Enhanced Room Management

Deployment Guide

Software Version 1.0

Document Version 1.b

January 2023

Contents

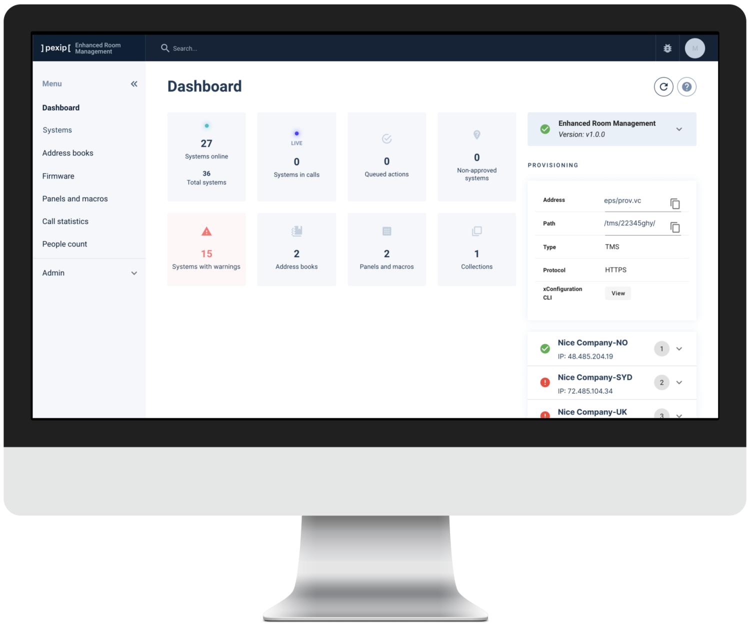
Enhanced Room Management overview

Enhanced Room Management (ERM) is a separately-installable Pexip product that provides management of your Cisco devices and room systems. From system monitoring to bulk provisioning of software upgrades, address books, and branding profiles, it provides everything you need to manage your systems from one single management interface.

Its main features include:

- **Monitoring, usage and diagnostic data**: it provides instant visibility into video systems and room usage data, allowing you to diagnose room system health in real-time. Call statistics allows you to generate valuable insights reports showing system usage per hour/day by participant or group.
- **Provisioning of video systems**: you can provision configuration settings to a single system or in bulk across your organization. You can also create and distribute powerful macros for room automation, and update firmware for any number of systems either immediately or scheduled for later that night.
- **Address books***: you can create address books from multiple sources, including importing from Cisco TMS. Entries in large phonebooks are easy to find by using the search and filtering functions.
- **People count**: real time monitoring of meeting room usage enables you to create powerful reporting from both online and offline meetings.
- **Branding profiles**: you can provision your branding profiles on all or some of your meeting room displays and touch panels across the organization as often as needed.

* Currently only available for self-hosted Pexip Infinity customers.



Address eps/prov.vc
Path /tms/22345ghy/
Type TMS
Protocol HTTPS
xConfiguration CLI

Nice Company-NO IP: 48.485.204.19 1
Nice Company-SYD IP: 72.485.104.34 2
Nice Company-UK 3

See this article for more information about ERM.

The following table provides a feature comparison between Pexip's standard room management service and Enhanced Room Management.

Room management feature	Standard Pexip Service *	Enhanced Room Management
Provisioning of settings		
Provisioning of address books		
Remotely run commands		
Update firmware		

Room management feature	Standard Pexip Service *	Enhanced Room Management
Call control with dial-out, change volume, mute		
Call statistics for specific system		
Multi-vendor support		
Manual entries for address books		
Multi-layer address books		
Provisioning multiple branding templates for Cisco endpoints		
Provisioning macros and collections		
People count support		
Import and export of backups		
Room call statistics		
Provisioning of root certificates		

* Using the standard Pexip Service tools and features: Pexip Portal, Pexip Control Center and the Video System Configuration client.

Supported

Partial support

Not supported

Supported endpoints

ERM currently supports the following endpoints:

- Cisco Webex Room series (Room, Room Kit)
- Cisco Webex Desk series (Desk, Desk pro)
- Cisco C series (C20, C40, C60, C90)
- Cisco DX series (DX70, DX80)
- Cisco EX series (EX60, EX90)
- Cisco MX series (MX200, MX300, MX700, MX800)
- Cisco SX series VTC systems (SX10, SX20, SX80)

and the following software versions:

- Cisco CE9.x and later
- RoomOS 10.x and later
- TC 7.3.x

Getting started

For more information about deploying ERM, see:

- Planning and prerequisites for Enhanced Room Management
- Deploying the ERM Installer virtual machine
- ERM Installer: initial setup and license management

Planning and prerequisites for Enhanced Room Management

This topic contains useful planning and prerequisite information that should be understood before you install ERM. It covers:

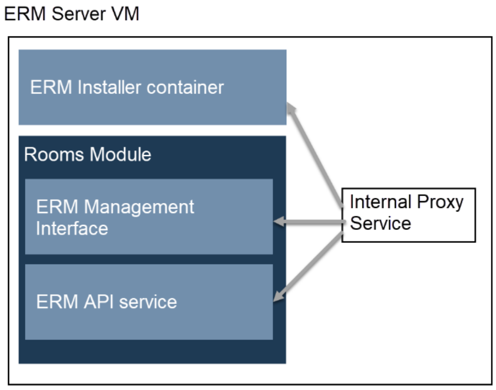
- Understanding the Virtual Machine and ERM components
- Network interface setup
- Network schematics
- Server specifications
- DNS
- Certificates
- Firewall ports
- LDAP authentication

Understanding the Virtual Machine and ERM components

The ERM product is deployed as a Virtual Machine within an on-premises IaaS environment (VMware or Hyper-V) or to a cloud provider (Azure or GCP). You can deploy the ERM VM in one of two modes:

- **Online**: it is deployed as a single VM with access to the Internet and the ERM online licensing and upgrade servers. The VM also provides the main ERM functions.
- **Offline**: it is deployed as two VMs — a secondary VM that has access to the Internet to activate licenses and fetch upgrades, and a primary VM that is "air-gapped" from the secondary VM and the internet and that provides the main ERM functions. There is no difference in the VM images you deploy, just in the way you configure and use them.

The ERM VM performs several functions using different services:



- **ERM Installer**: allows administrators to set up and configure the ERM product. The primary purpose of the installer is to enable the deployment, configuration and updating of the main ERM modules.

  Currently, there is only one module, the core Enhanced Rooms Management application. Pexip intends to release additional modules in due course.

