EndPoint Manager Quick Start Guide

Revision -

CLEARCUBE®

Technical Support

See the Support Web site for technical updates, additional warranty information and documentation, and software revisions:

Web: http://www.clearcube.com/support/

Email: support@clearcube.com

Phone: (512) 652-3400

(866) 652-3400

ClearCube Technology, Inc.

1505 Volta Drive, Suite 100

Cedar Park, TX 78641

E-mail info@clearcube.com

Phone: (512) 652-3500 or call toll free (866) 652-3500

Alternatively, contact your local ClearCube Reseller or Authorized Service Provider.

Copyrights

Trademarks

Patents

The ClearCube Architecture and its components described in this user manual are protected by numerous granted and pending U.S. and international patents. Granted patents include US05926172, US05966056, US05994952, US06012101, US06020839, US06037884, US06038616, US06119146, US06148182, US06167241, US06385666, US06421393, US06426970, US06633934, US06708247, US06735658, and US06886055.

Patents pending include: US S/N 09/755378, US S/N 10/279475, US S/N 10/198719, US S/N 10/198650, US S/N 10/409219, US S/N 09/728667, US S/N 09/728669, US S/N 10/411804, US S/N 10/411908, US S/N 10/458853, US S/N 10/364584, US S/N 10/301536, US S/N 60/411066, US S/N 10/662933, US S/N 10/662889, US S/N 10/662932, US S/N 10/662968, US S/N 10/301563, US S/N 10/662936, US S/N 10/301518, US S/N 10/662955 and US S/N 10/662954.

Direct all inquiries about patented technology to ClearCube Corporate Headquarters.

Contents

This Page Is Intentionally Blank

1. Introduction

Endpoint Manager (EPM) provides IT administrators one dashboard to monitor and control their entire deployment of local and remote computing assets: thin clients and blade PCs. Designed to scale from small businesses to large enterprises, ClearCube EPM gives IT departments total control by:

- Allowing endpoints to connect with server.
- Applying customized and default profiles to endpoints.
- Backup and apply OS images to thin clients.

2. Minimum Requirements and Support

The table below shows minimum requirements for EPM components and supported operating systems.

Table 1. Minimum requirements for EPM components and supported software

Component	Minimum Requirements and Supported Items	Recommended or Comments
EPM Server	2.4 GHz processor	Intel Core™ i7 1st generation or higher Xeon® 3400 series (4 cores) or higher
	3GB RAM	8 GB RAM or higher
	4GB free space	Free space according to the amount of images to be stored
	Separate FTP server for backups	Free space according to the amount of backups to be stored
EPM client	64 bit processor	Intel Core™ i7 1st generation or higher Xeon® 3400 series (4 cores) or higher
	2 GB RAM	8 GB RAM or higher
	2.4 GB free space for firmware + Space according to GuestOS	8 GB free space or higher
Hypervisor	VMware ESXi version 6.0.0	VMware ESXi version 6.5 or greater
Operating systems	Ubuntu 18.04	Supported on EPM server
	Windows 10 IoT	Supported on Thin Clients
	Windows 10 Pro	Supported on Thin Clients

Table 2. Ports used by EPM Appliance

PID	Program Name
3306	mysqld
53	systemd-resolve
22	sshd
9191	java
8080	java
22	sshd

3. Installation Prerequisites

The sections below give an overview of installation prerequisites and show important items to remember when deploying the server appliance.

4: Overview

EndPoint Manager server appliance comes with FTP server and MySQL database. To deploy the server appliance, upload the appliance Virtual Machine on a VMWare ESXi Hypervisor.

4.1: Device Discovery

To discover endpoints, **one** of the following methods must be configured:

1) DNS. An entry by the name of "**epmserve**r" must be made on the DNS server

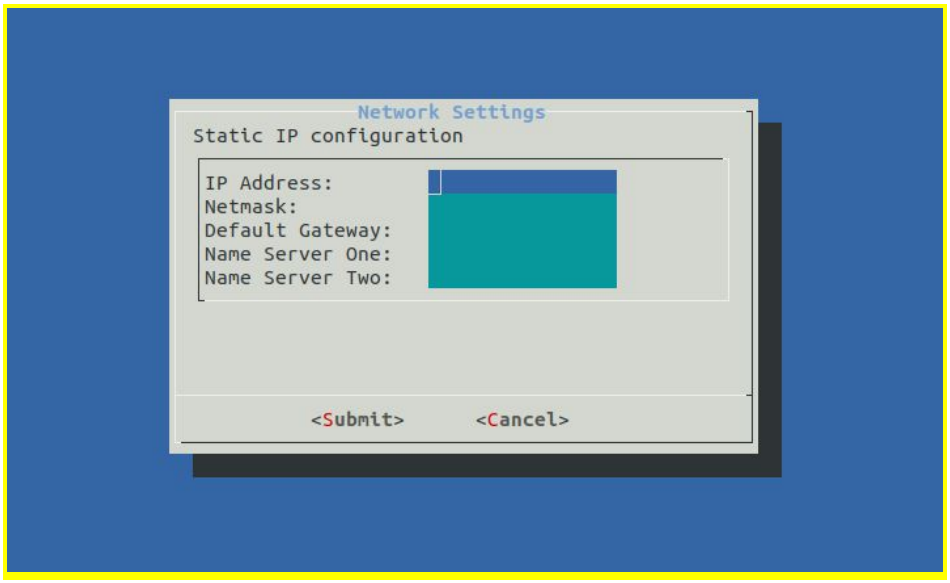
2) DHCP. An entry by the name of "**epmserver**" must be made on the DHCP

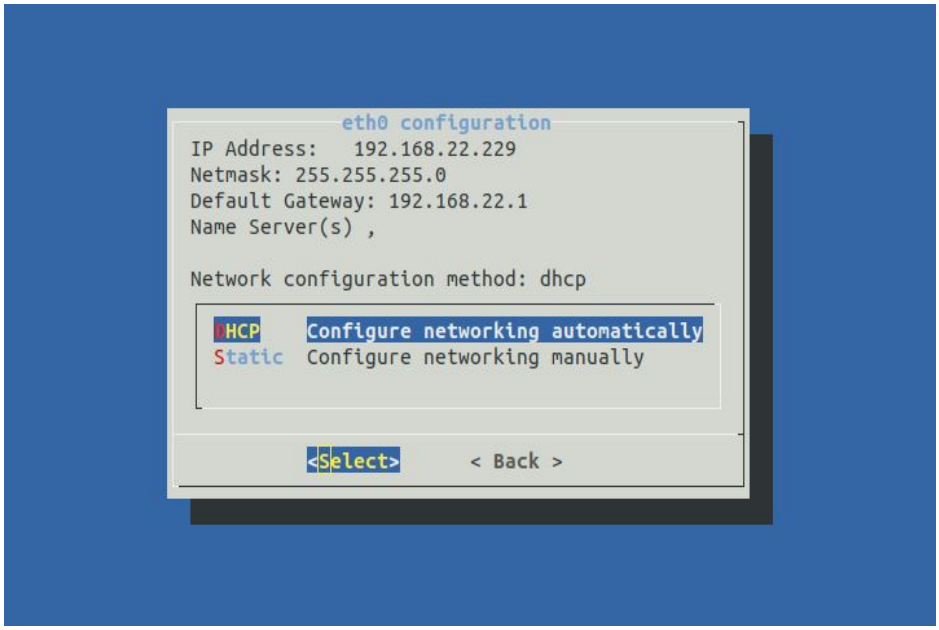
3) Broadcast discovery must be enabled on the network

4) Manually entering the IP onto the client firmware after entering the PIN (See sec: "9.1 Manual Server Discovery")

4.2: Manual IP configuration (Appliance)

Manual IP configurations can be done on the Appliance configurations screen accessible by the console view of Appliance on the VMware vSphere Client.





5: Accessing EPM Server

To access EPM server, open any browser type:

epmserver:8080

Or, for the full link, click on:

https://192.168.1.2

This will open the EPM server login page.

NOTE:	Both machines should be on same network and be accessible to each other

6: Using the EPM Administrator Account

EPM provides a default Administrator account. Use the Administrator account to log in to EPM for the first time, and configure settings such as password change.

After performing initial configurations, you can change the default settings. The steps below show how to log in using the default EPM account.

1. Go to Login page as described in the previous section.
2. Enter the default account credentials shown in the table below.

   Table 2. The Default EPM account credentials

Login Item	Value
Username	Administrator
Password	clearcube

3. Click **Login**.

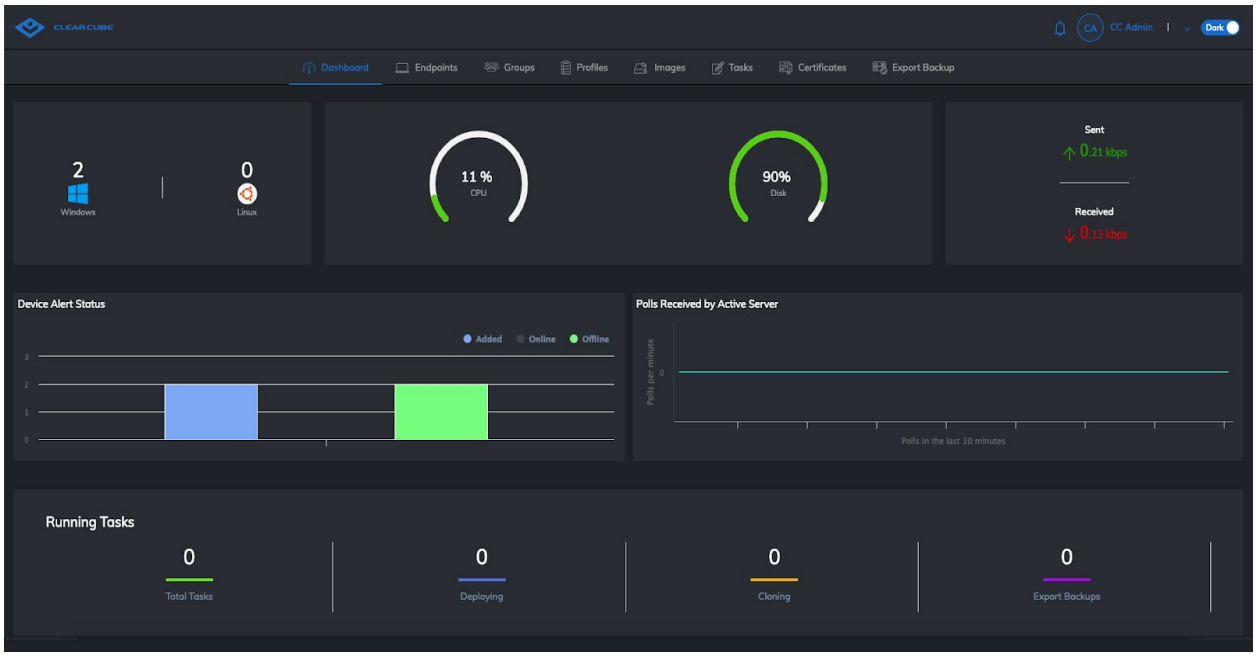
   Result: EPM displays the Dashboard.

