdate` from the device console command line interface to force an immediate synchronization between your device and the configured NTP servers.

Certificate Authorities

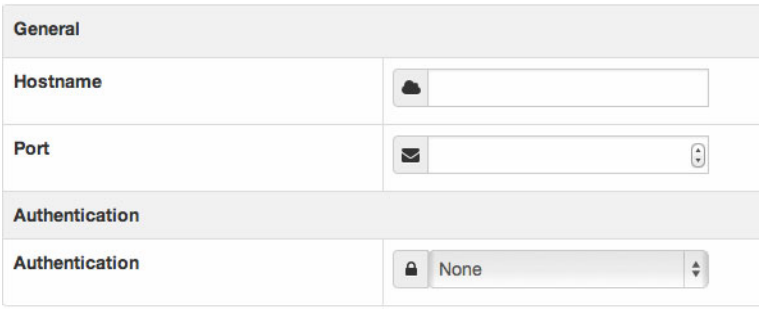
The Certificate Authorities page allows you to manage root certificates for your Services if you want to use a custom certificate authority. You can download or delete your existing root certificate.

Click **Add Certificate Authority** to add a new root certificate to your Private Cloud device. From the Add Certificate Authority page click **+Add Certificate Root** to browse to and select the root certificate, then click Upload.



Proxy

If there is a proxy between your FireAMP Private Cloud device and the upstream server, you must specify the settings on this page. Only HTTP proxies are supported.



Hostname is the name or IP address of the proxy.

Port is the port number the proxy listens on.

Authentication can be None or Basic. If you select Basic you must also provide the Username and Password for proxy authentication.

Notifications

Notifications are alerts and informational messages about your FireAMP Private Cloud device. These include audit, recovery, health, and system events. You can enter one or more email addresses to receive the notifications along with the notification frequency.

Critical Notification Frequency lets you set how often critical device notifications are sent. Critical notifications can be set with a different frequency since these events usually require immediate attention and have an impact on the functionality of your FireAMP Private Cloud device, the FireAMP Console, and FireAMP Connectors.

IMPORTANT! It is highly recommended that the Critical Notification Frequency be set to 5 minutes as these alerts will require immediate attention to continue uninterrupted service.

Notification Frequency lets you set how often all other notifications are sent. Since these notifications are not critical a longer interval can safely be used.

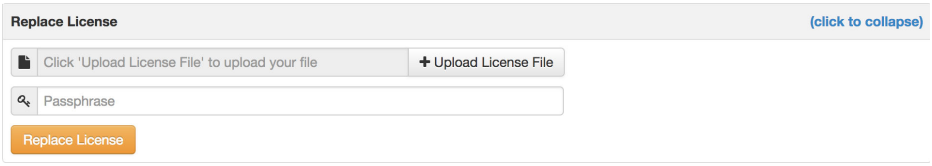
Enter the email addresses of the individuals or distribution groups to receive these alerts in the **Notification Recipients** field. Multiple email address entries must be separated by a comma.

You can also specify the **Notification Sender Address** and **Notification Sender Name** for the emails. If you have multiple Private Cloud devices it can also be useful to specify the **Device Name** for notifications. This will appear as part of the email subject line when specified.

Once you configure notifications you can click the **Send a Test Notification** button to verify your settings.

License

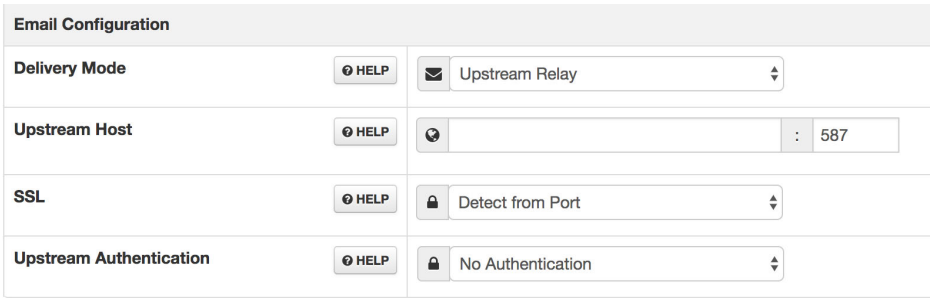
The license page allows you to view information about your current FireAMP Private Cloud license and install a new license. On this page you will find your **Device ID**, the **Licensee** and **Business** that the license is assigned to, the **Validity** dates of the license, the **Product SKU**, and number of **Seats**.



To install a new license, expand the Replace License section then click **+Upload License File** and select your license file. Enter the accompanying Passphrase for the license and click **Replace License**.

Email

The Email configuration page allows you to choose how your device will send email notifications. This includes device notifications and subscription email from the FireAMP console.



You can set the configuration to have the device send email messages directly, or you can configure the device to route all email through an upstream relay.

If you choose to use an upstream relay you will have to enter the upstream host and port number. If the upstream relay uses SASL authentication you will also have to provide a username and password. Once your email server settings are complete you will need to reconfigure the device then go to **Configuration > Notifications** to send a test notification to verify email delivery.

Backups

The scheduled backups page displays your current automated backup schedule and retention policy. Backup files contain your FireAMP Private Cloud databases and configuration and are saved in /data/backups (Private Cloud device) or /other/backups (Private Cloud appliance) as files named amp-backup-yyyymmdd-hhmm.ss.bak. yyyymmdd represents the date and hhmm.ss the time the backup file was created.