  The installer is used to deploy ERM modules directly within the same VM or to create "offline bundles" for use within a second air-gapped VM. In addition, the administrator can activate a license key (enabling specific modules and features), set basic network details (such as FQDNs), configure TLS certificates, and define an LDAP connection for AD multi-user login, and to manage upgrades of the various modules.
- **Enhanced Rooms Management application**: within this module, there are two separate functions:
  - **ERM GUI**: provides the primary user interface for support personnel to manage videoconferencing endpoints within their estate. For example, the administrator can add video systems, prepare configuration templates, monitor their usage, define firmware updates and address books, apply branding, etc.
  - **ERM API service**: provides RESTful endpoints to allow the provisioning of supported Cisco videoconferencing devices and updates to phonebooks.

- **Internal proxy service**: handles the proxying of HTTP requests to the various ERM services. This service does not require manual intervention as it is automatically configured depending on how the administrator configures the ERM modules.

Note that the different functions of the ERM VM can be updated independently, therefore, they each have their own version numbering.

See ERM deployment overview for more information.

ERM Proxy virtual machine

The ERM Proxy is a virtual machine that is installed separately from the rest of the Enhanced Room Management product suite. It allows an ERM server to provision multiple Cisco endpoints located on a private network, such as behind a firewall/NAT router, that would otherwise be non-*directly* contactable by ERM.

See ERM Proxy virtual machine for more information.

Network interface setup

An ERM VM can be configured with either one or two network interfaces (NICs). The purpose of the NICs is to allow for a separation of network layer traffic. All transport layer ports and higher layer services are bound to both interfaces so all ERM services can be reached through either interface. The internal ERM proxy/routing engine uses the SNI (Server Name Indication) and the FQDN of the relevant ERM service supplied by the client, to route traffic to the correct service.

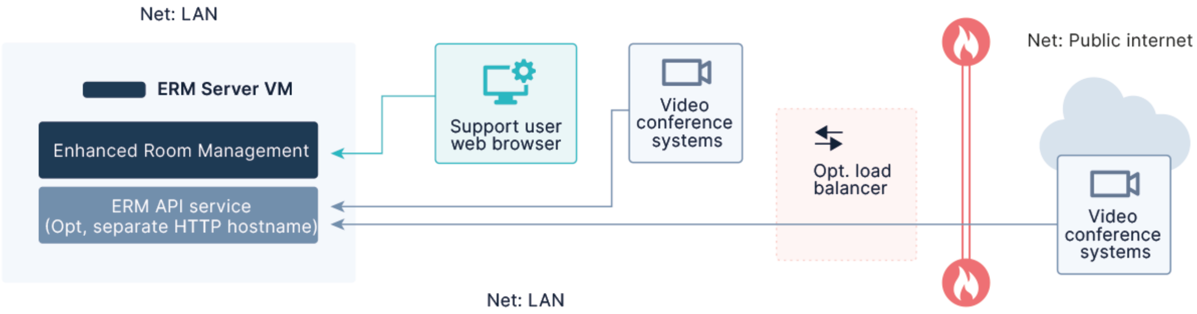
- **Single NIC configurations**: For a VM deployment that uses a single NIC, the first NIC handles all traffic (internal and external). A single IP address is assigned; however, different FQDNs can be applied to the different services, and the internal proxy/routing engine will route traffic appropriately using SNI.
- **Dual NIC configurations**: For a VM deployment with a dual NIC configuration. the first NIC is designed to handle all DMZ and public routed traffic, and the second NIC is designed to handle all internal traffic. However, there is no separation of services across the NICs, thus a service can be reached via either NIC. The intention is to provide more distinct routing capabilities.

Network schematics

ERM can be deployed in your network in a number of different ways that suit your organization.

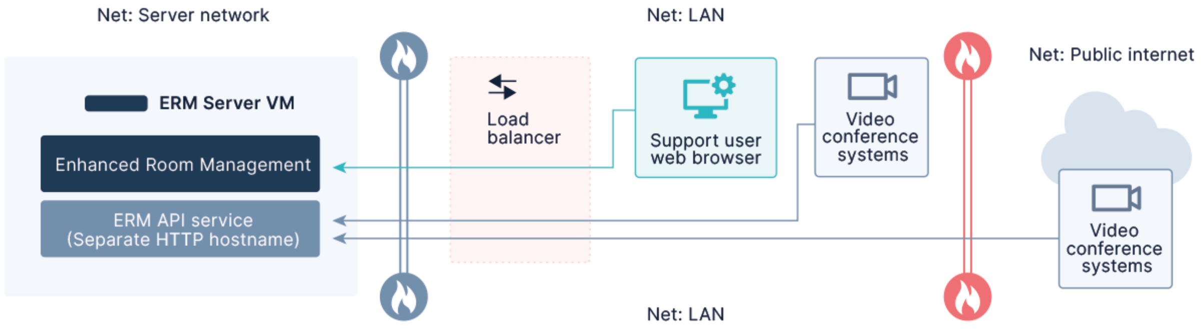
Single VM and a load balancer for external clients

This diagram shows a single VM and access control using a load balancer for external clients:



Single VM and a load balancer for all clients

This diagram shows a single VM and access control using a load balancer for all clients:



Server specifications

Before you install the ERM Installer VM, please review the following recommended system requirements for a production use, single server/VM:

Normal traffic installation	High traffic installation *
<1000 concurrent call participants	>1000 concurrent call participants
<500 managed endpoints/devices	>500 managed endpoints/devices
4x vCPU	8x vCPU
6GB RAM	16GB RAM
100GB storage, SSD/SAN is recommended **	200GB storage, SSD/SAN based **
1x NIC, possibly behind firewall/reverse proxy	1x NIC, possibly behind firewall/reverse proxy

* For larger installations, contact Pexip for a customized deployment.

** In ERM installations, you need to take the disk space of firmware files into consideration. Each firmware version may require 1-2 GB of additional storage space.

We recommend using thick disk provisioning for your virtual machine, thin disk provisioning will also most likely work but use with caution.

DNS

As the ERM product has several functions within a single VM, you should define DNS FQDNs that can be used to access these services.

For example, for services that share the same listening port binding, a proxy service on the VM uses the TLS SNI header to determine which request should be directed to which service:

- The ERM Installer (such as **erm-installer.example.net**). This service binds to port 8999.
- The ERM core application management interface (such as **erm-mgt.example.net**). This service binds to ports 80 and 443.
- (Optional) The ERM API service for video endpoint API requests (for access control) (such as **erm-api.example.net**). This service binds to ports 80 and 443. Note that this service can be combined with and accessed using the ERM core application FQDN.

See Network schematics above for more information.

Certificates

In addition to defining DNS FQDNs, TLS certificates should be used to secure the ERM services. You can use individual certificates, a single SAN certificate (combining all DNS FQDNs), or a wildcard certificate (which would secure an entire domain space, such as ***.example.net**).