7: Dashboard

Dashboard is the landing page of the EPM server. It shows summary of the following server data:

- **Online Endpoints** (Number of discovered endpoints that are online).

- **Device Alert Status** (Number of endpoints that are discovered, online and offline).
- **Polls Received by Active Server** (Number of polls sent by endpoints to EPM server).
- **OS Type** (OS types of endpoints currently discovered on EPM server).
- **Running tasks** (Same as Current tasks).
- **Disk Usage** (Amount of hard disk space on EPM server appliance).
- **Network Usage.**
- **CPU Usage.**



8: Configuring EPM

The Configurations field provides an overview of the main server configuration options. After logging in, open the configuration field by clicking **'Configurations'** on the top right corner. You can use the EPM Administrator account to login to EPM to configure EPM..

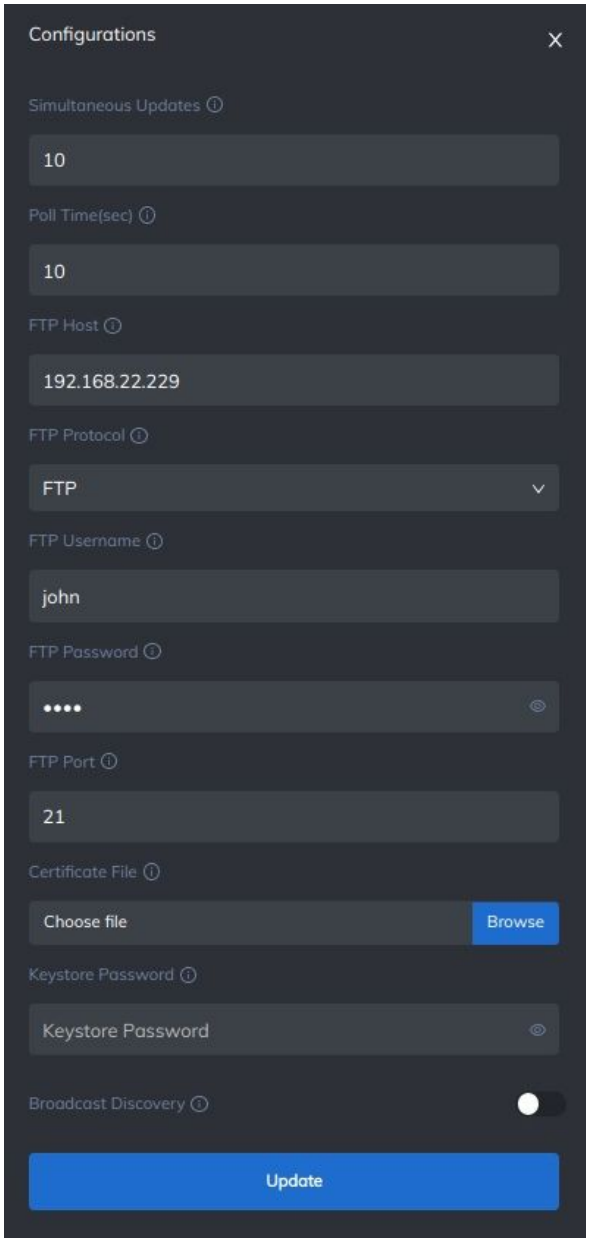


Figure 1. The Configurations field (displayed at Dashboard by clicking Configuration)

8.1: Configuration options

The table below shows settings for the database and FTP server. These fields are located in the Configuration of the top right menu.

Table 3. Configurations fields and options

Field	Description
Simultaneous updates	This is the number of clients that can be updated simultaneously. If this limit is reached, the remaining updates are queued to be executed later.

Poll time (sec)	Time interval after which clients send polls to server.
FTP host	Hostname/IP of FTP server. Export backups are saved on FTP server. ClearCube recommends using a static IP address.
FTP protocol	This is used to connect to the server that is dedicatedly used to store files.
FTP username	This field specifies the user name for the FTP server. The default value is **clearcube**.
FTP password	This field specifies the password for the FTP user. The default password is provided by EPM server appliance. Asterisks appear in place of the characters entered.
FTP port	Port of FTP server.
Certificate file	This field identifies the EPM server when running the TLS protocol. To provide the SSL certificate for the EPM server, it must be in PKCS12 format.
Keystore password	This allows the EPM server to extract the certificate information from the PKCS12 file.
Broadcast delivery	This detects and adds running EPM clients to the EPM server without the need for any user interaction.

NOTE: Database settings and FTP server settings are provided with server appliance.

8.2: User Management

EPM allows the user to change password for the Administrator account. The table below shows the settings for changing password.

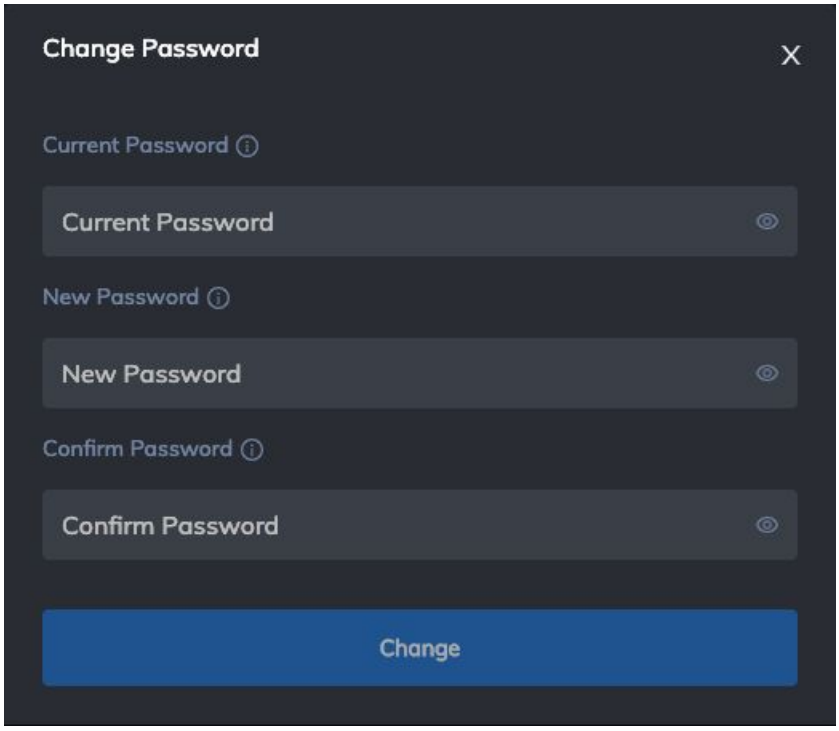


Figure 4. User Management tab

Table 5. Change password fields

Field	Description
Current Password	This field specifies current password of administrator account.
New Password	This field specifies new password. Enter the new password in this field.
Confirm New Password	This field confirms new password. Enter the same password as New Password field. Both passwords should match.

9: EPM Firmware Configurations

EPM allows you to perform certain important functions on endpoint firmware. Some of these functionalities are discussed below.

9.1: Manual Server Discovery

Endpoints discover the EPM server when they are on the same network. If server discovery fails, EPM allows you to manually enter server IP and poll it. To manually enter server IP (when broadcast discovery fails):

- Access an endpoint when EPM firmware is installed on it.
- A popup appears when discovery fails.
- Click **Enter Server IP** and click **OK.**

  Result: 'Server pin' popup appears.

- Enter server pin and click **OK.** *(Default pin: 123456)*
- Now enter server IP and click **OK.**

  Result: Endpoint discovers EPM server

9.2: Wi-fi configuration

EPM allows you to manually configure and connect to Wi-fi on firmware. To connect to a Wi-fi network:

- Press **Ctrl + Alt + W** on EPM firmware.
- Select the available network card.
- Click on Wi-fi network that you want to connect from the list of available Wi-fi networks.
- Enter Wi-fi Password.
- Click **Connect.**

  Result: Endpoint connects to the selected Wi-fi network.

NOTE:	You can disconnect the Wi-fi network and choose another one to connect to.

10: TLS in EPM

EPM facilitates secure communication with endpoints. EPM supports SSL security authentication which is enabled by default. ClearCube EPM provides a self-signed certificate with the appliance.

10.1: Generating Self Signed Certificates

Following commands can be used to generate a self signed certificate using openssl.

i. ***openssl genrsa -aes256 -out server.key 2048***

Above command is used for RSA key generation. User will be prompted to enter the pass-phrase for the key. After successful completion of this step a key file will be generated.

ii. ***openssl req -new -key server.key -sha256 -out server.csr***

Above command uses the generated key to generate a new csr file. User will be prompted to enter the pass-phrase for the key generated above. If the key entered is correct user would be required to enter further information. After successful completion of this step a csr file will be generated.

iii. **openssl x509 -req -days 365 -in server.csr -signkey server.key -sha256 -out server.crt**

Above command use the csr and key generated in step (i) and (ii) to generate -sha256 crt which has a validity of 365 days. User will be prompted to enter the pass-phrase for the key. After successful completion of this step a crt file will be generated.

iv. ***openssl x509 -in server.crt -out server.pem -outform PEM***

The above command generates a pem file using the crt file. After successful completion of this step a pem file will be generated.

v. ***openssl pkcs12 -export -in server.crt -inkey server.key -out server.p12 -name tomcat -CAfile server.crt -caname root -chain***

Above command generates a PKCS12 format p12 file using the crt and key generated above which has the alias tomcat. This file will be uploaded to the EPM Appliance. User will be prompted to enter the pass-phrase for the key. If key is validated user will be asked to enter export password. After successful completion of this step a p12 file will be generated.