You can access your previous backups by navigating to **Operations >** Backups or from `/data/backups`.

IMPORTANT! A backup job cannot start while another backup job is already running or a Protect DB import is in progress.

SSH

The SSH screen allows you to add public keys to the device to allow remote shell access to the Administration Portal. SSH keys also give the user remote root authentication to the device. Only trusted users should be granted access. Your Private Cloud device requires an OpenSSH formatted RSA key. You can convert a putty key from .ppk format to OpenSSH using ssh-keygen with the -i and -f switches.

Syslog

You can configure your Private Cloud device to send log events and FireAMP notifications to a remote syslog server. Enter the hostname of the syslog server and select TCP or UDP to enable this feature. You can specify a specific port by appending a colon and port number to the hostname. If you don't supply a port number, TCP port 514 will be used by default. Leaving the hostname field blank will disable the syslog feature.

Updates

The Updates page is used to configure Device Updates, Content Updates, and Protect DB Updates. **Device Updates** include new and updated operating system binaries to add functionality, improve performance, and patch bugs. **Content Updates** include new TETRA and ClamAV definitions, SPERO trees, Indications of Compromise, and DFC lists. **Protect DB Updates** include disposition information on SHA-256 values used by your FireAMP Connectors.

Device Update **Frequency** can be set to Daily, Weekly, or Never. The **Action** taken can be to Notify that a new update is available or to Download the update. You can also select the **Hour** of the day that you want the update check to occur.

Content Update **Frequency** can be set to Hourly, Daily, Weekly, or Never. The **Action** taken can be to Download the update, Notify that an update is available, or Apply/Install the update. You can also select the **Hour** of the day that you want the update check to occur unless you select a Frequency of Hourly.

IMPORTANT! Setting a large interval between content updates could result in heavy network traffic when an update is downloaded. If you set a large interval between updates make sure to schedule the update at a time when network demand will be low for an extended period such as during the night or on a weekend.

Services

Sub-menu items under Services allow you to replace the SSL certificate and key pairs for the services on your FireAMP Private Cloud. Certificates must be signed by a trusted authority or by one of the root certificates you added to Certificate Authorities.

IMPORTANT! You must upload the chain certificate for each hostname. Uploading the individual or leaf certificate will result in an error.

Administration Portal

The **Administration Portal** allows you to manage the back end of your Private Cloud device.

Authentication

The **Authentication** service will be used in future versions of Private Cloud to handle user authentication.

FireAMP Console

FireAMP Console is the DNS name where the FireAMP administrator can access the FireAMP Console and FireAMP Connectors receive new policies and updates.

Disposition Server

Disposition Server is the DNS name where the FireAMP Connectors send and retrieve cloud lookup information.

Disposition Server - Extended Protocol

Disposition Server - Extended Protocol is the DNS name where newer FireAMP Connectors send and retrieve cloud lookup information.

Disposition Update Service

Disposition Update Service is used when you link a Cisco Threat Grid appliance to your Private Cloud device. The Threat Grid appliance is used to send files for analysis from the FireAMP Console and the Disposition Update Service is used by Threat Grid to update the disposition (clean or malicious) of files after they have been analyzed.

Firepower Management Center

Firepower Management Center Link lets you link a Cisco Firepower Management Center (FMC) device to your Private Cloud device. This allows you to display FireAMP data in your FMC dashboard. For more information on FMC integration with FireAMP see your FMC documentation.

Chapter 5
Operations

This section describes the operational aspects of maintaining the FireAMP Private Cloud device.

Backups

The Backups page allows you to perform manual backups of your device and download previous backups. Older backups or backups you have already moved off site can also be deleted to free disk space on your device.

IMPORTANT! A disk space check is performed before a backup job begins. If there is not enough disk space then older backup files will be deleted until there is enough free space. If there is still not enough free space after deleting old backup files the backup job will not start.

Click the **Perform Backup** button to start an immediate backup of your databases as long as another backup job or Protect DB import is not running. This is useful before updating the device software or performing other maintenance tasks like adding additional storage. Backup files contain your FireAMP Private Cloud databases and configuration and are saved in /data/backups (Private Cloud device) or /other/backups (Private Cloud appliance) as files named amp-backup-yyyymmdd-hhmm.ss.bak. yyyymmdd represents the date and hhmm.ss the time the backup file was created.

IMPORTANT! Backups include sensitive information like passwords and cryptographic key material so they should always be stored in secure locations with limited access.

Registration

(Cloud proxy mode only) Registration allows you to verify connectivity between your device and Cisco cloud servers. If you change proxy or firewall configuration settings you can verify connectivity through this page. If you are experiencing a 100% cloud query failure rate you can also re-register to see if this corrects the problem.

Apply Configuration

Your device must be reconfigured after changing certain settings. Usually a notification that the device requires reconfiguration will be displayed after you change one of these settings. If you want to change multiple settings at once you can change each one then navigate to this page to reconfigure the device.

Migrations

Migrations are operations which may be required to enable new features or maintain system performance on your device. Migrations may appear after a system upgrade. If a migration is available, the steps for performing the specific migration will be available at that time.