See Certificate management for more information.

Firewall ports

Configure firewall ports according to the ERM network port requirements.

LDAP authentication

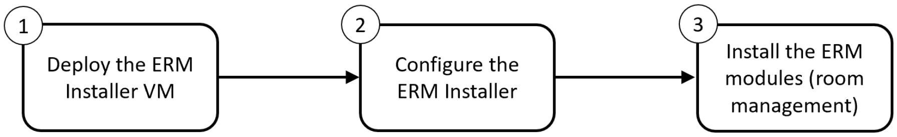
You can optionally use an external LDAP / Active Directory database to authenticate users accessing ERM.

See LDAP authentication settings for more information.

Enhanced Room Management: installation

ERM deployment overview

The Enhanced Room Management installation and deployment process involves three main steps:


1
Deploy the ERM Installer VM
2
Configure the ERM Installer
3
Install the ERM modules (room management)

1. **Deploying the ERM Installer VM**: the first thing you need to do is to deploy the ERM Installer virtual machine to your network. The ERM Installer is used to manage the installation of all of the other modules in the ERM suite.

   See Deploying the ERM Installer virtual machine.
2. **Configuring the ERM Installer**: after you have installed the ERM Installer VM you can set it up for your environment by configuring server settings, adding licenses and so on.

   See ERM Installer: initial setup and license management.
3. **Installing ERM modules**: after you have set up the ERM Installer you are now ready to install the different ERM modules — currently this is just the core ERM application that is used to manage Cisco/Webex room systems.

   See Installing the ERM module for device management.

Enhanced Room Management: deploying the installer VM

Deploying the ERM Installer virtual machine

The primary purpose of the ERM Installer is to enable the deployment, configuration and updating of the main ERM modules. Currently, there is only one module, the core Enhanced Rooms Management application. Pexip intends to release additional modules in due course.

You can deploy ERM on VMware or Hyper-V in your own server network, or you can deploy it as a cloud service in Microsoft Azure or Google Cloud Platform.

- For VMware or Hyper-V in your own server network, see VMware and Hyper-V deployments below.
- For Microsoft Azure, see Deploying ERM in Microsoft Azure.
- For Google Cloud Platform, see Deploying ERM in Google Cloud Platform (GCP).

VMware and Hyper-V deployments

The first step is to add the ERM Installer virtual machine to your server network.

Where this server should be set up depends on your particular network environment. For examples and more detailed network schemas, see Network schematics.

Before you start, you should review the Server specifications for the virtual machine, and the Network port requirements.

Download the ERM Installer VM

Start by downloading our Installer VM. The latest version is available at the Pexip download page.

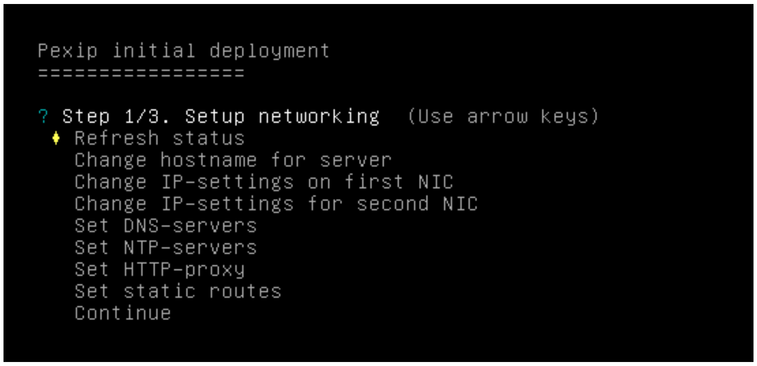
Supported hypervisors

We currently support:

- VMware 6.5 and later
- Hyper-V 2016 and later

Initial VM deployment and network settings

When you first start up the virtual machine, you are presented with a list of choices that you can navigate using the arrow keys. The first section is for your network settings:



```
Pexip initial deployment
=================

? Step 1/3. Setup networking  (Use arrow keys)
 ♦ Refresh status
   Change hostname for server
   Change IP-settings on first NIC
   Change IP-settings for second NIC
   Set DNS-servers
   Set NTP-servers
   Set HTTP-proxy
   Set static routes
   Continue
```

The options are:

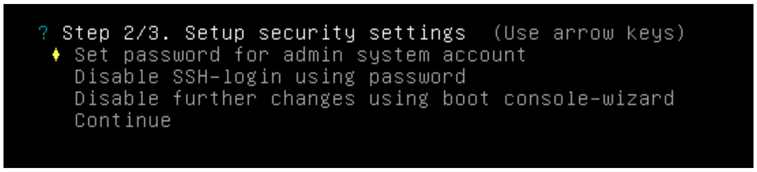
Option	Description
Refresh status	Run this to see the current status of the machine, such as which IP number has been assigned via DHCP, as well as disk space and usage, which can both be helpful during installation.
Change hostname for server	Here you can set the hostname for the server (this is primarily for internal use). This is helpful when monitoring entries in different types of event logs.
Change IP-settings on first/second NIC	Choose this option to switch between using DHCP or manually entering IP numbers and other network settings such as gateway and DNS servers.
Set DNS-servers	This option allows you to specify a standalone DNS server to apply to the server. Even if DHCP is used, an override DNS or similar setup might be used, which you then can specify here.
Set NTP-servers	You can manually specify which NTP servers to use. This can, for example, be useful for a more secure network with a dedicated internal server which you can then enter an IP number or hostname for. If a hostname is specified, it requires an available working DNS server.
Set HTTP-proxy	Use this option if you lock outgoing HTTP(s) requests in your network. It allows all requests to exit via a third-party HTTP proxy where you can verify the traffic and lock down addresses that are not allowed. The format for defining the HTTP(s) proxies is: http://user:password@address:port
Set static routes	This option is available if you have several different subnets in your network. For example, traffic can go by default through the default gateway, but that 10.0.0.0/24 should instead go through a router that has an IP address 192.168.1.100.

Some choices may require a restart to take effect. You can choose to either restart after each step or, if you prefer, you can complete all settings and then restart at the end of your setup.

When you are satisfied with your network settings, select **Continue** at the bottom of the list. This takes you to the next section on security settings.