NOTE:	You will have to use the password: clearcube1_ for all of the above commands

10.2: Generating Certificate Fingerprint

openssl x509 -in server.pem -noout -sha256 -fingerprint

Above command is used to get the fingerprint of the certificate generated in section 9.1.

10.3: Configuring DNS

You are required to manually make an entry by the name of "**epmserver**" on the DNS server. To add an entry in DNS server:

- Open the DNS server with administrative rights.
- In side menu, click the network name on which EPM server is deployed.
- Click **Actions** in the menu bar and select **Other New Record**.
- Select **Resource Record Type** as 'text' and click **Create Record**.

  Result: 'Create new record' popup appears.

- Enter '**epmserve**r' in Record name.
- Enter EPM certificate fingerprint (generated in Section 9.2) in '**Text**' field. It should be written in the following format:

  <some variable e.g. ClearCube> = <EPM SSL certificate fingerprint>

- Click **Done.**
- Discover all endpoints from EPM server.

  Result: All communication between EPM server and endpoints is secured

NOTE:	The fingerprint/key entered in DNS server should match with the one present in EPM server appliance. If the entries do not match, then a certificate error message shows on endpoints.

10.4: Adding Certificate to EPM Appliance

- Connect to the appliance using any FTP client using the appliance IP.
- Replace the .p12 file generated as the result of Setcion 9.2 in the folder.
- Reboot the Appliance.

11: Basic Operations

The section shows basic tasks you can perform after configuring the EPM Server.

11.1: Image Backups

EPM server allows administrators to backup OS images of Endpoints. Image backups are saved in Images on the server. The steps below show how to backup an OS image:

1. Go to **Groups** and select a client.
2. Select the End point by clicking on the the check box on the left corner.
3. From the Menu, Select **More >> Backup Image.**

   Result: Backup image popup opens. The image below shows '**Backup image**' popup.

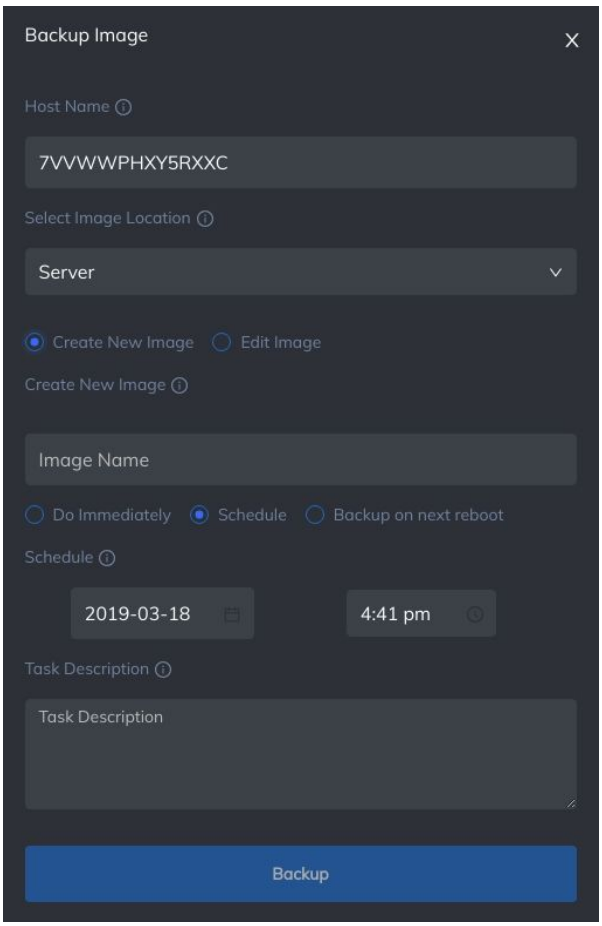


Figure 4. Backup Image popup

4. Complete the fields in the Backup Image Dialog. After completing the fields, click **Schedule** to schedule an image backup. You can choose to backup immediately by clicking **Do Immediately.**

NOTE:	You will have to restart the client (manually or from EPM server) for image backup process to start.

The table below shows description of all fields in Image Backup popup.

Table 8. Backup Image fields

Field	Description
MAC Address	This field specifies MAC address of the endpoint selected for image backup.
Image Location	Location for the backup image. The image can be saved remotely on the server or locally on the endpoint.
Create New Image	This option specifies that image backup will be saved as a new image in inventory. If you select this option, add a name in Image name field.
Edit Image	Edit and overwrite an existing image from image inventory.
Image Name	Name of the backup image file.
Schedule	Date and time for the backup process to start.
Task Description	Information about the Task being created.
Do Immediately	Immediately start image backup.

5. You can now view the scheduled tasks in the Schedule Screen.

11.2: Change Image

EPM server allows administrators to remotely change/update an OS image on a Thin client. You can either redeploy the same image on the client or change an image from Image inventory. To change an image, go to **Groups** and select a client. Click **More >> Change image.**

The steps below show how to change/update an OS image:

1. From the Menu, Select **More>>Change Image.**

Result: Change Image Dialog opens.

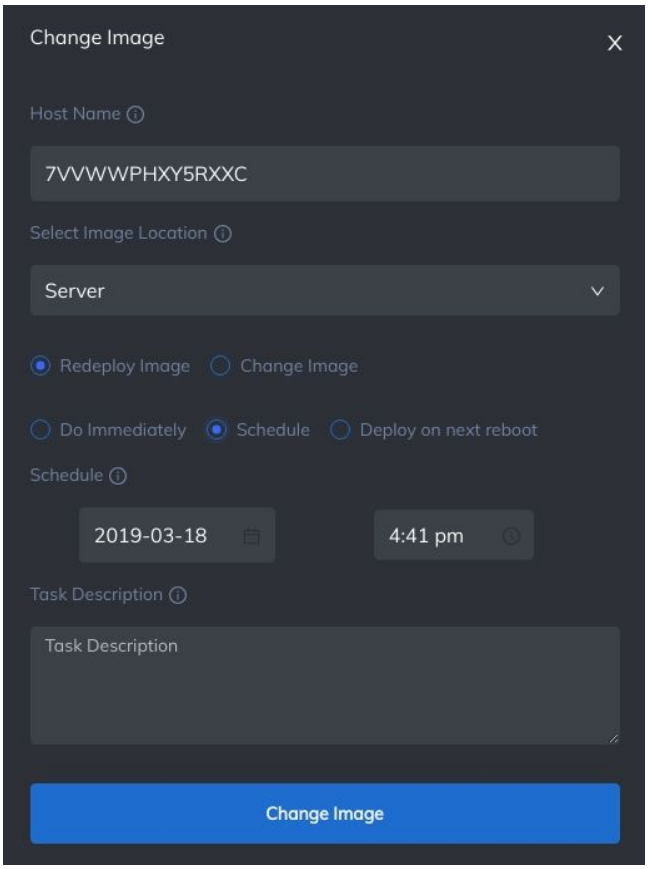


Figure 5. Change Image popup

2. Complete the fields in the Change Image Dialog. After completing the fields, click **Change Image** to continue.

The table below shows all fields.

Table 8. Backup Image fields

Field	Description
Image Location	Location for the backup image. The image can be saved remotely on the server or locally on the endpoint.
Redeploy Image	Selecting this property would redeploy an already deployed image.
Change Image	Selecting this property would replace the existing image with a different selected image.
Image Name	Select the image file to be deployed in place of the existing Image.

Schedule	Date and time for the change image process to start.
Schedule Description	Information about the Schedule being created.
Do Immediately	Selecting this property would Immediately start image change process.
Deploy on next reboot	If this property is selected, the new image would be deployed on the next device reboot.

3. Finish the process by clicking **Change Image.** Image would be changed according to the selected schedule and options.

11.3: Update Firmware

The user can update the firmware of a client from the EPM server. This is done to update EPM's own client software in case of updates and/or feature addition.

Select the client and click on the menu that displays the drop down option. From there, you can update the firmware.

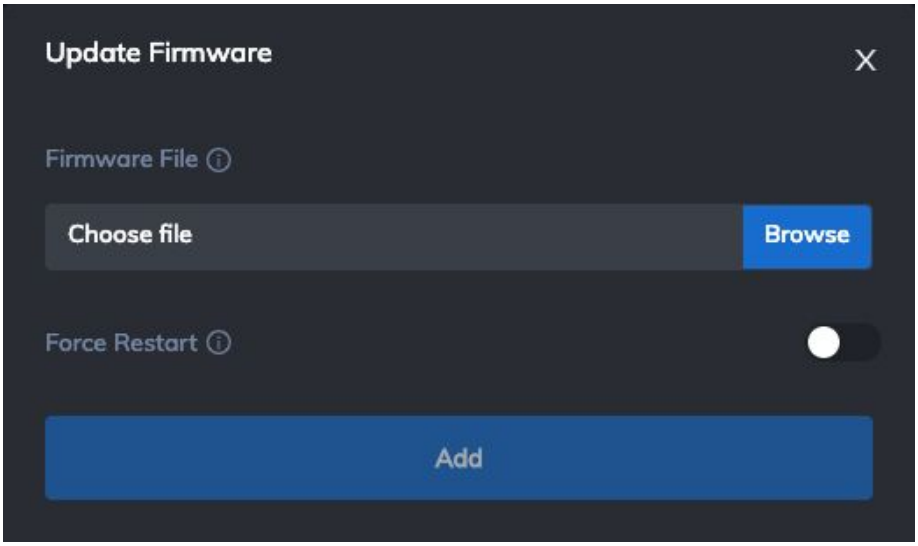


Figure 6. Update Firmware popup

Table 7. Update firmware fields

Field	Description

• **Firmware File**	Select the location for the firmware file.
• **Force Restart**	Select this option if you want to force restart the endpoint.

11.4: Restart Client

EPM server allows you to remotely restart/reboot endpoints. To restart an endpoint, go to **Groups** and sele8ct a client. Click **'Restart'.** A Restart task will be created and the device will restart immediately.

NOTE:	Only those endpoints can be restarted whose status is '**Online/Logged in**'.

11.5: Take Screenshot

EPM allows you to remotely capture a screenshot of the current state of an endpoint. Select an endpoint, scroll to the right, click on the **Actions** menu, and select **Screenshots**. This will capture the screenshot which can be viewed by clicking the **'View'** button in the screenshot column.