Maintenance Mode

Maintenance Mode stops all external services on your FireAMP Private Cloud device. It should only be used when adding additional storage to the device, updating the device, or when instructed by support during extended troubleshooting.

IMPORTANT! While the device is in Maintenance Mode your FireAMP Connectors will not be able to perform cloud lookups and the device cannot download Protect DB updates. Only put the device into Maintenance Mode when required and take it out of Maintenance Mode immediately after.

Update Device

The Update Device page allows you to update the definitions for your FireAMP Connectors, DFC lists, SPERO trees, Indications of Compromise, TETRA definitions, and the Private Cloud device software, as well as the Protect DB for Standalone deployments. In Proxy Mode and Standalone Connected Mode you need an Internet connection from your device to Cisco servers, while in Standalone Air Gap Mode you will have to use amp-sync to create an ISO file and mount it in your virtual machine.

Proxy Mode

You can check for content updates for your FireAMP Connectors outside of your scheduled Updates or if you have chosen not to have your device check for updates automatically. Content updates include TETRA, Linux, and Mac definitions, SPERO trees, and IP white and black lists. Click **Check / Download Updates** to check for new

updates and download them to your device. Click **Update Content** once the download has completed to apply the update. You can also view the update details by clicking on the information link.

IMPORTANT! If you have not downloaded new device content for a long period of time make sure to initiate the update at a time when network demand will be low for an extended period such as during the night or on a weekend as the size of the update could be significant.

You can also check for updates to your FireAMP Private Cloud device outside of your scheduled Updates or if you have chosen not to have your device check for updates automatically. Click **Check / Download Updates** to check for new updates and download them to your device. Click **Update Software** once the download has completed. Your device will automatically be put into Maintenance Mode before running the update. You can also view the update details by clicking on the information link.

IMPORTANT! Always perform a backup and take a snapshot of your device before running an update.

Standalone Connected Mode

You can check for content updates for your FireAMP Connectors outside of your scheduled Updates or if you have chosen not to have your device check for updates automatically. Content updates include the Protect DB, TETRA, Linux, and Mac definitions, SPERO trees, and IP white and black lists. Click **Check / Download Updates** to check for new updates and download them to your device. Click **Update Content** once the download has completed to apply the update. You can also view the update details by clicking on the information link.The first time you go to the Updates / Protect DB page click **Check / Download Updates** then click **Import Protect DB** to load a Protect database on your device.

IMPORTANT! Your Private Cloud appliance comes with a version of Protect DB already loaded but it will be out of date. You should update the Protect DB as soon as possible.

You can also check for updates to your FireAMP Private Cloud device outside of your scheduled Updates or if you have chosen not to have your device check for updates automatically. Click **Check / Download Updates** to check for new updates and download them to your device. Click **Update Software** once the download has completed. Your device will automatically be put into Maintenance Mode before running the update. You can also view the update details by clicking on the information link.

IMPORTANT! Always perform a backup and take a snapshot of your device before running an update.

Standalone Air Gap Mode

Use this page to mount the ISO created using amp-sync so that you can update your device. The ISO can contain software updates for your Private Cloud device and FireAMP Console as well as updates to the Protect DB. The Protect DB is a database containing file dispositions - files are classified by SHA-256 value as being clean or malicious.

IMPORTANT! Your Private Cloud appliance comes with a version of Protect DB already loaded but it will be out of date. You should run amp-sync to update the Protect DB as soon as possible.

Attach your ISO file to the device through the Cisco Integrated Management Controller (CIMC) on your appliance, then click **Check Update ISO**. The first time you go to the Updates / Protect DB page and mount an ISO with a Protect DB, click **Import Protect DB** to load a protect database on your device.

If you already have a Protect DB installed you can click the **Update Software** button to install software updates or click the **Update Content** button to install incremental updates to your Protect DB. Importing a Protect DB and updating the device software will automatically put the device into Maintenance Mode.

IMPORTANT! Do not unmount your ISO during an update as this can put your device into an unusable state. Detaching your ISO from the virtual machine without unmounting it first can cause your device to stop responding.

Chapter 6
Status

The items in the Status menu of your device give you information on software versions, various metrics, and the device event log.

About

The About page lists the version of your FireAMP Private Cloud device and version numbers of all associated packages. This information can be useful when troubleshooting issues with a support engineer.

Metrics

Metrics include various operating statistics of your device, including the status of your cloud proxy, disk usage and performance, and system performance. Graphs in the granular metric views show the current trend by default but can also be expanded to the last hour, day, week, or month.

Key

Key metrics provide a representation of your current general device status at a glance. Click Details below each metric for a more detailed view of the particular metric. Metrics displayed in green are within normal operating parameters, while those in yellow or red require attention. Metrics displayed in yellow will require attention, but the device is still functional, while those in red require immediate attention as the device may be in a state that severely impacts its performance.

Cisco Cloud

(Cloud proxy mode only) The FireAMP Private Cloud device functions as a proxy for cloud queries between your Connectors and the Cisco cloud. Cisco Cloud metrics describe communications between your device and the upstream destination.

Cisco Cloud Query Failure Rate displays the percentage of disposition queries that have failed.

Cisco Cloud Query Latency shows the latency in milliseconds for both upstream and downstream communication between your device and the Cisco cloud. High latency rates may indicate that your network link is running at or near capacity.