Server security settings

After configuring the network settings you can define the security settings for your server.



```
? Step 2/3. Setup security settings  (Use arrow keys)
 ♦ Set password for admin system account
   Disable SSH-login using password
   Disable further changes using boot console-wizard
   Continue
```

The options are:

Option	Description
Set password for admin system account	Here you create a password for the default system user (username: admin), which can then be used to log in to the Linux console, for example, to troubleshoot or change a specific setting (with guidance from Pexip support). After the password has been set, this option changes to allow the disabling or re-enabling of the admin account.
Disable SSH-login using password	Choose this option to disable login via SSH with a password. SSH is enabled with the use of SSH keys by default, and not by using a password. First, add your SSH key to the VM. To do this, temporarily activate SSH login using a password, add your SSH public key (to the **~/.ssh/authorized_keys** file) and then deactivate this option for increased security.
Disable further changes using boot console-wizard	If you select this option, you will no longer be able to access the terminal menu without first logging in. ℹ If you have not enabled the admin system account, you will be locked out of the VM entirely and be unable to log in so will need to redeploy the appliance.

When you have chosen your options in this section, select **Continue** at the bottom of the list to proceed. As long as you have not selected **Disable further changes using boot console-wizard**, you can always return to these security choices later on to make additional changes.

VM deployment now completed

Selecting **Continue** from the security settings section means you have completed setting up the new server. If you have made changes to any of the sections that require a restart, you can now restart the machine before proceeding to the next step.

You now see the status view of the ERM Installer VM, including whether the Installer is running, and filesystem information. The following options are available:

Option	Description
Refresh status	Updates the current status view.
Network settings	Brings up the network settings (as described above).
Security settings	Brings up the security settings (as described above).
Login shell	Lets you log in to the VM terminal shell.
Upgrade installer	Even though you can update the Installer from the web interface, you can upgrade it directly from the terminal if, for example, the Installer cannot be reached via the browser. Note that this option does not work in offline environments.
Hard drive cleanup	This option lets you clean up data from your VM including debug logs/raw call data, old versions and unused images.

Next steps

The status view also indicates the IP address of the machine. You can now start adding products from the ERM product suite.

To proceed, make a note of the URL of the ERM Installer displayed in the command line and enter that URL in your web browser to start the Installer.

You may now continue as described in ERM Installer: initial setup and license management.

ERM network port requirements

The table below describes all of the network port requirements for your ERM server.

For a visual guide, see Network schematics.

Public services	Incoming (TCP)
Web UI, feedback events, CDR, API	443 (multiple hostnames)
Browser redirect to HTTPS. Feedback events, passive provisioning for endpoints without TLS support.	80 (optional)

Internal/operational services	Incoming (TCP)
Installer web UI	8999 (may be filtered in firewall)
Low level troubleshooting	22 (may be filtered in firewall)

Outbound connections	Outbound port
API requests to Pexip Infinity	443 (configurable)
Video endpoints	443 (TCP)
DNS	53 (TCP)
LDAP	389 / 636 (configurable)
NTP	123 (UDP)
ERM license activations 185.94.242.28 (erm-activation.pexip.io)	443 (TCP)
ERM docker images registry and OS updates 185.94.242.28 (erm-registry.pexip.io)	443 (TCP)

ERM Proxy virtual machine

The ERM Proxy is a virtual machine that is installed separately from the rest of the Enhanced Room Management product suite. It allows an ERM server to provision multiple Cisco endpoints located on a private network, such as behind a firewall/NAT router, that would otherwise be non-*directly* contactable by ERM.

Additionally, when compared to passive provisioning alone, it provides a more immediate contact with a Cisco endpoint and, thus, a more immersive experience. For example, with passive provisioning alone, the Cisco endpoint will only act on configuration changes after it calls home to the ERM service (which can occur at some point between 45-400 seconds). Whereas, the ERM Proxy allows the ERM service to immediately push both configuration and commands to the Cisco endpoint, allowing them to be controlled and updated in real-time.

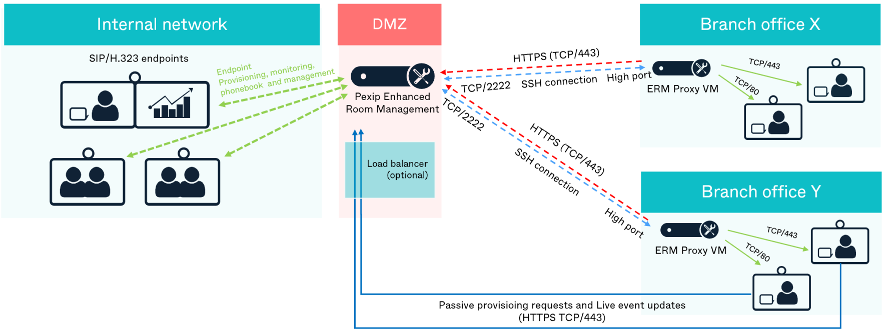
This topic covers:

- ERM Proxy architecture
- How it works
- Server specifications and network options
- Use of Load Balancers or Reverse Proxies
- Installing the ERM Proxy

ERM Proxy architecture

The ERM Proxy virtual machine can be installed in VMware ESXi or Microsoft Hyper-V, and should be deployed as per your security policy. In a geographically-dispersed organization you would normally install multiple ERM Proxys — one in each region or office to manage the local endpoints in that location.

A typical ERM architectural overview that includes the ERM Proxy is shown below:

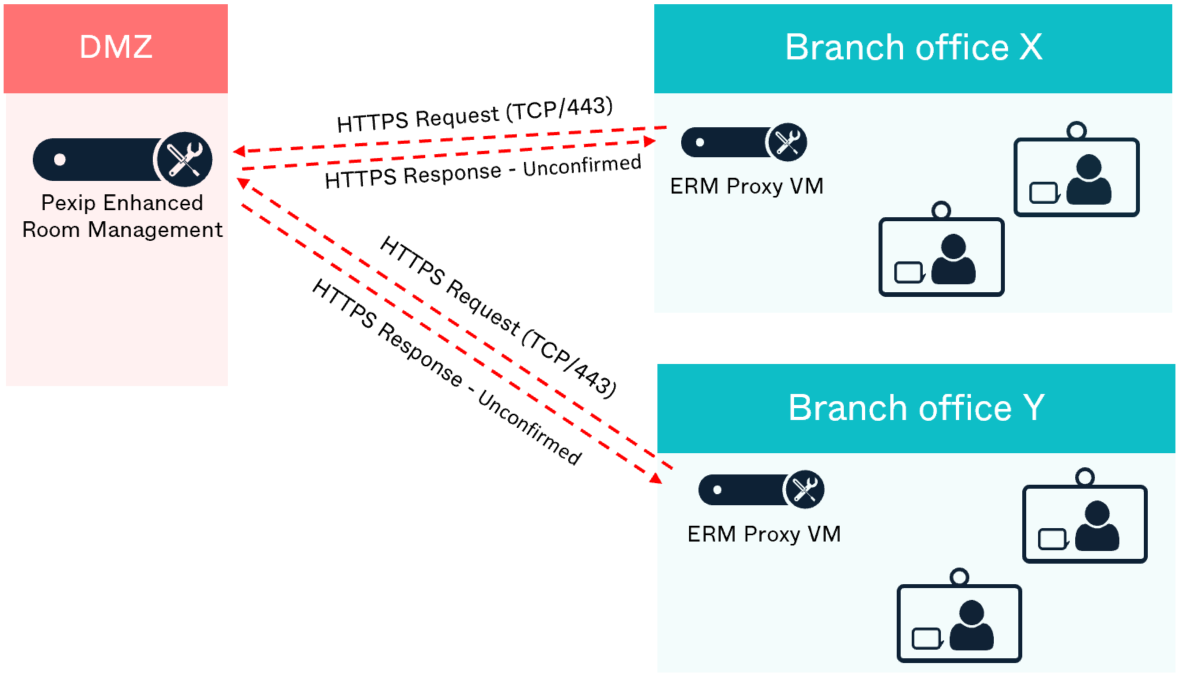


How it works

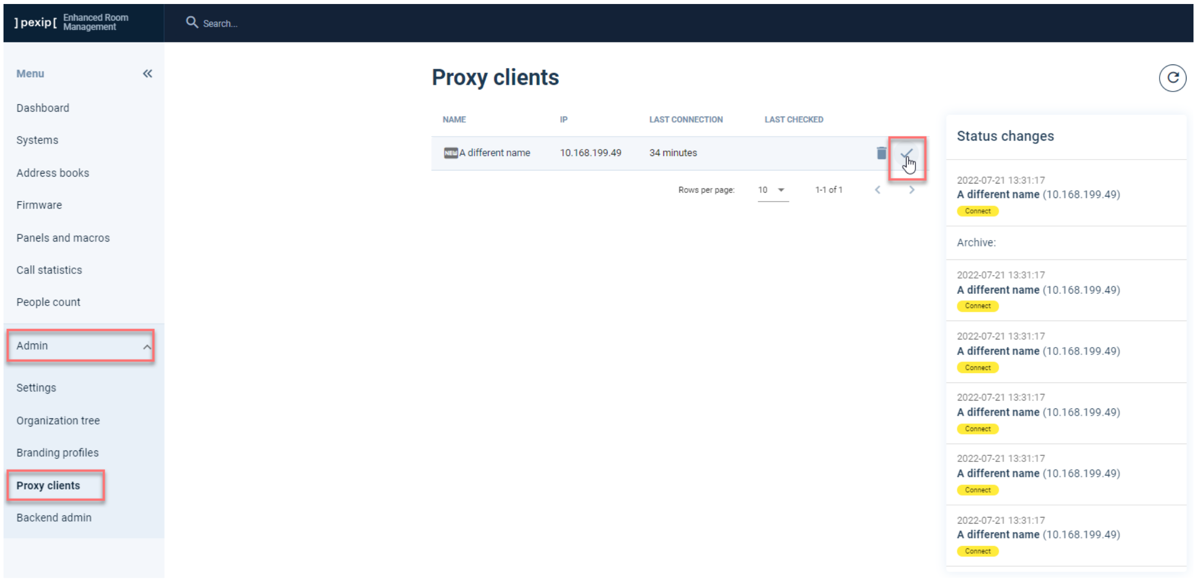
When the initial configuration of the ERM Proxy is complete, the following process occurs:

1. The proxy sends an HTTP request to the ERM service using a TLS-secured connection (toward port 443), authenticated with the proxy client password, to request admission as a proxy client. In addition, the request includes a public SSH key from the proxy to enable a key-based SSH connection to be established in a later step.

   Assuming the ERM Proxy successfully authenticates, the ERM service will initially deny the setup of the SSH connection. After that, the proxy continues to periodically send requests toward the ERM service to see if access has been granted.

2. A successfully authenticated ERM Proxy appears on the **Proxy clients** page within the ERM GUI. An ERM administrator must now manually confirm the proxy connection to the ERM service. See ERM proxy clients for more information.



Proxy clients

NAME	IP	LAST CONNECTION	LAST CHECKED
NEW A different name	10.168.199.49	34 minutes	

Rows per page: 10 1-1 of 1

Status changes

2022-07-21 13:31:17
A different name (10.168.199.49)
Connect

Archive:

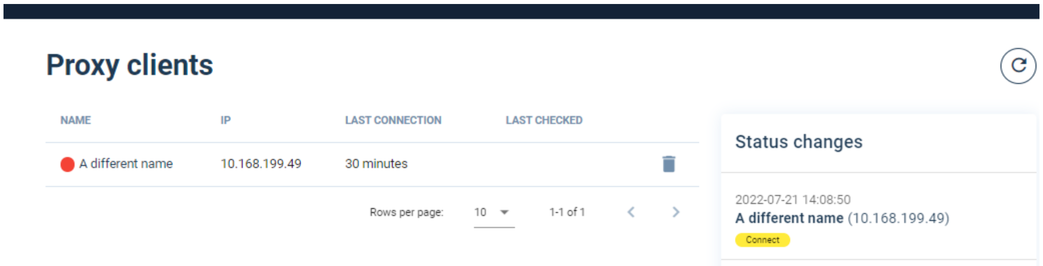
2022-07-21 13:31:17
A different name (10.168.199.49)
Connect