NOTE:	Screenshots are available for only those clients can whose status is '**Online/Logged in**'.

11.6: Server Backups

EPM allows you to export Server backups and import them on EPM server to restore data. To export server data, go to **Configurations >> Backup/Restore** (as discussed in sec 7.2 Backup/Restore). Choose the backup type you want to export and then click **'Export'**. A disk space confirmation popup will appear. Click **OK** to start backup.

Server backup progress can be viewed in **'Export backup'** tab.

11.7: Certificates

EPM server enables secure communication with clients. EPM supports TLS and 802.1x security authentications. EPM allows the user to upload certificates using the Certificates tab. EPM SSH certificate can be updated and pushed to endpoints from this screen. To upload a certificate perform the following steps:

1. Upload the Certificate on EPM server by going to **Certificates >> Add certificate**.
2. On clicking **Add Certificate,** the following popup appears.

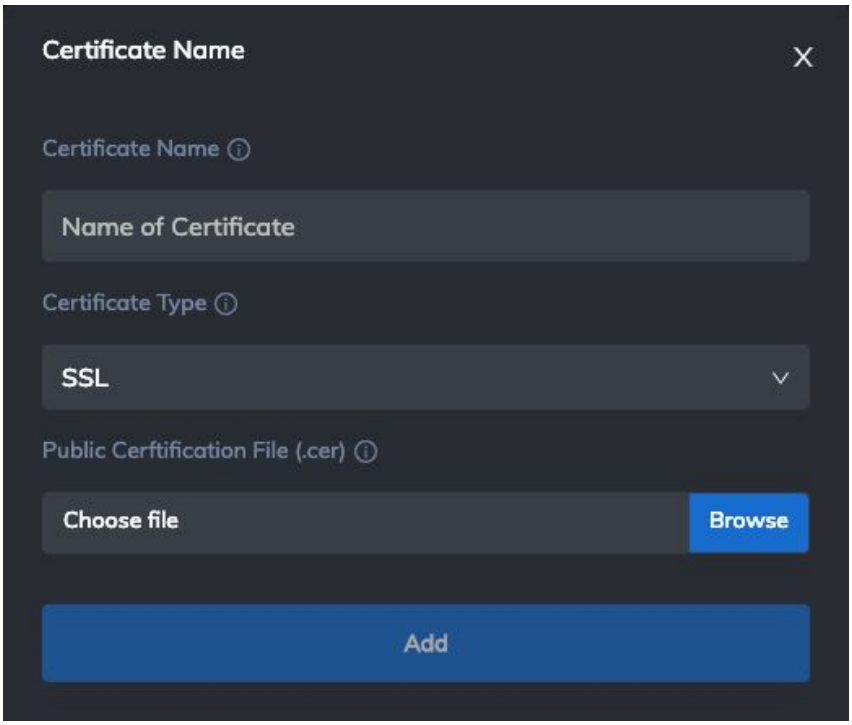


Figure 7. Add Certificate popup

3. Complete the data required in the table below and click Add.

Table 8. Add Certificate fields

Field	Description
• Certificate Name	Enter a certificate name. This will be referenced while creating profiles.
• Certificate Type	This field specifies type of the certificate. Options include: • SSH • 802.1x Authentication
• Public Certification File (.cer)	Select the Location for EPM Server's public SSL certificate (.cer file).

• 802 Username	Enter identity string for 802.1x EAP.
• 802 Password	Enter password string for 802.1x EAP.
• 802 Domain	Enter Domain name for 802.1x EAP.
• 802 Authentication	Enter space-separated list of accepted 802.1x EAP methods (MD5, MSCHAPV2, PEAP, TLS)
• 802 Encryption	Enter Inner authentication with TLS tunnel (EAP-PEAP, EAP-TTLS)
• 802 CA	Select a Certificate file (.cer/.pem/.der/.pfx). You can have one or more trusted CA certificates. If CA certificate is not included, server certificate will not be verified. This is insecure and CA file should always be configured.
• 802 Private Key	Select path to client private key file (.cer/.pem/.der/.pfx). In this case, both the private key and certificate will be read from the PKCS#12 file.
• 802 Client	Select file path to client certificate file (PEM/DER).

12: Device Discovery

All devices/endpoints must be discovered on your EPM server to perform any management operations. Thin clients and blade agents and automatically discovered. Broadcast discovery is enabled on EPM server by default. After discovering endpoints, EPM displays them in groups. All discovered endpoints appear in default group. You can create more groups and move endpoints in other groups.

Client discovery can be done in the following ways:

1) via DNS (an entry by the name of "**epmserver**" has to be made on the DNS server)

2) via DHCP

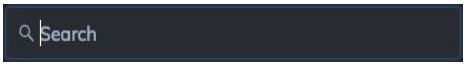
3) Broadcast discovery (it only works if the above two do not work and the clients are on the same subnet as the server).

4) Manually type server IP onto the client firmware after entering the PIN.

In order to view discovered clients, click on **Groups** and then select the group that you want to open and view devices.

NOTE:	After the first deployment, all discovered endpoints will appear in default group.

13: Search Options

EPM enables you to search for devices and relevant data on every screen. It uses wildcard search technique in every screen to maximize search results. To search data from any screen/tab, go to that screen and search for data by clicking on Search input field 

on the top right corner.

Result: Search results will appear in the table.

14: Configuring Endpoints Using Client Profiles

The sections below show how to configure EPM endpoints (thin clients and blade agents) using Client Profiles.

14.1: About Client Profiles

Client profiles enable administrators to apply a device-level configuration to groups of endpoints through a RESTful API call, rather than configuring clients individually. Profiles configuration contains the following settings:

- Profile name
- Security Settings
- Application settings
- Autostart settings

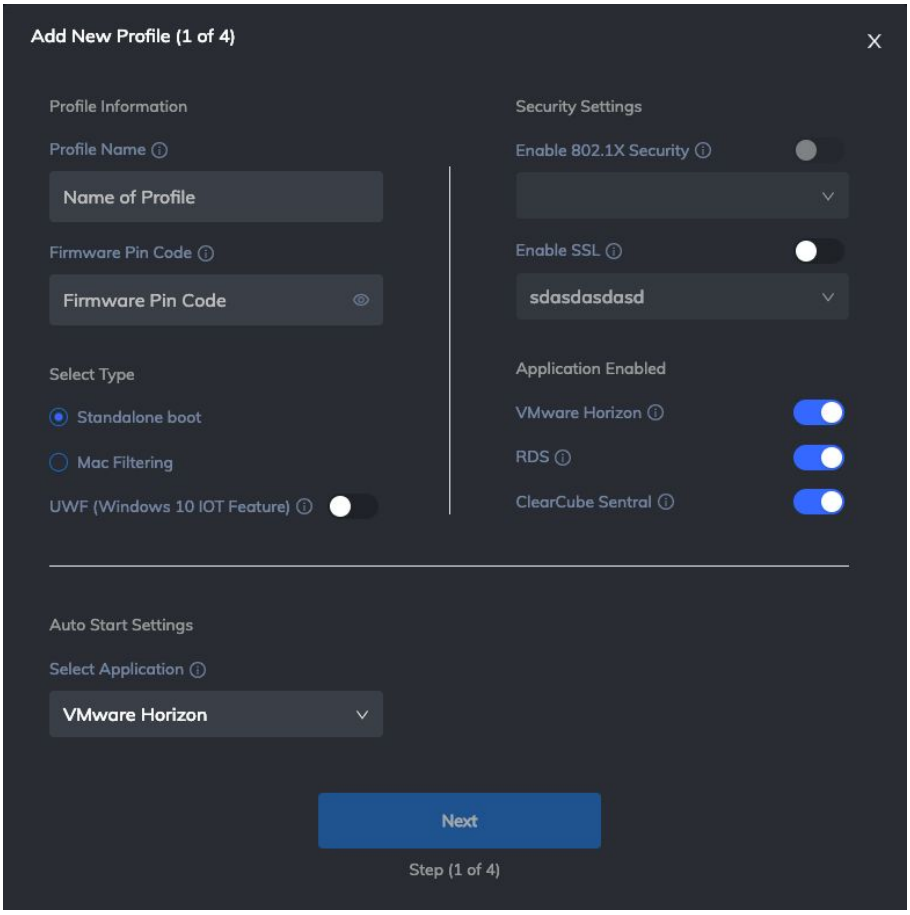


Figure 8. Add Profile popup

Table 9. Add Profile fields

Field	Description
Profile Information Section	
Profile Name	Type a name for this profile.
Firmware Pin Code	Set an administrator pin code for the firmware.
Standalone boot	When this property is selected, the endpoint is allowed to boot as a standalone device independent of the server.
MAC Filtering	When this property is selected, Mac filtering is enabled. The endpoint needs to be allowed on the server to boot.
UWF (Windows 10 IOT Feature)	When this property is enabled UWF. If supported on the endpoint OS, it is enabled.
Security Settings	
Enable SSL	Select this option to enable SSL authentication for communication between EPM Server and endpoints.

Enable 802.1x Security	Select this option to enable 802.1x encryption.
Applications Enabled	
Applications Enabled	This pull-down menu specifies which applications should be enabled on the endpoint. Options include: ● VMware Horizon ● RDS ● ClearCube
Autostart Settings	
Select Application	This pull-down menu specifies the application that would initiate automatically on the endpoint upon startup. Options include: ● VMware Horizon ● RDS ● ClearCube ● None

14.2: Auto-start settings in Profiles

This section shows settings for applications that can be enabled in Profiles. EPM allows the clients to automatically start selected application on reboot. The settings for these applications can be configured in Profiles. EPM allows the following applications to auto-start remotely:

- VMware
- RDS
- ClearCube Sentral

NOTE:	Auto-start settings are only pushed to applications that are selected to auto-start on reboot.

14.2.1: VMware Horizon Client Settings

This table shows the VMware Horizon Client Settings.