Cisco Cloud Query Total shows the number of queries per second your device is handling.

Disposition Server

Active Connections shows how many FireAMP Connectors are currently attached to your Private Cloud device.

Disk Performance

Disk performance represents the seek time for disk reads and writes.

Disk latency : sda represents the latency for your first storage device, the boot partition by default.

Disk latency : sdb represents the latency for your second storage device, the root partition by default.

Disk latency : sdc represents the latency for your third storage device, the data partition by default.

Disk latency : sdd represents the latency for your fourth storage device, the var partition by default.

If you have attached any other storage devices to your Private Cloud device they will each be listed here in a separate graph as sde, sdf, sdg, and so on.

Disk Usage

Disk Usage metrics indicate the percentage of used drive space and inodes. High disk usage percentage can be resolved by adding additional storage to your virtual machine and allocating it to the appropriate partition.

Partition Usage: / shows the disk usage of your root partition. This partition contains the operating system and software packages.

PartitionUsage: /boot shows the disk usage of your boot partition. This partition contains the boot loader for your device.

Partition Usage: /data shows the disk usage of your data partition. This partition contains all the databases used by your device.

Partition Usage: /var shows the disk usage of your var partition. This partition is used as a disk cache.

(Private Cloud Appliance only) **Partition Usage: /boot/efi** shows the usage of your boot loader.

(Private Cloud Appliance only) **Partition Usage: /recovery2** shows the disk usage of your recovery partition. This partition is used to store the two most recent ISO images for recovery purposes as well as a Protect DB snapshot.

(Private Cloud Appliance only) **Disk Usage: /other** shows the disk usage of your other partition. This partition is used to store backups, fetched files, and some Protect DB information.

System

System metrics show the CPU and RAM usage on the device. While it is normal for these metrics to show spikes due to periods of high demand, sustained levels in yellow or red may indicate that the device requires more CPU cores or additional RAM allocated to the virtual machine.

CPU Usage shows the percentage of cycles the device is consuming. Both kernel and total cycles are displayed.

Memory Usage shows the percentage of RAM in use. Memory usage with and without caching are displayed.

Notifications

The Notifications page shows various events on your FireAMP Private Cloud device. Events categories include Audit, Recovery, Health, and System. Click the category buttons at the top of the page to filter on these types.

Audit events are related to logins and password changes.

Recovery events include scheduled backups and pruning of stale backup files defined by your backup retention setting.

Health events cover the device health such as disk space and latency, cloud connectivity, and CPU and memory usage.

System events are all actions that occur on a system level such as updates, configuration changes, and when the device enters and leaves maintenance mode.

Events are also divided into four severity levels.

Notice events are normal operating events that are logged.

Warning events can affect device performance and connectivity but are within operating parameters, such as entering maintenance mode.

Error events affect device operations and require attention and intervention. The device may continue to operate after an error event but performance and connectivity may be impacted.

Critical events require immediate intervention to resume proper operations. Essential device operations will be impacted and continue to be impacted until corrected.

Chapter 7
Integrations

The Integrations menu allows you to connect your Private Cloud device to other Cisco appliances in your environment. Currently Private Cloud supports integrations with Cisco Firepower Management Center, Email Security Appliance, Web Security Appliance, Cisco Threat Grid, and Virus Total.

Firepower Management Center

This page allows you to connect a Firepower Management Center (FMC) to your FireAMP Private Cloud device. If you have not set up a Firepower Management Center Link you will be prompted to do so. Follow the instructions on the page to link your FMC to your FireAMP Private Cloud device. You will need access to both the FMC console and the FireAMP Console to complete the link.

Email Security Appliance

This page allows you to connect an Email Security Appliance (ESA) to your FireAMP Private Cloud device. Follow the instructions on the page to link your ESA to your FireAMP Private Cloud device. You will need access to the ESA portal to complete the integration.

Web Security Appliance

This page allows you to connect a Web Security Appliance (WSA) to your FireAMP Private Cloud device. Follow the instructions on the page to link your WSA to your FireAMP Private Cloud device. You will need access to the WSA portal to complete the integration.

Threat Grid

This page helps you connect a Cisco Threat Grid appliance to your Private Cloud. Connecting a Threat Grid appliance allows you to use the File Analysis feature in FireAMP and also perform automatic analysis of Low Prevalence Executables. The Threat Grid Appliance also interacts with the Disposition Update Service on your Private Cloud device to mark previously unknown files as malicious when necessary.

VirusTotal

(Proxy mode only) If you have a VirusTotal API key you can enable VirusTotal lookups for SHA-256 values in your FireAMP Console. Right-clicking on a SHA-256 value will show how many vendors detect the file and the longest common name used for the file on VirusTotal. To set up the integration enter your API key, test the connection, and click Save.

Chapter 8
Support

This section describes how to start live support sessions and take support snapshots.

Live Support Session

Live Support Sessions allow a support engineer to connect to your FireAMP Private Cloud device remotely to assist in diagnosing and repairing problems. To maintain security and privacy support sessions use unique, per-session authentication keys that expire after the session is terminated.

Before starting a support session or submitting a support snapshot, you must send your support identity. The support identity is unique to your device and only needs to be sent once. The first time you open a ticket with support that requires a support session or snapshot, the support engineer will request your identity.