2022-07-21 13:31:17
A different name (10.168.199.49)
Connect

2022-07-21 13:31:17
A different name (10.168.199.49)
Connect

2022-07-21 13:31:17
A different name (10.168.199.49)
Connect

2022-07-21 13:31:17
A different name (10.168.199.49)
Connect



Proxy clients

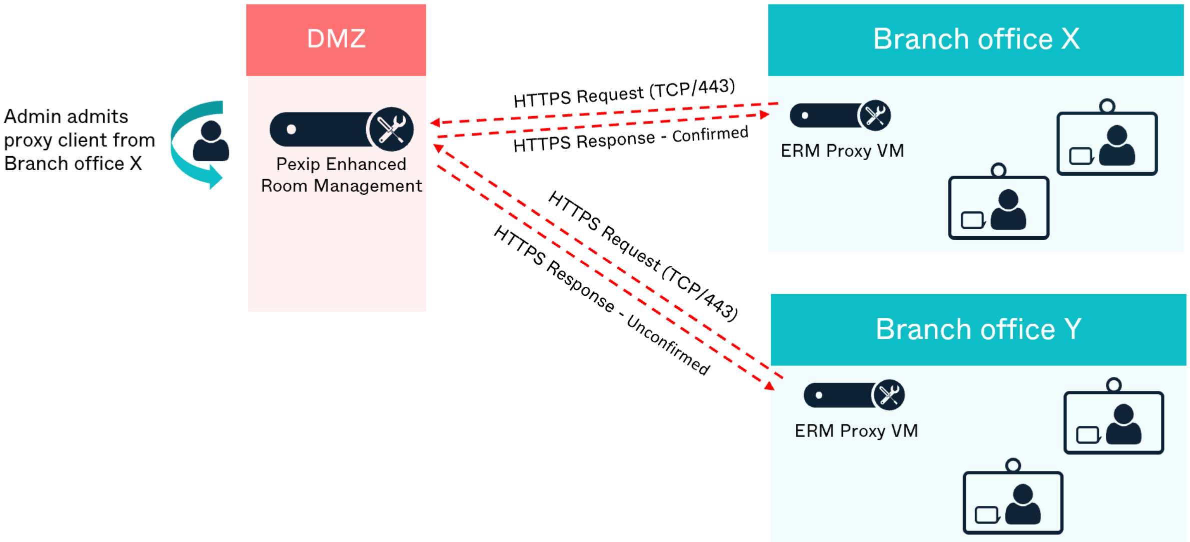
NAME	IP	LAST CONNECTION	LAST CHECKED
● A different name	10.168.199.49	30 minutes	

Rows per page: 10 1-1 of 1

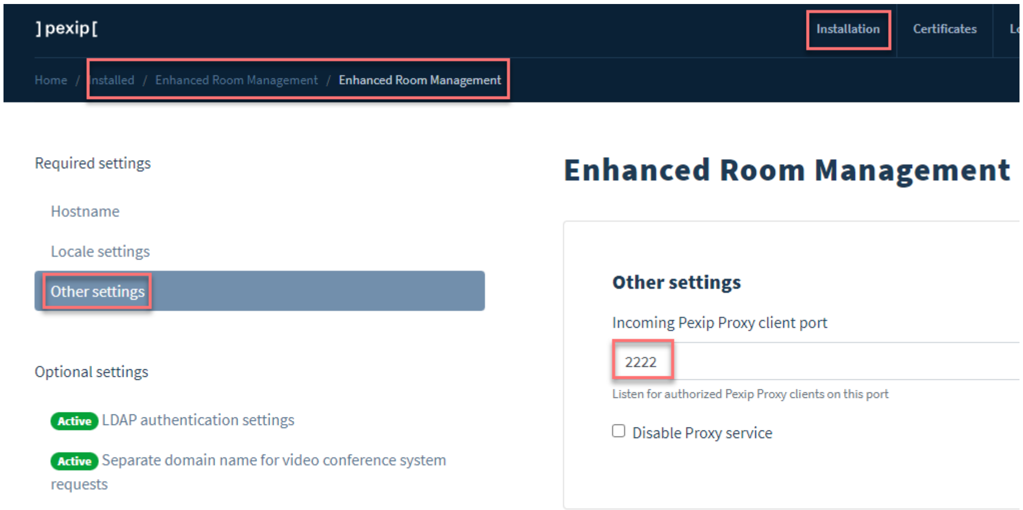
Status changes

2022-07-21 14:08:50
A different name (10.168.199.49)
Connect

3. When the proxy connection is confirmed, the ERM service stores this confirmation. Then, during the next request cycle from the ERM Proxy, the ERM service responds with details required to establish an SSH connection, including the relevant port for this connection and additional security parameters.


DMZ
Branch office X
Admin admits proxy client from Branch office X
Pexip Enhanced Room Management
HTTPS Request (TCP/443)
HTTPS Response - Confirmed
ERM Proxy VM
HTTPS Request (TCP/443)
HTTPS Response - Unconfirmed
Branch office Y
ERM Proxy VM

Note that the default listening port used by the ERM service to enable this SSH connection from the ERM Proxy is TCP 2222. This is configurable within the ERM Installer (via **Installation > (ERM module) Details > Configure > Other settings > Incoming Pexip Proxy client port**). Any updates to this configuration via the Installer must be deployed to the ERM module to take effect.


]pexip[
Installation
Certificates
Home / Installed / Enhanced Room Management / Enhanced Room Management
Required settings
Hostname
Locale settings
Other settings
Optional settings
Active LDAP authentication settings
Active Separate domain name for video conference system requests