Table 9. VMware Settings fields

Field	Description
SSL verification mode	This pull-down menu specifies the SSL Verification Mode to use. It includes the following options: ● Reject if any verification fails. ● Warn but allow self-signed connections. ● Perform no verification check.
All monitors	Selecting this property would hide the host operating system and open the Horizon Client UI in full screen mode on all monitors that are connected when the client is launched.
Auto Connect to server	When this property is selected, VMWare Horizon Client would automatically connect to the server used.
URL Horizon Server	Sets the URL for Horizon Server.
VMware Server Username	Sets the user name that Horizon Client uses for all connections. For kiosk mode, the account name can be based on the client's MAC address, or it can begin with a recognized prefix string e.g. custom-***
VMware Server Password	Sets the password that Horizon Client uses for all connections and adds it to Password field in the authentication dialog box if View Connection Server accepts password authentication.
VMware Server Domain	Sets the domain name that Horizon Client uses for all connections and adds it to Domain Name field in the authentication dialog box.
Auto Connect VM	If this property is selected the client would automatically connect to the last View desktop. In the text field, you can specify which desktop to use when user has access to multiple desktops.
Allow Send Ctrl+Alt+Del to Local	Selecting this property would send the key combination Ctrl+Alt+Del to client system rather than opening a dialog box to prompt the user to disconnect from view desktop.
Allow Send Ctrl+Alt+Del to VM	Selecting this property would send the key combination Ctrl+Alt+Del to the virtual desktop rather than opening a dialog box to prompt the user to disconnect from view desktop.
Kiosk mode	Select this property to authenticate Horizon client to use kiosk mode account.
Reconnecting VM in case of error	If this property is selected, the Horizon Client would retry connecting in case of an error.
Show Menu Bar	Select this property to suppress Horizon client menu bar when user is in full screen mode.

14.2.2: RDS Settings

This section shows how to configure RDS settings for auto-start mode. These settings will automatically be applied when a client with this profile reboots. The table below shows each field for RDS settings.

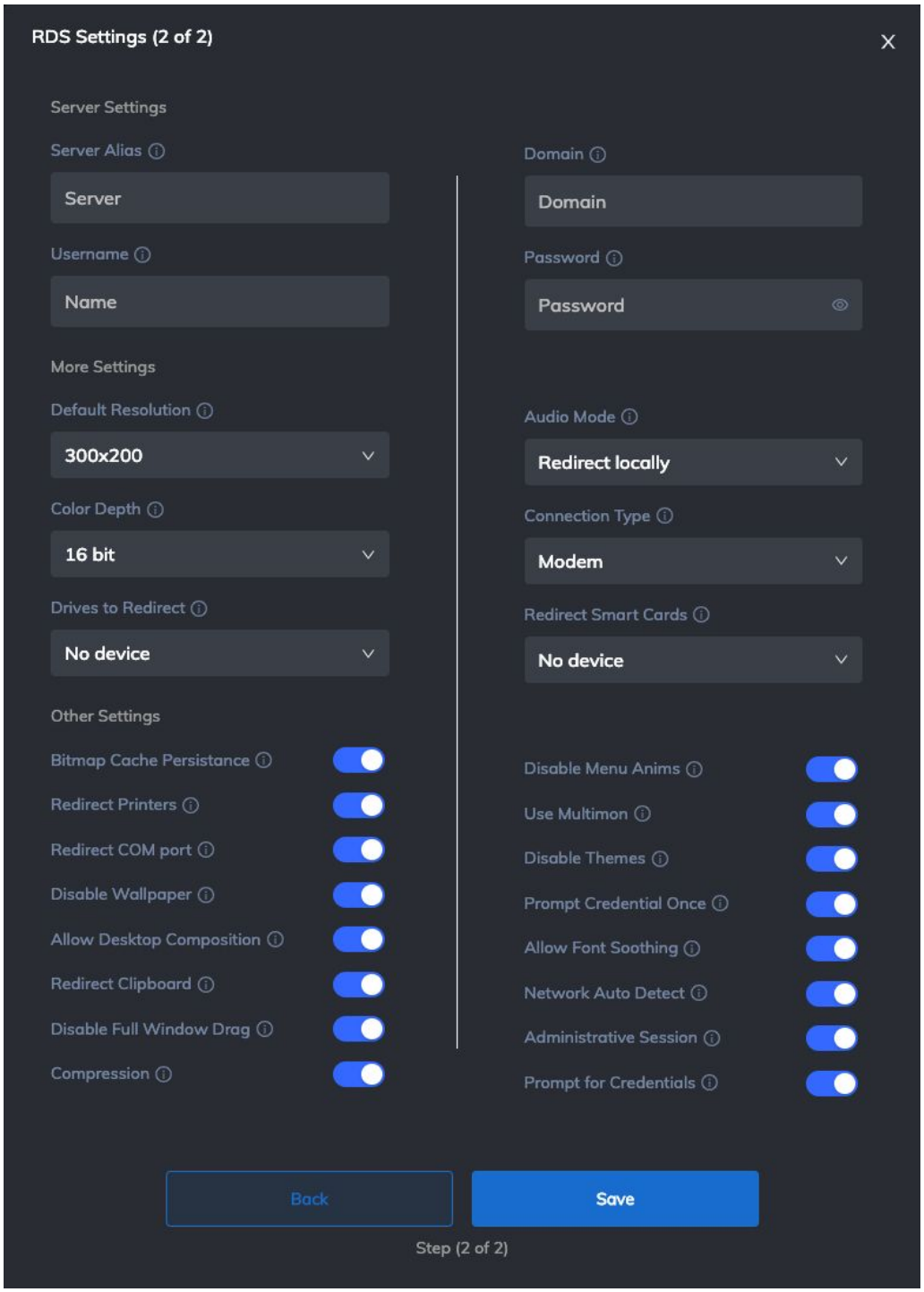


Figure 9. RDS Settings

Table 11. RDS Settings fields

Field	Description
Server Alias	Allows you to enter Alias for the Server.
Username	Specifies the name of the user to log in to the remote device.
Password	Specifies the password for the user that logs in to the remote device.
Domain	Specifies the Domain to log in to for the session.
Default Resolution	Set the default resolution for the remote session.
Bitmap Cache Persistence	Determines if bitmap caching occurs on the local computer (disk-based cache). Bitmap caching can improve the performance of your remote session. 0 – Do not cache bitmaps. 1 – Cache bitmaps.
Redirect Printers	Makes printers configured on the thin client available in remote sessions. 0 – The local printers on the thin client are not available on the remote host computer. 1 – The local printers on the thin client are available on the remote computer.
Redirect COM port	Makes COM ports configured on the thin client available in the remote session. 0 – The local COM ports on the thin client are not available on the remote host computer. 1 – The local COM ports on the thin client are available on the remote computer.
Audio Mode	Determines how audio output is handled when the thin client is connected to a remote computer. 0 – Play sounds on the thin client. 1 – Play sounds on the remote computer. 2 – Do not play sounds.
Disable Wallpaper	Determines whether the desktop background is displayed in the remote session. 0 – Display wallpaper. 1 – Do not display wallpaper.
Allow Desktop Composition	Determines whether desktop composition (needed for Aero) is permitted when you log on to the remote computer. 0 – Disable desktop composition in the remote session. 1 – Desktop composition is permitted.
Disable Menu Anims	Determines if menu and window animation effects occur in the remote session. 0 – Menu and window animation is permitted.

	1 – Menu and window animation is not permitted.
Prompt Credential Once	Determines whether Remote Desktop Connection prompts for credentials when connecting to a remote computer for which credentials were previously saved. 0 – Use the saved credentials and do not prompt for credentials. 1 – Prompt for credentials.
Network Auto detect	Automatically detects network characteristics and optimizes user experience accordingly. 0 – RDP does not detect any network settings. 1 – RDP automatically detects the best network settings.
Color Depth	Specifies the color depth of the remote session. Select 15-bit, 16-bit, 24-bit, or 32-bit.
Drives To Redirect	Determines which local thin client disk drives are redirected and available in the remote session. No Drives – Do not redirect any drives * – Redirect all disk drives, including drives connected later. Dynamic Drives – Redirect any drives that are connected later.
Redirect Smard Cards	Specifies if smart cards are redirected and available in a remote session. 0 – Smart card on thin client is not available in remote session. 1 – Smart card on thin client is available in the remote session.
Compression	Determines whether the connection should use bulk compression. 0 – Do not use bulk compression. 1 – Use bulk compression.
Use Multimon	Determines whether the session should use true multiple monitor support when connecting to the remote computer. 0 – Do not enable multiple monitor support. 1 – Enable multiple monitor support.
Connection Type	Specifies predefined performance settings for the Remote Desktop session. 1 – Modem (56kbps) 2 – Low-speed broadband (256 kbps – 2 Mbps) 3 – Satellite (2 Mbps – 16 Mbps with high latency) 4 – High-speed broadband (2 Mbps – 10 Mbps) 5 – WAN (10 Mbps or higher with high latency) 6 – LAN (10 Mbps or higher) 7 – Auto detect When selected, this option changes multiple performance-related settings (themes, animation, font smoothing, etc.). This setting is superseded by any changes to the individual settings. See the RPC GUI's Experience tab for list of individual settings that are affected.
Allow Font Smoothing	This setting determines whether font smoothing is used in the remote session.

	0 – Disable font smoothing in the remote session. 1 – Permit font smoothing.
Disable Full Window Drag	Determines whether window content is displayed when you drag the window to a new location. 0 – Show the contents of the window while dragging. 1 – Show an outline of the window while dragging.
Disable Themes	Determines whether themes are permitted when you log on to the remote computer. 0 – Themes are permitted. 1 – Disable theme in the remote session.
Redirect Clipboard	Determines whether the thin client clipboard is redirected and available in the remote session, and the same for the remote computer's clipboard. 0 – Do not redirect the clipboard. 1 – Redirect the clipboard.
Prompt For Credentials	Determines if Remote Desktop Connection requests credentials when connecting to a remote computer for which the credentials were previously saved. 0 – Use the saved credentials and do not prompt. 1 – Prompt for credentials.
Administrative Session	Connect to the administrative session of the remote computer. 0 – Do not use the administrative session. 1 – Connect to the administrative session.

14.2.3: ClearCube Sentral Settings

This section shows how to configure ClearCube Sentral settings for auto-start mode. These settings will automatically be applied when a client with this profile reboots. The table below shows each field for Sentral settings.