Support Snapshots

A support snapshot contains log files and system information to assist with the diagnosis of problems with your FireAMP Private Cloud device. To create a support snapshot, click the Create Snapshot button then select the information to include as directed by support. Click Go to generate the snapshot. You can click the Details button to see the commands being executed and any errors.

Once the snapshot has been generated, you can download it and attach it to your support case. After you have submitted the snapshot you can view the submission details or delete the snapshot.

Appendix A
Command Line Tools

The FireAMP Private Cloud device console includes several command line tools to manage your device. Go to your device console and select Console from the menu to launch the command line interface (CLI).

AMP-CTL Commands

You can get a list of commands by typing `amp-ctl -h` at the prompt. Type `amp-ctl <command> -h` to get help on a specific command. All [options] are optional, while all <options> are required.

The following sections describe the amp-ctl commands:

backup

Allows the user to create a backup of the device configuration and databases saved in `/data/backups` (Private Cloud device) or `/other/backups` (Private Cloud appliance).

Syntax

```
amp-ctl backup [options]
```

where options are -n to create a notification event after each task is complete,-v for verbose output, and -h for help. The resulting backup archive will be named amp-backup-yyyymmdd-hhmm.ss.bak where yyyymmdd represents the date and hhmm.ss represents the time the backup file was created. Backups created through the command line tool are subject to the backup retention policy and other constraints specified in the Administration Portal under Configuration > Backups.

Example

```
> amp-ctl backup -n
```

chef

Chef performs configuration or reconfiguration of the device.

Syntax

```
amp-ctl chef [options] <operation>
```

where options are -f to force the operation, -v for verbose output, and -h for help. Operation can be opadmin to configure changes to the administration portal or periodic to run the periodic configuration.

Example

```
> amp-ctl chef opadmin
```

check

Check device connectivity, see if it is ready to be updated, check for configuration problems.

Syntax

```
amp-ctl check [options] [operation]
```

where options are -v for verbose output and -h for help. Operation can be connectivity to check that the device can connect to external hosts, pre-update to check that the device is ready for an update, pre-update-content to check that the device is ready for a content update, and sanity to check for configuration problems.

Example

```
> amp-ctl check connectivity
```

config-updates

Configure update settings for the device such as frequency, automatic downloads, and the update server to use.

Syntax

```
amp-ctl config-updates [options]
```

where options are:

-C [freq]	Set the automatic content update frequency to never, 1h, 1d, or 1w.
-c [action]	Set the automatic content update action to notify, download, or install.
-S [host]	Set the content update server to [host].
-s [host]	Set the software update server to [host].
-U [freq]	Set the software update frequency to never, 1d, or 1w.
-u [action]	Set the software update action to notify or download.

Example

```
> amp-ctl config-updates -C 1d -c notify
```

iso (Standalone only)

View information about the currently loaded update data. Update data can be in one of the following states:

- **missing** - An ISO is mounted, but no update data is present. Check that the mounted ISO was built for the installed version of this product.
- **present** - Update data is present; you may use amp-ctl to check for or apply updates and/or content updates, or to load a new Protect DB snapshot if desired.
- **unmounted** - Update data is not present, and an ISO is not mounted.

Syntax

```
amp-ctl iso [options]
```

where option can be

-h	Display this help information.
-m	Mount the currently loaded ISO to the update directory
-u	Unmount the currently loaded ISO to the update directory.
-v	Increase output verbosity.

maintenance

Check if the device is in maintenance mode or toggle maintenance mode.

Syntax

```
amp-ctl maintenance [options] [command]
```

where option can be -h to display the help. Command can be enable to enter maintenance mode, disable to leave maintenance mode, and query to display whether the device is currently in maintenance mode.

Example

```
> amp-ctl maintenance enable
```

ntpdate

Run this command to force an immediate synchronization between your device and the specified NTP servers. You can also use this command to manually set the time and date on the device.

Syntax

```
amp-ctl ntpdate [options] [server]
```

where options can be -f to force a synchronization, -h to display the help, -s [STR] to set the time and date to [STR] in the format YYYY-MM-DD HH:MM:SS, and -v to increase the output verbosity.

Example

```
> amp-ctl ntpdate -s 2014-01-15 15:32:00
```

pdb (Standalone only)

Install or view information about the device's Protect DB (threat intelligence database).

Syntax

```
amp-ctl pdb [options]
```

where options can be

-I	Install a new Protect DB snapshot from the currently loaded update ISO. This option requires maintenance mode to be enabled.
-U	Unsafe install. Installs over the current snapshot, but requires less disk space. The opposite of -s.
-i <path>	Install a new Protect DB snapshot from the data at <path>. This option requires maintenance mode to be enabled.
-f	Force operation; can be used to install a Protect DB snapshot with a bad or missing PGP signature.
-h	Display this help information.

-l	List the currently installed Protect DB snapshot. When in verbose mode, will also print information on deltas.
-s	Safe install. Preserves an existing database as long as possible when installing, so a failed install won't destroy the existing one. Requires a significant amount of extra disk space. (default)
-v	Increase output verbosity.

power

Power down or reboot your Private Cloud device. All running services will be terminated before the device shuts down.

Syntax

```
amp-ctl power [options] [command]
```

where options can be -h to display the help and command is cycle to reboot the device or off to shut the device down.