Enhanced Room Management

Other settings

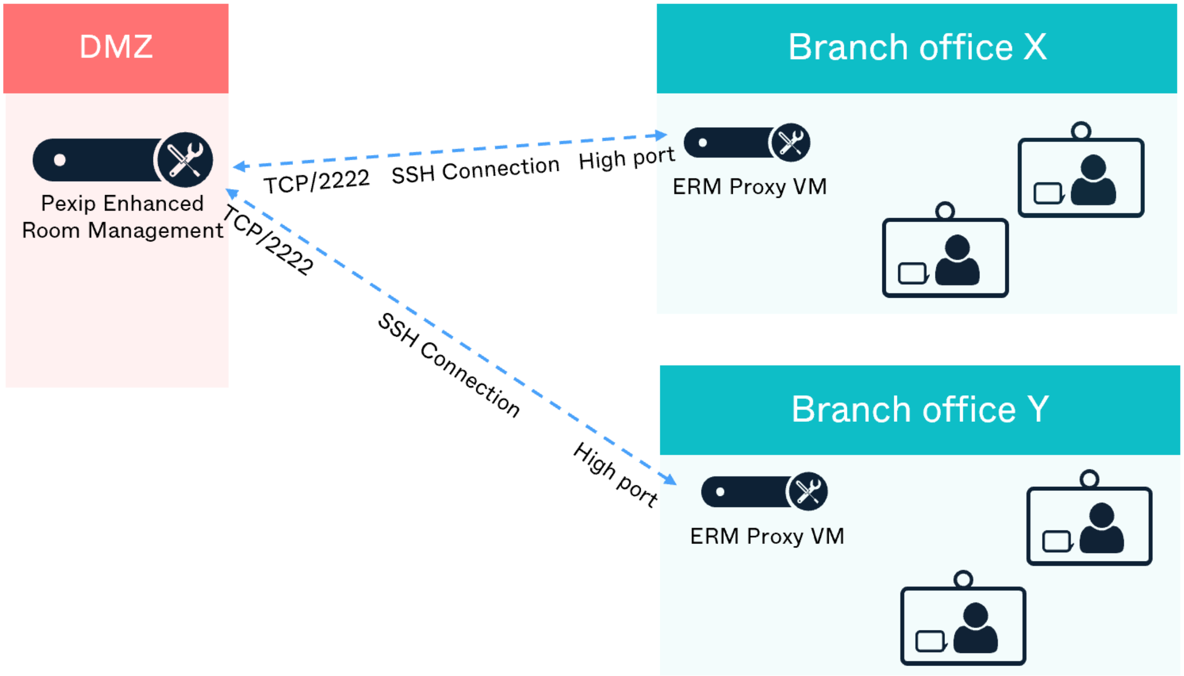
Incoming Pexip Proxy client port

2222

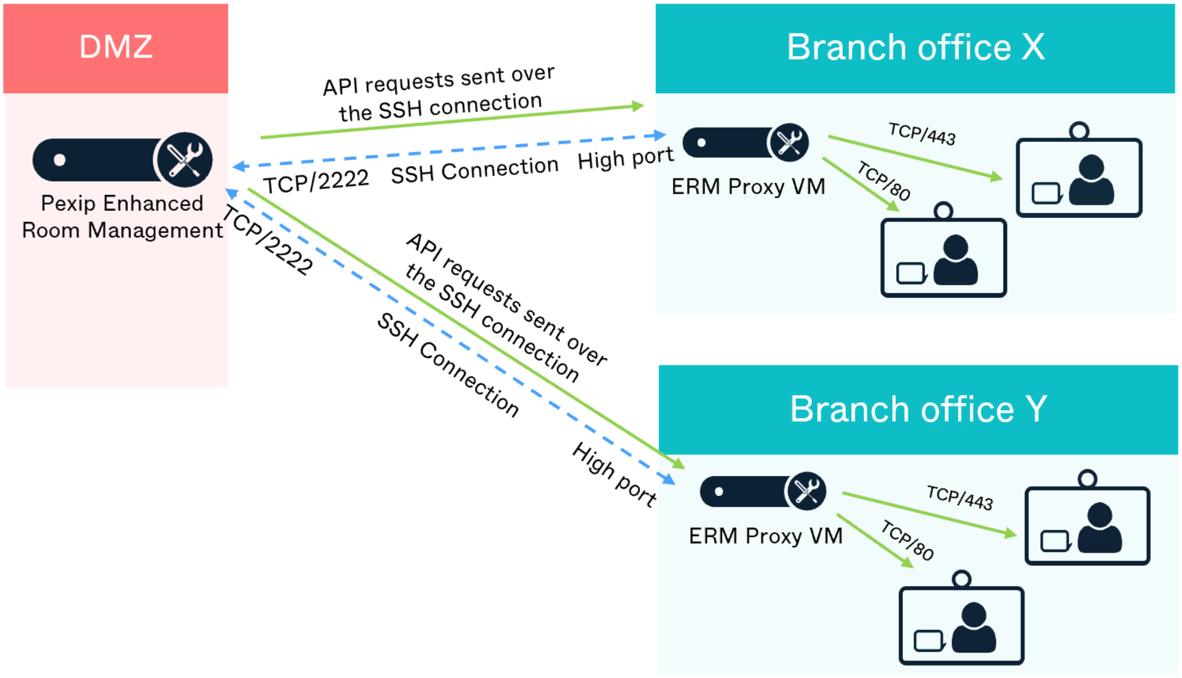
Listen for authorized Pexip Proxy clients on this port

□ Disable Proxy service

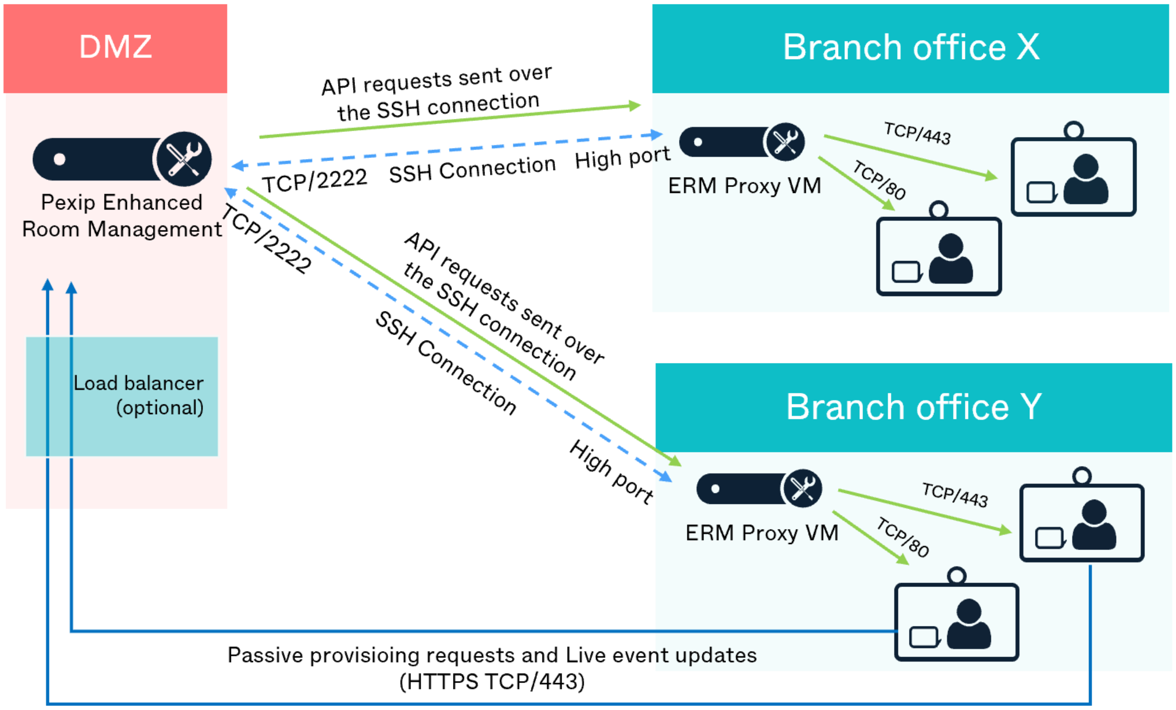
4. The ERM Proxy establishes an SSH connection towards the ERM service using the configured port and negotiated security parameters.



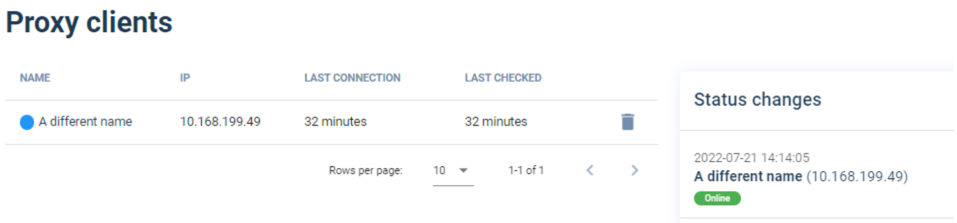
5. The SSH connection enables the ERM service to send provisioning details and API commands via the ERM Proxy to the remote systems. The ERM Proxy forwards the API requests received via the SSH connection as HTTP(s) requests to the Cisco endpoints (TCP port 80/443).