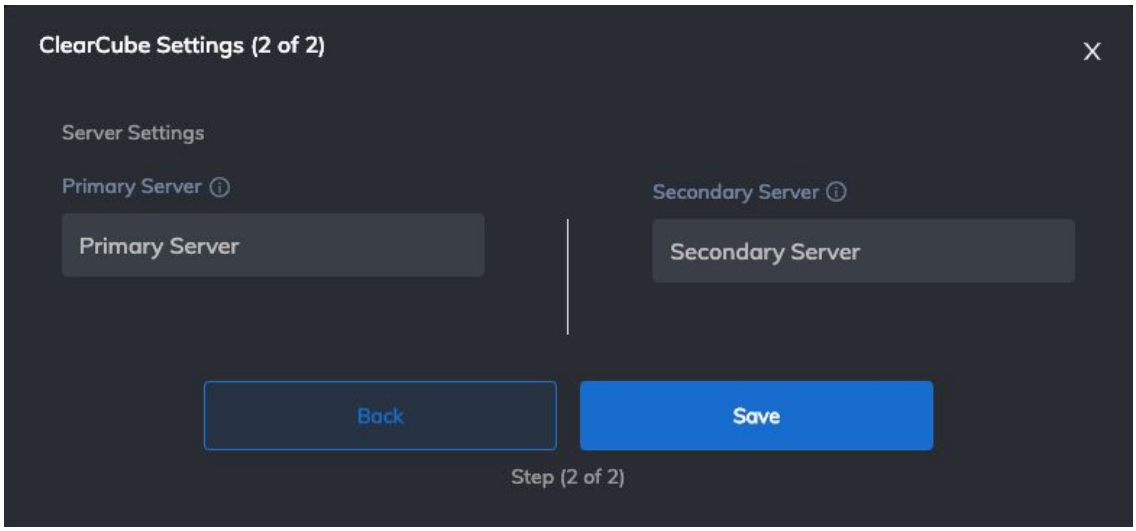


Figure 10. ClearCube Settings

Table 12. ClearCube Settings fields

Field	Description
Primary Server	Enter ClearCube Sentral primary server IP in this field.
Secondary Server	Enter ClearCube Sentral secondary server IP in this field.

14.3: Default Profile

EPM applies a client profile whenever a new endpoint is discovered. This profile is present in the server by default and applied to Default group. You can add a new profile (see sec 15.1 "Create a New Profile") and apply it to groups.

NOTE:	You cannot edit or delete a default profile.

14.4: Create a New Profile

If you have specific configuration requirements for groups of endpoints (for example, clients used in particular locations, or for types of users), you can create custom profiles for those devices. Create a new group for these devices, add the devices to the group, and then apply a custom profile to the group. It will be pushed to all of the devices in the group. You can apply a profile to any number of device groups (multiple groups can use the same profile).

Create a New Profile

1. From the side menu, click **Profiles > Add Profile**.

   Result: The 'Add Profile' popup appears.

2. Complete the profile fields and then click **Save**. See 14.1 "About Client Profiles" above for details about all Profile field descriptions.

   Result: A success message appears. Profile has been added.

14.5: Apply a Profile to a Group

This section shows how to apply a profile to an existing group. To apply a profile to a new group (see sec 16.1 "Creating a new group")

1. From the side menu, click **Groups.**
2. Select a group and click **Edit Group.**

   Result: Edit New Group popup appears

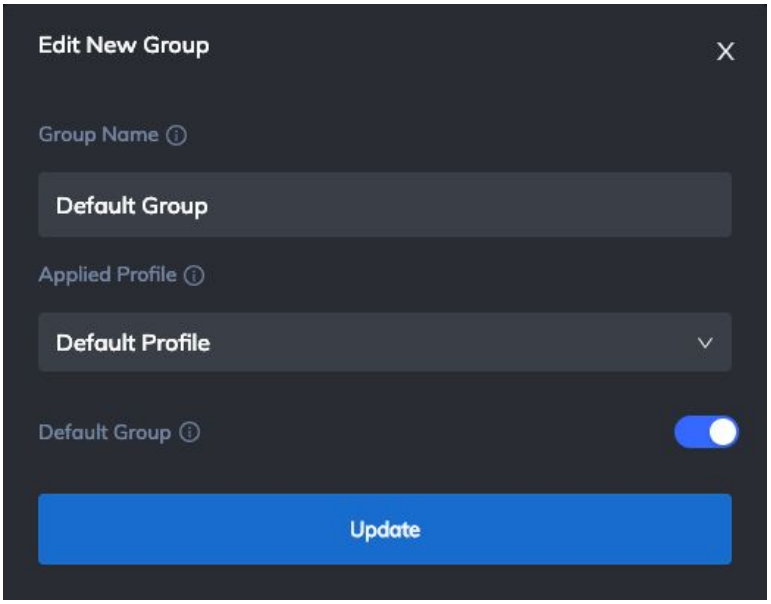


Figure 11. Edit New Group popup

3. Click on **Applied Profile** dropdown.
4. From the applicable profile names in the dropdown, select the name of the name of the profile which you want to apply.
5. Click **Update.** A success message appears at the bottom of the popup indicating that changes have been saved.
6. Reboot all endpoints in edited group to apply the profile.
7. In order to verify that profile has been applied, view Notifications in top right corner.

NOTE:	Profile applies to both Firmware and Guest OS. The notifications appear in same order.

14.6: Deleting a Profile

EPM allows you to delete profiles. To delete a profile:

1. Go to **Profiles.**
2. Select a profile and click **Delete Profile.**
3. A confirmation popup appears. Click **OK.**

   Result: A success message appears and selected profile is deleted.

You can also delete multiple profiles by selecting them together.

NOTE:	Profile(s) applied on group(s) cannot be deleted.

15: Groups (Required for all Management tasks)

In EPM server, endpoints are managed through groups. After discovery, endpoints are added in Default Group (see sec 16.2 "Default Group"). Endpoints must be in an EPM group for all management tasks. The list of groups is accessible from the **Groups** menu**.**

The table below shows description of all columns in **Groups** screen.

Table 13. Groups fields Description

Field	Description
MAC Address	This column shows physical MAC address of endpoint.
MAC Access	This column shows whether an endpoint is allowed to connect to serve or not. Its value can be 'Allowed' or 'Denied' (see sec 17.2 "Change Permissions")

Firmware/Client version	This column shows the current firmware version of an endpoint.
Guest OS	This column shows the current Guest OS type on an endpoint.
IP Address	This column shows current IP address of an endpoint.
Status	This column shows current status of endpoint. Status can be: ● Online/Logged In ● Online/Logged Off ● Connecting ● Offline
Last Poll	This column shows the Last poll sent by endpoint to EPM server. To view Last poll, hover over **Details.**
Current Image (Version)	This column shows the OS image and its version that is currently deployed on endpoint.
Applied Image (Version)	This column shows the OS image and its version that is queued to be deployed on endpoint.
Screenshot	This column shows current shows last captured screenshot os endpoint (see “11.5: Take Screenshot”)
Services	This column shows the list of services currently running on an endpoint. Services can only be viewed for Windows Guest OS.
Host Name	This column shows the hostname of endpoint.
Log File	This column shows a file containing endpoint logs from when it is connected with the EPM server.

15.1: Creating a new Group

To create a group:

1. From the side menu, click **Groups.**
2. Select **Add New Group.**

   Result: Create New Group popup appears. Add group field descriptions are mentioned below.

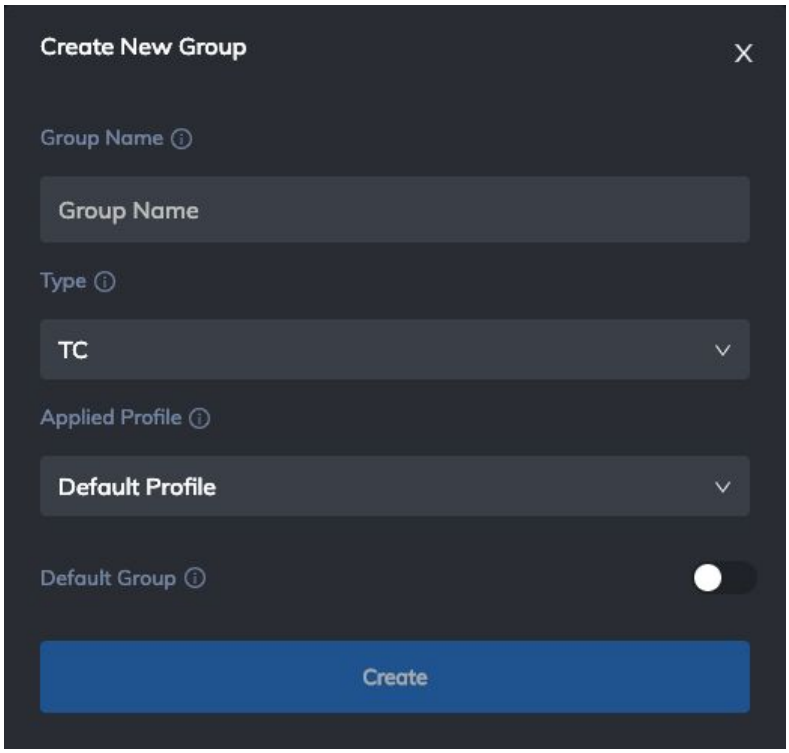


Figure 12. Create New Group popup

3. Complete the Group Name, Group Type, Applied profile fields, and then click **Add.**

   Result: Group is added. Selected profile will apply when endpoint(s) in that group reboot.

4. You can also make a group default by checking **Mark this group default** see sec 16.2 "Default Group"

Table 13. Add Group fields

Field	Description
Group Name	This field specifies the group name that you want to choose.
Group Type	This field specifies group type according to the endpoint(s) in that group.

Applied Profile	This dropdown field specifies profile that will apply on the group. This list comes from **Profiles** tab.

15.2: Default Group

EPM displays all endpoints in groups. All discovered endpoints appear in default group. The Default Group is already present when the EPM server is deployed. A default group cannot be deleted. You can add a new group and make it Default.

To make a group Default:

1. Go to **Groups.**
2. Select a group and click **Edit Group.**
3. Select **Mark group as default.**
4. Click **Update.**

   Result: A success message appears and selected group is marked as Default.

You can also verify this in **Groups** list. The value for Default Group column is **True** for a default group.

15.3: Deleting a Group

EPM allows you to delete a group. To delete a group:

5. Go to **Groups.**
6. Select a group and click **Delete Group.**
7. A confirmation popup appears. Click **OK.**

   Result: A success message appears and selected group is deleted.