Example

```
> amp-ctl power off
```

reboot

Reboot your Private Cloud device. All running services will be terminated before the device shuts down.

Syntax

```
amp-ctl reboot
```

Example

```
> amp-ctl reboot
```

register (Proxy Mode only)

Use this command to register a device with the FireAMP Cloud or an upstream device.

Syntax

```
amp-ctl register [options]
```

where options can be:

-a <host>	Use <host> for the upstream asn server.
-e <host>	Use <host> for the upstream est server.
-c <path>	Use alternate certificate to validate the upstream est server.
-d <path>	Use alternate certificate to validate the upstream asn server.

-B <path>	Use an alternate public key file located at <path> for the remote server.
-P <pstr>	Use <pstr> for the protocol and protocol options string.
-V <path>	Use an alternate private key file located at <path> for the client identity.
-b <path>	Use an alternate public key file located at <path> for the client identity.
-g <guid>	Use <guid> as the connector GUID.
-f	Force registration even if it has already completed.
-h	Display the help.
-n	Generate a notification event after the command has completed.
-p <count>	Send <count> cloud-PING queries to the upstream server.
-s <host>	Use <host> for the upstream server.
-v	Enable verbose output.

Example

```
> amp-ctl register -B /tmp/key/key.pub
```

service

This command lets you list and control the services running on the device.

Syntax

```
amp-ctl service [options] [command] [service]
```

where options can be -h to display the help or -v for verbose output. Service is the name of an individual service and command can be:

disable	Stop a service and prevent it from being restarted after a reboot.
enable	Start a service and ensure it restarts after a reboot.
list	List the device services.
restart	Restart a service.
running	Check if a service is running.

start	Start a service.
status	Display the status of a service. If a service name is not specified it will display the status of all services.
stop	Stop a service.
stop-all	Stop all services.
term	Terminate a service. If the service is enabled it will restart automatically.
term-all	Terminate all services. Any services that are enabled will restart automatically.

Example

```
> amp-ctl service list
```

shutdown

Power off your Private Cloud device. All running services will be terminated before the device shuts down.

Syntax

```
amp-ctl shutdown
```

Example

```
> amp-ctl shutdown
```

update

Installs any available updates.

Syntax

```
amp-ctl update [options]
```

where options can be -f to force the update when the pre-update check fails, -v for verbose output, and -h to display the help.

Example

```
> amp-ctl update -f
```

update-check

Checks your configured update server for any available updates.

Syntax

```
amp-ctl update-check [options]
```

where options can be -d to download all available updates, -n to generate a notification event after the check has completed, -v to increase output verbosity, -D to delay for a random number of seconds before checking,and -h to display the help.

Example

```
> amp-ctl update-check -d
```

update-check-content

Check your configured update server for any available content updates. Content updates include TETRA and ClamAV definitions, SPERO trees, and IP white and black lists. In Standalone Connected mode it will also check for Protect DB deltas.

Syntax

```
amp-ctl update-check-content [options]
```

where options can be -d to download all available content updates, -n to generate a notification event after the check has completed, -v to increase output verbosity, -D to delay for a random number of seconds before checking, and -h to display the help.

Example

```
> amp-ctl update-check-content -d -v
```

update-content

Install available content updates downloaded using update-check-content.

Syntax

```
amp-ctl update-content [options]
```

where options can be -f to force the update when the pre-update check fails, -v for verbose output, and -h to display the help.

Example

```
> amp-ctl update-content
```

AMP-Storage-Container Commands

The amp-storage-container command is used to grow the storage containers on your device or create new ones. Before you can allocate additional space you will have to add a storage device to your virtual machine. See your virtual machine management software documentation for more information.

IMPORTANT! After adding a new storage device you may need to reboot your Private Cloud device or run `amp-storage-container rescan` before it is available.

You can get a list of commands by typing `amp-storage-container -h` at the prompt. Type `amp-storage-container <command> -h` to get help on a specific command. All [options] are optional, while all <options> are required.

The following sections describe the amp-ctl commands:

create

Used to create a new storage container on your device.

Syntax

```
amp-storage-container create [options] <container> <disk> [disk]
[...]
```

where options can be -v to enable verbose output or -h to display help. Container will be one of your storage containers and disk will be the name of the block device(s) you added to your virtual machine.

Example

```
> amp-storage-container create data sdf
```

destroy

Used to destroy an existing storage container on your device.

Syntax

```
amp-storage-container destroy [options] <container>
```

where options can be -f to force the command to run, -y to skip confirmation, or -h to display help.

Example

```
> amp-storage-container destroy -y backups
```

disks

This command displays a list of the available block devices attached to your Private Cloud device available for use to grow an existing storage container or create a new one.

Syntax

```
amp-storage-container disks [options]
```

where options can be -j to return the output in JSON format, -v for verbose output, or -h to display the help.

Example

```
> amp-storage-container disks -v
```

grow

Lets you add a block device to an existing storage container to add more disk space to it.

Syntax

```
amp-storage-container grow [options] <container> <disk> [disk]
[...]
```

where options can be -x to grow an XFS container, -v for verbose output, and -h to display the help. Container will be one of your storage containers and disk will be the name of the block device(s) you added to your virtual machine.

Example

```
> amp-storage-container grow data sdd sde sdf
```

health

Checks the health of all storage containers on the device.

Syntax

```
amp-storage-container health [options]
```

where options can be -v for verbose output or -h to display the help.

Example

```
> amp-storage-container health -v
```

list

Display a list of all the storage containers that are currently configured on the device.

Syntax

```
amp-storage-container list [options]
```

where options can be -v for verbose output, -j to return the output in JSON format, or -h to display the help.

Example

```
> amp-storage-container list -j
```

rescan

Scans all available controllers for new disks. Use this command when you add a new disk to the virtual machine but it does not appear when you run the disks command.

Syntax

```
amp-storage-container rescan [options]
```

where option can be -v for verbose output or -h to display the help.

Example

```
> amp-storage-container rescan -v
```

Appendix B
amp-sync

The FireAMP Private Cloud Sync tool allows you to download device and content updates from a remote host, then package the data into an ISO file that can be mounted on a Private Cloud device to update it in an air-gapped environment. Updates include the protect database (Protect DB), which contains file dispositions, and device updates. You should install amp-sync on a computer that has Internet access, sufficient drive space for updates, and a way to write the ISO to transferable media.

Protect DB snapshots and incremental updates are published along with a manifest file that includes SHA-256 checksums for each of the files. The manifest itself is signed and verified (on the Private Cloud appliance rather than the host running amp-sync) before either an initial snapshot is imported or a daily update is applied.

System requirements

To run amp-sync you must have a computer running CentOS 6.6 or higher with at least 500 GB of free disk space. To transfer ISOs to your Private Cloud device in standalone mode, the computer must have the ability to write the ISO to external media such as a USB drive.

CentOS

Installing dependencies

To run amp-sync you will first have to install EPEL, curl, genisoimage, and xmlstarlet.

1. To enable the EPEL repo.

```
> wget
http://download.fedoraproject.org/pub/epel/6/x86_64/epel-
release-6-8.noarch.rpm
> sudo rpm -ivh epel-release-6-8.noarch.rpm
```

2. Install dependencies via yum.

```
> sudo yum install genisoimage
> sudo yum install xmlstarlet
> sudo yum install curl
```

Install amp-sync

1. Download amp-sync from your Private Cloud device and transfer it to your update host. On your update host run the following command:

```
> chmod 700 amp-sync
```

2. To view the amp-sync help:

```
> ./amp-sync -h
```

3. To download all updates, verify them, and package them into an ISO:

```
> ./amp-sync all
```

IMPORTANT! You will have to run `amp-sync all` when you first install the Private Cloud device in standalone mode in order to receive the Protect DB.

Windows 7 x86

1. Download and install the x86 version of Cygwin.
2. Run setup-x86.exe and go through the installation process choosing all the defaults.
3. Choose a download mirror.
4. Select the following packages to install:

   All -> Net -> curl

   All -> Utils -> genisoimage

   All -> Utils -> xmlstarlet

Install amp-sync

1. Download amp-sync from your Private Cloud device and transfer it to your update host in C:\cygwin\home\%username%\
2. To view the amp-sync help:

```
> ./amp-sync -h
```

3. To download all updates, verify them, and package them into an ISO:

```
> ./amp-sync all
```

IMPORTANT! You will have to run `amp-sync all` when you first install the Private Cloud device in standalone mode in order to receive the Protect DB.

Windows 7 x64

1. Download and install the x64 version of Cygwin.
2. Run setup-x86_64.exe and go through the installation process choosing all the defaults.
3. Choose a download mirror.
4. Select the following packages to install:

   All -> Net -> curl

   All -> Utils -> genisoimage

   All -> Utils -> xmlstarlet

Install amp-sync

1. Download amp-sync from your Private Cloud device and transfer it to your update host in C:\cygwin\home\%username%\
2. To view the amp-sync help:

```
> ./amp-sync -h
```

3. To download all updates, verify them, and package them into an ISO:

```
> ./amp-sync all
```

IMPORTANT! You will have to run `amp-sync all` when you first install the Private Cloud device in standalone mode in order to receive the Protect DB.

amp-sync commands

You can get a list of commands by typing ./`amp-sync -h` at the prompt. Type ./`amp-sync <command> -h` to get help on a specific command. All [options] are optional, while all <options> are required.

The following sections describe the amp-sync commands:

all

Fetch, verify, and package content update data from a Cisco FireAMP update server to an ISO.

Syntax

```
./amp-sync all [options]
```

Where [options] can be:

-D	Delete old database deltas. Requires -M.
-M <seq>	Include deltas starting at sequence number <seq>. Use this option with the lowest sequence number needed across all of your FireAMP Private Cloud devices to reduce the amount of data fetched and stored on your ISO.
-N	Fetch new snapshot. A full database snapshot is fetched the first time a fetch is done. Afterwards, only deltas are retrieved. Snapshots are loaded by a FireAMP Private Cloud device only when installing or restoring from backup. Use this option to refresh the snapshot available on your update ISO before installing or restoring a device to avoid needing to apply a large amount of deltas.
-X	Exclude snapshot. Use this option to reduce the size of your ISO. An ISO generated with this option can only be used to update a Private Cloud device, not to install or restore one.
-h	Display this help information.
-l <rate>	Limit download speed to <rate> bytes per second. Defaults to having no limit.
-o <file>	Output to <file> instead of %{PRODUCT}-%{VERSION}-Updates-%{DATE}.iso.
-P <size>	Split file into <size>-byte chunks. The <size> may be a number indicating the number of bytes to use, or one of the following presets: • bluray1 - Single Layer Blu-Ray Disc (25 GB) • bluray2 - Double Layer Blu-Ray Disc (50 GB) • bluray3 - 3-Layer XL Blu-Ray Disc (100 GB) • bluray4 - 4-Layer XL Blu-Ray Disc (128 GB) • cd - CD (700 MB) • dvd - DVD (4.7 GB)

-s <host>	Use <host> as your update server. Defaults to packages.amp.sourcefire.com.
-v	Increase output verbosity.