You can also delete multiple groups by selecting them together.

NOTE:	- When a group is deleted, all its endpoints move to Default Group. - Default group cannot be deleted.

16: Managing a Client in Group

All management tasks in EPM are done by adding endpoints in Groups. To access a group, click **Groups** in side menu and select a group from the list in side menu. Following is a description of tasks that can be performed by adding clients in Groups.

16.1: Change Group

You can move an endpoint from one group to another. When an endpoint moves to a new group, the profile applied to that group is pushed to endpoint. New profile applies when endpoint reboots. To move an endpoint from one group to another:

1. In side menu, click **Groups/**
2. Side menu expands, select a group.
3. Click on an endpoint in that group and click **Change Group.16.3: Delete Client**

   Result: Change group popup appears.

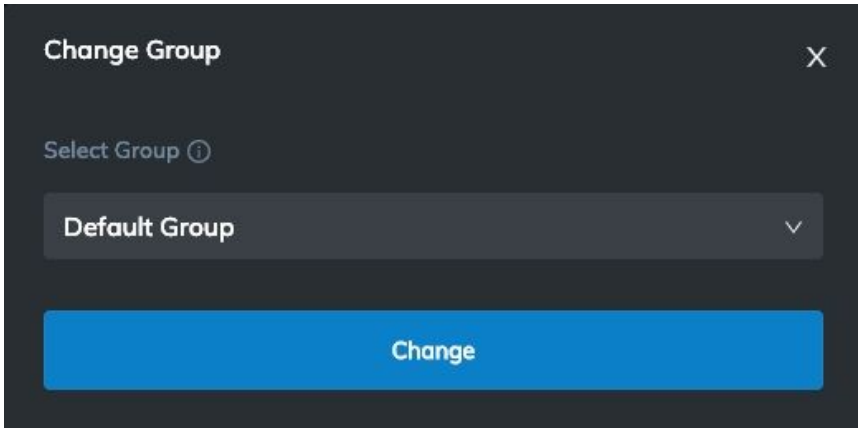


Figure 13. Change Group popup

4. In the Groups dropdown, select the client that you want to move the endpoint to.
5. Click **Update.**

   Result: Success message appears and endpoint moves to new group.

16.2: Change Permissions

'Change permissions' settings apply on an endpoint when MAC filtering is enabled in Profiles (see "15.1 About Client Profiles"). These settings determine on discovery, whether an endpoint is allowed or denied to connect with EPM. To allow/deny an endpoint, select the endpoint and click **Change Permissions.** Change the permissions and click **Apply.**

Result: Permissions apply accordingly.

16.3: Delete Client

You can delete an endpoint from a group. To delete an endpoint, select it and click **Delete Client.** This will delete the client from that group. However, when the client reboots, it will appear in Default group.

17: View All Endpoints

EPM allows you to view all discovered endpoints in one screen. To view discovered endpoints click **"All Endpoints"** from the menu. This shows the list of all endpoints. When the user clicks on the endpoint row, they are navigated to the endpoints list in the corresponding Group. The selected endpoint row is highlighted.

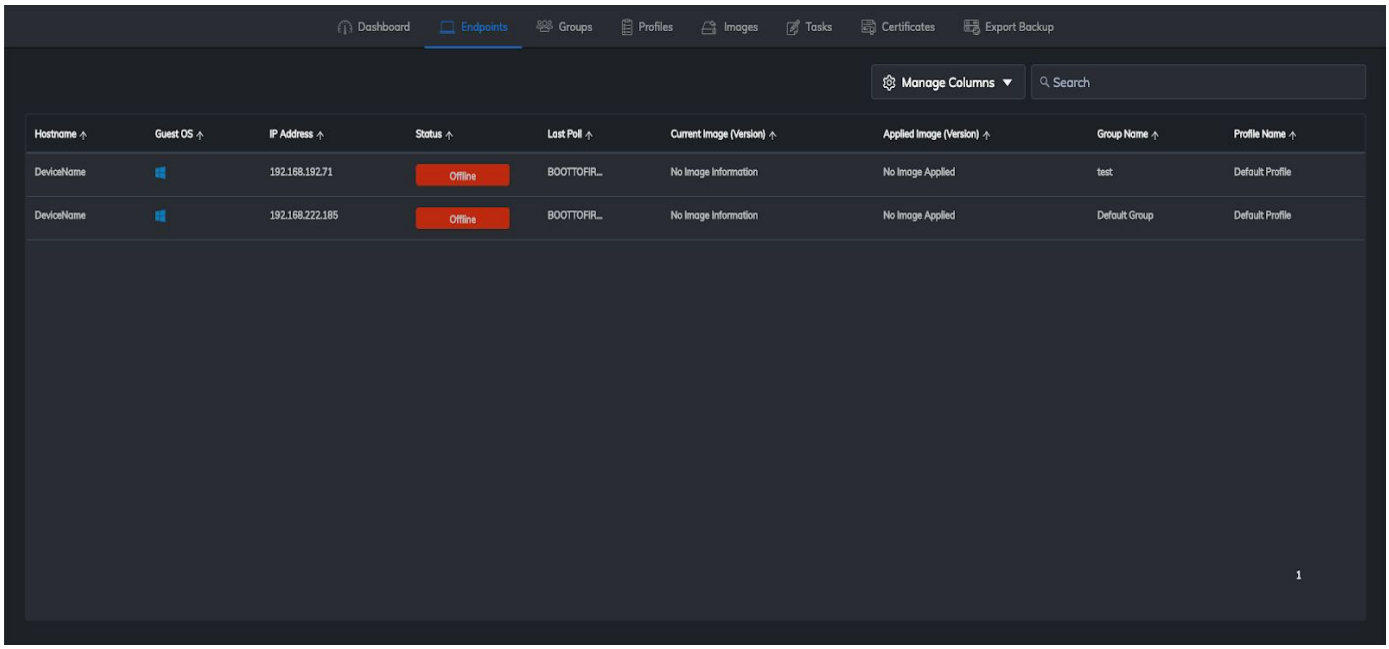


Figure 14. All Endpoints screen

18: Tasks

Tasks can be viewed by selecting the **Tasks** tab from the menu. This will display the **All Tasks** field and from here, users can also choose to view their **Current Tasks** by clicking on the top left corner.

18.1: All Tasks

All Tasks displays all tasks that are queued/scheduled for endpoints along with endpoints' MAC address and task status. This screen shows all tasks initiated from EPM server. Tasks screen will show All Tasks when opened. From here, you can perform multiple tasks by clicking on the **Actions** menu. The table below shows descriptions of all columns in the **All Tasks** screen.

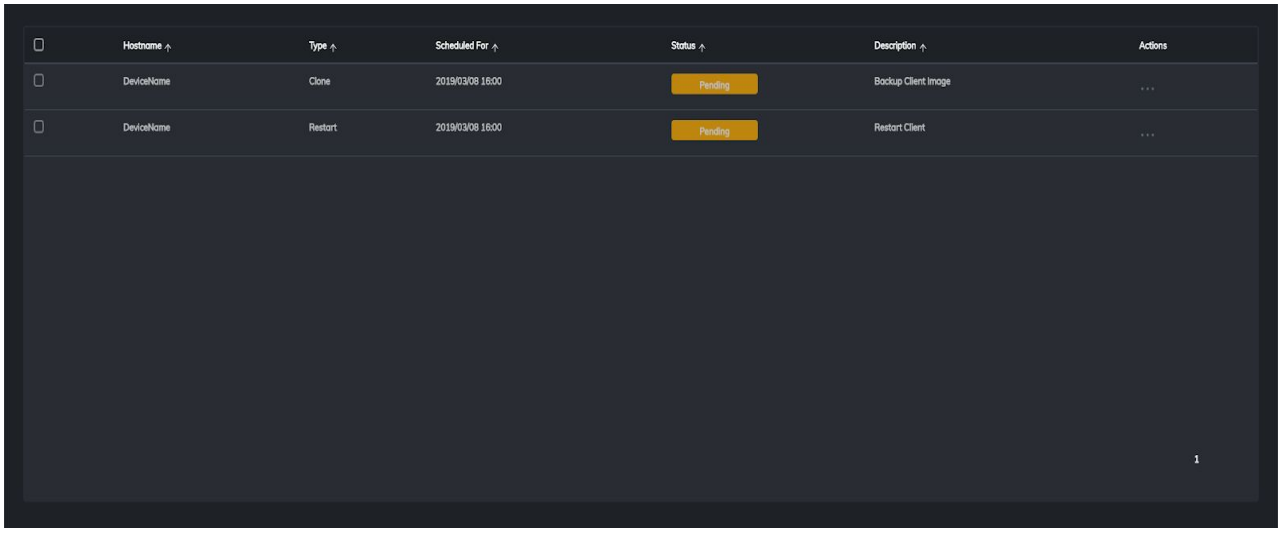


Figure 15. All Tasks screen

Table 14. All Task columns

Field	Description
Type	This column shows type of the task that is queued.
Scheduled For	This column shows date and time for which task is scheduled to be executed.
Status	This column shows the current status of a task. Status can be: • Pending • Started • Done • Failed • Cancelled
Description	This column shows description for a task. For Image Change and Image Backup, description can

	be added (see sec 11.1: “Image Backups” and sec 11.2: “Change Image”)
MAC Address	This column shows MAC address of the endpoint for which task is scheduled. For server backup task, this field shows ‘Server’.

18.2: Current Tasks

Current Tasks are the tasks currently executing on the EPM server. To view currently running tasks, click **“Current Tasks”** button on the Tasks page.. This screen shows progress of each task. Click on the **Actions** menu to display an option to cancel a currently running task. The screen shows no data if no task is in progress. The table below shows descriptions of all columns in the **Current Tasks** screen.