Example

```
> ./amp-sync all -X
```

fetch

Fetch update and content update data from a Cisco FireAMP update server.

Syntax

```
./amp-sync fetch [options]
```

Where [options] can be:

-D	Delete old database deltas. Must be used in combination with -M, in which case delta files earlier than the specified version will be deleted from the local system. Use this to reduce the storage space being used on your update host.
-M <seq>	Fetch deltas starting at sequence number <seq>. Use this option with the lowest sequence number needed across all of your FireAMP Private Cloud devices to reduce the amount of data fetched on a new update host.
-N	Fetch new snapshot. A full database snapshot is fetched the first time a fetch is done. Afterwards, only deltas are retrieved. Snapshots are loaded by a FireAMP Private Cloud device only when installing or restoring from backup. Use this option to refresh the snapshot available on your update ISO before installing or restoring a device.
-R	Resume. Try downloading a previously started download again, without checking the server for new content. Use this when you're using a slow network link and are having problems completing a full download.
-h	Display this help information.
-l <rate>	Limit download speed to <rate> bytes per second. Defaults to having no limit.
-s <host>	Use <host> as your update server. Defaults to packages.amp.sourcefire.com.
-x	Exclude Protect DB snapshot. Use this option to reduce the size of your download. An ISO generated with this option can only be used to update a Private Cloud device, not to install or restore.
-v	Increase output verbosity.

Example

```
> ./amp-sync fetch -R
```

package

Package fetched update data into an ISO file.

Syntax

```
./amp-sync package [options]
```

Where [options] can be:

-M <seq>	Package deltas starting at sequence number <seq>. Use this option with the lowest sequence number needed across all of your FireAMP Private Cloud devices to reduce the size of the generated ISO.
-X	Exclude Protect DB snapshot. Use this option to reduce the size of your ISO. An ISO generated with this option can only be used to update a Private Cloud device, not to install or restore one.
-h	Display this help information.
-o <file>	Output to <file> instead of %{PRODUCT}-%{VERSION}-Updates-%{DATE}.iso.
-P <size>	Split file into <size>-byte chunks. The <size> may be a number indicating the number of bytes to use, or one of the following presets: • bluray1 - Single Layer Blu-Ray Disc (25 GB) • bluray2 - Double Layer Blu-Ray Disc (50 GB) • bluray3 - 3-Layer XL Blu-Ray Disc (100 GB) • bluray4 - 4-Layer XL Blu-Ray Disc (128 GB) • cd - CD (700 MB) • dvd - DVD (4.7 GB)
-q	Run quietly.
-v	Increase output verbosity.

Example

```
> ./amp-sync package -o newfile.iso
```

verify

Verify downloaded update data.

Syntax

```
./amp-sync verify [options]
```

Where [options] can be:

-e	Exit early with an error on the first verification failure.
-h	Display this help information.
-q	Run quietly with minimal output.
-v	Increase output verbosity.

Example

```
> ./amp-sync verify -e
```

Appendix C
Supporting Documents

The following supporting documents are available for download.

Cisco FireAMP Private Cloud Console User Guide

The current version of the FireAMP Console User Guide can be downloaded here.

Download the User Guide

Cisco FireAMP Private Cloud User Guide

The current version of the Administration Portal User Guide can be downloaded here.

Download the Administration Portal User Guide

Cisco FireAMP Private Cloud Quick Start Guide

This guide walks through setting up groups, policies, and exclusions then deploying FireAMP Connectors. This guide is useful for evaluating FireAMP.

Download the Quick Start Guide

Cisco FireAMP Private Cloud Deployment Strategy Guide

This guide provides a more detailed look at preparing and planning for a production deployment of FireAMP along with best practices and troubleshooting tips.

Download the Deployment Strategy Guide

Cisco Endpoint IOC Attributes

The Endpoint IOC Attributes document details IOC attributes supported by the Endpoint IOC scanner included in the FireAMP Connector. Sample IOC documents that can be uploaded to your FireAMP Console are also included.

Download the Endpoint IOC Attributes

Cisco FireAMP Private Cloud Release Notes

The Release Notes contain the FireAMP change log.

Download the Release Notes

Cisco FireAMP Demo Data Stories

The Demo Data stories describe some of the samples that are shown when Demo Data is enabled in FireAMP.

Download the SFEICAR document

Download the ZAccess document

Download the ZBot document

Download the CozyDuke document

Download the Upatre document

Download the PlugX document

Download the Cryptowall document

Download the Low Prevalence Executable document

A

B

C

D

E

F

G

H

I

K

L

M

N

P

R

S

U

V