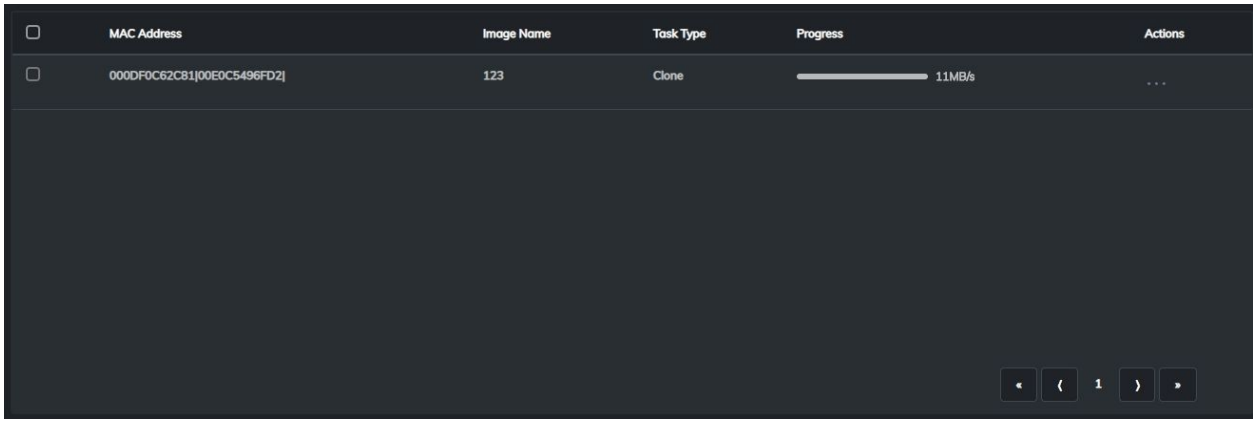


Table 14. Current Task columns

Field	Description
MAC Address	This column shows MAC address of the endpoint for which task is scheduled. For server backup task, this field shows ‘Server’.
Image Name	This column shows image name that is currently being cloned or deployed.
Task Type	This column shows type of the task that is queued.
Progress	This column shows current progress of the task.

19: Images

Images displays all the endpoints' OS images in EPM server. It contains images that can be applied to clients. All image backups of endpoints are saved here. To view this, click **Images** from the menu. You can also update and revert OS images. Below is an image of Images screen.

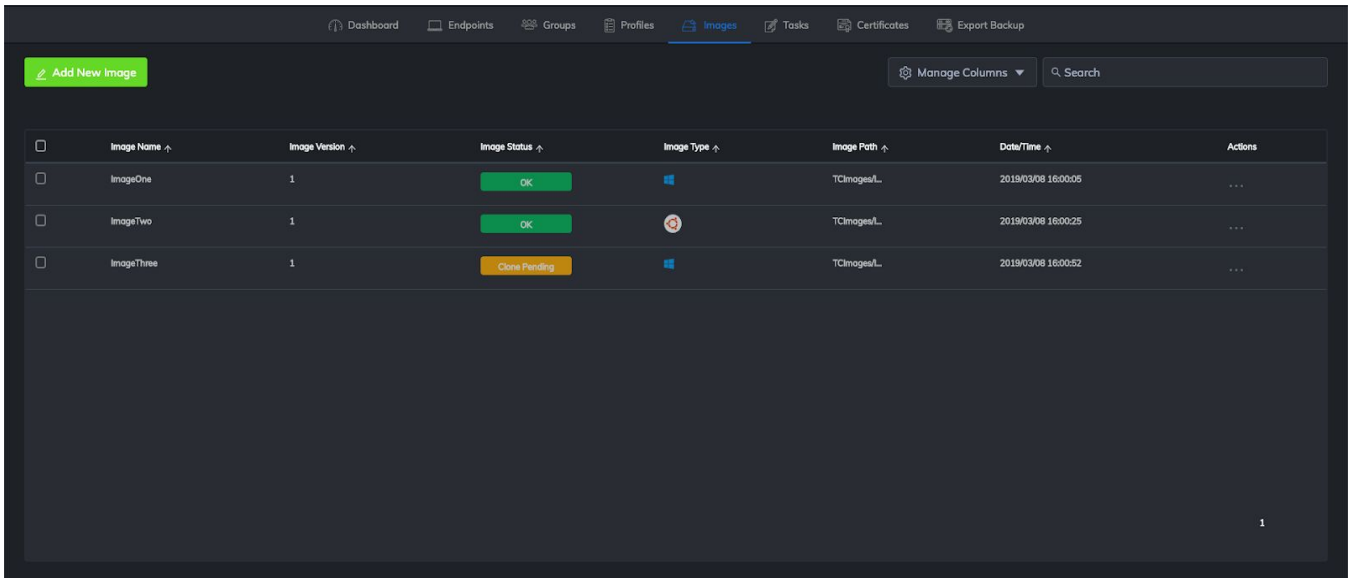


Figure 14. Images screen

19.1: Add Image

EPM allows you to upload OS images (.gz files) in Image Inventory. These images can be applied on endpoints (see 11.2 "Change Image"). To add an image:

1. Go to **Images**.
2. Click **Add New Image.**

   Result: 'Add New Image' popup opens

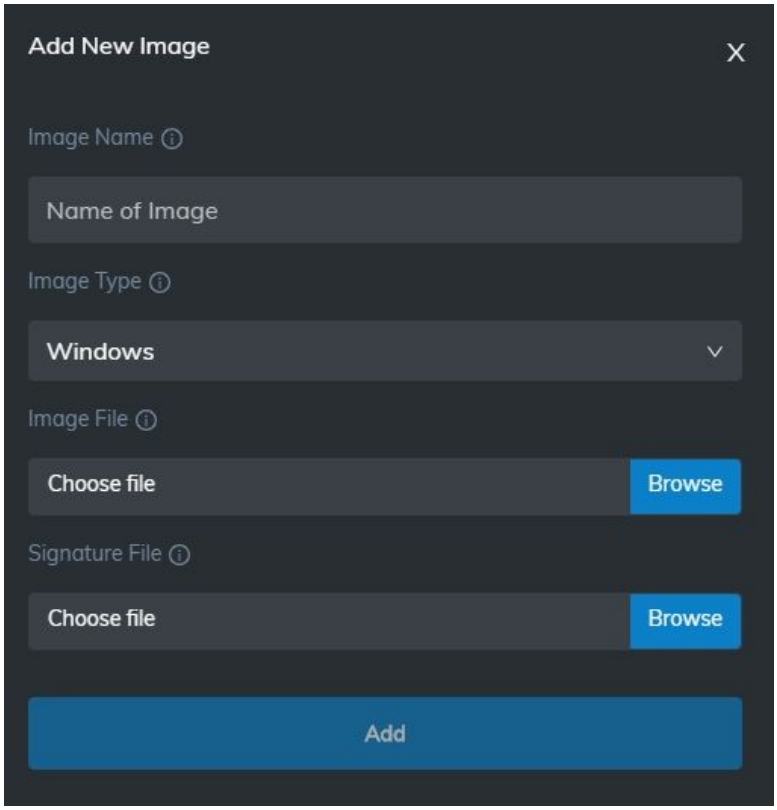


Figure 14. Add New Image popup

3. Add Image Name, Image Type and Image file, and Signature file.
4. Click **Add.**

   Result: Success message appears and image uploads in Images.

The table below shows description for each field in 'Add New Image' popup.

Table 13. Add new image fields

Field	Description
Image Name	This field specifies the name that you want to choose for OS image.
Image Type	This field specifies image type according to the image. There are two image types: Linux and Windows.
Image File	In this field you can upload OS image (.gz file)
Signature File	This is part of the complete OS image

19.2: Delete Image

EPM allows you to delete OS images from image inventory. To delete an image from inventory, select it and click **Delete Image.**

Result: A confirmation popup appears and OS image is deleted.

You can also delete multiple images by selecting them together.

NOTE:	You cannot delete images that are applied on endpoints.

19.3: Update Image

EPM allows you to override/update an OS image. To update an image, select an already present image and click **Update Image.** Upload the new file in 'Update Image' popup and click **Update.**

Result: OS image is uploaded and its version has been updated.

19.4: Revert Image

EPM allows you to revert an updated image back to its previous version. To revert an image in inventory, select it and click **Revert Image.** This reverts the image and changes its version number.

NOTE:	Only those images can be reverted that have been updated before.

19.5: Download Image

EPM allows you to download an OS image. To download an image in inventory, select an image and click **Download Image** in the **Actions** menu.

20: Export Backup

Export backup shows list of server backups that are exported. All server backups are present in the **Export Backup** screen. To view this, click **Export Backup** from the menu. You can also restore a backup from this screen. To restore a backup, select **Restore Backup** option from the **Actions** menu.

Result: Server backup restore starts and EPM server is logged out.

NOTE:	You can only export backup once you have an FTPS server setup.

20.1: Create Backup

To create a Server backup, click on the **Create Backup**. You will not be allowed to perform any activity on server when server backup is in progress. Server backups can be exported in two ways: “Images” and “Everything”. The table below shows Backup options.

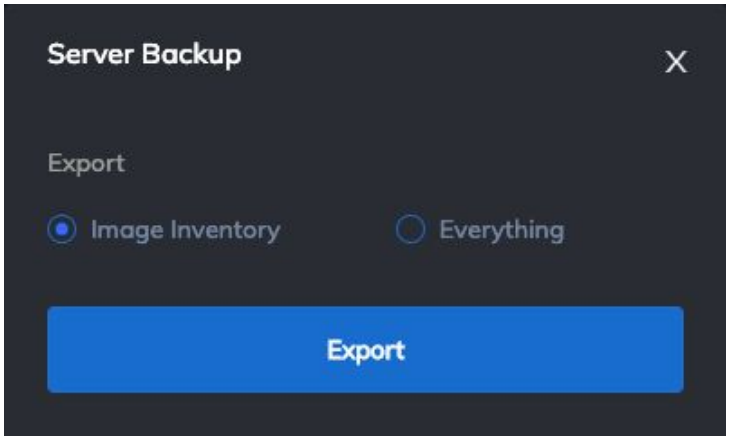


Figure 2. Backup/Restore tab

Table 4. Backup/Restore Configuration fields and options

Field	Description
Images	This field specifies Image backup. It will only export data saved in images.
Everything	This field specifies complete server backup. It will export data saved in image inventory, schedules, certificates, groups and profiles.

20.2: Restore Backup

To restore a server backup, select a server backup in **‘Export backup’** tab and click **‘Restore’** in **Actions** menu**.** Backup will be restored on server. You will be logged out of EPM server when server restore is in progress.

NOTE:	Server backups are saved on FTP server and not in EPM server working directory.

You can restore a server backup to a new appliance as well. To do so, connect to the same FTP server in Configurations (see 8.1 “Configuration options”) and restore backup.

This Page is Intentionally Blank