6. Endpoints are configured for passive provisioning and live event updates. These HTTP requests are sent directly from the endpoints to the ERM service. Configuration of passive provisioning enables a fallback connection to the ERM service.



7. An administrator can check the SSH connection status on the ERM service via the **Admin > Proxy clients** menu (see ERM proxy clients for more information).



Proxy clients

NAME	IP	LAST CONNECTION	LAST CHECKED
● A different name	10.168.199.49	32 minutes	32 minutes

Rows per page: 10 1-1 of 1

Status changes

2022-07-21 14:14:05
A different name (10.168.199.49)
Online

Server specifications and network options

The default virtual appliance requires:

- 4 cores (most modern processors will suffice)
- 1.5 GB RAM
- 15 GB SSD storage

This specification should be suitable for most installations as the required data traffic and compute levels are low. It also means that the virtual appliance would be appropriate to run on a shared compute host (with the caveat that there should be minimal oversubscription of the underlying host resources).

Depending on the network topology, the ERM Proxy can be deployed with one or two network interfaces in various configurations:

- Single NIC, the first NIC is used to route all traffic.
- Dual NIC:
  - The first NIC routes external traffic via the DMZ or public network.
  - The second NIC is used to route internal traffic via the LAN network.

Use of Load Balancers or Reverse Proxies

A load balancer or reverse proxy may be used in front of the ERM Proxy and/or the main ERM service.

When a load balancer is used in front of the ERM service, the ERM Proxy connects to the upstream ERM service through this device using both HTTP and SSH connections. The ERM module may be configured using either one or two FQDNs (see Installing the ERM module for device management):

- If the ERM service uses a single FQDN (defined in the **Hostname** field of the main ERM module configuration), then this FQDN should be exposed on the load balancer.
- If the ERM service uses the optional **Separate domain name for video conference system requests**, then this FQDN should be exposed on the load balancer.

The use of such infrastructure can introduce additional complexities and issues. For example, a man-in-the-middle (MITM) device may terminate the HTTP stream as a transparent proxy, and the certificate chain presented toward the ERM Proxy may be issued from an untrusted Certificate Authority. As a result, the attempted connection will fail if the ERM Proxy has been configured to check the certificate validity (which is the default configuration setting).

Installing the ERM Proxy

Pexip provides the ERM Proxy appliance via an OVA or VHDx template suitable for deployment on VMware ESXi or Microsoft Hyper-V. The templates are provided "as-is", offering a reference installation suitable for integrating with an existing Pexip ERM deployment.

No changes should be made to any ERM Proxy via the terminal interface (other than as described when running the initial installation wizard) unless directed to do so by Pexip support. This includes (but is not limited to) changes to the time zone, changes to IP tables, the configuration of Ethernet interfaces, or the installation of any third-party code/applications.

The information you need to specify during the initial configuration of an ERM Proxy includes:

- The FQDN of the ERM service where the ERM Proxy will connect towards.
- The name of the ERM Proxy.
- A proxy client password (which enables the ERM Proxy to authenticate with the ERM service and establish a trust relationship to set up an SSH tunnel).

The installation process for the ERM Proxy is similar to that seen with the standard ERM Installer.

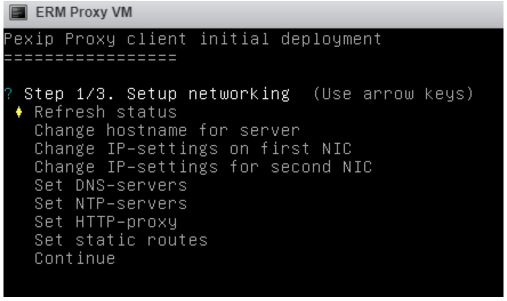
Obtaining the installation image

Download links tbc

Initial VM deployment and network settings

When you first start up the virtual machine, you are presented with a CLI installation wizard that offers a list of choices that you can navigate using the arrow keys.

The first section is for your network settings:



```
Pexip Proxy client initial deployment
=================

? Step 1/3. Setup networking  (Use arrow keys)
 ❯ Refresh status
   Change hostname for server
   Change IP-settings on first NIC
   Change IP-settings for second NIC
   Set DNS-servers
   Set NTP-servers
   Set HTTP-proxy
   Set static routes
   Continue
```

By default the VM appliance uses a single NIC which obtains its IP details via DHCP.

The options are:

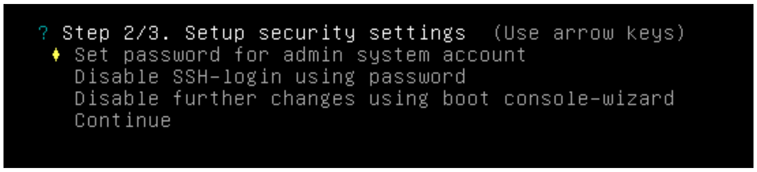
Option	Description
Refresh status	Run this to see the current status of the machine, such as which IP number has been assigned via DHCP, as well as disk space and usage, which can both be helpful during installation.
Change hostname for server	Here you can set the hostname for the server (this is primarily for internal use). This is helpful when monitoring entries in different types of event logs.
Change IP-settings on first/second NIC	Choose this option to switch between using DHCP or manually entering IP numbers and other network settings such as gateway and DNS servers.
Set DNS-servers	This option allows you to specify a standalone DNS server to apply to the server. Even if DHCP is used, an override DNS or similar setup might be used, which you then can specify here.
Set NTP-servers	You can manually specify which NTP servers to use. This can, for example, be useful for a more secure network with a dedicated internal server which you can then enter an IP number or hostname for. If a hostname is specified, it requires an available working DNS server.
Set HTTP-proxy	Use this option if you lock outgoing HTTP(s) requests in your network. It allows all requests to exit via a third-party HTTP proxy where you can verify the traffic and lock down addresses that are not allowed. The format for defining the HTTP(s) proxies is: http://user:password@address:port
Set static routes	This option is available if you have several different subnets in your network. For example, traffic can go by default through the default gateway, but that 10.0.0.0/24 should instead go through a router that has an IP address 192.168.1.100.

Some choices may require a restart to take effect. You can choose to either restart after each step or, if you prefer, you can complete all settings and then restart at the end of your setup.

When you are satisfied with your network settings, select **Continue** at the bottom of the list. This takes you to the next section on security settings.

Server security settings

After configuring the network settings you can define the security settings for your server.



```
? Step 2/3. Setup security settings  (Use arrow keys)
 ♦ Set password for admin system account
   Disable SSH-login using password
   Disable further changes using boot console-wizard
   Continue
```

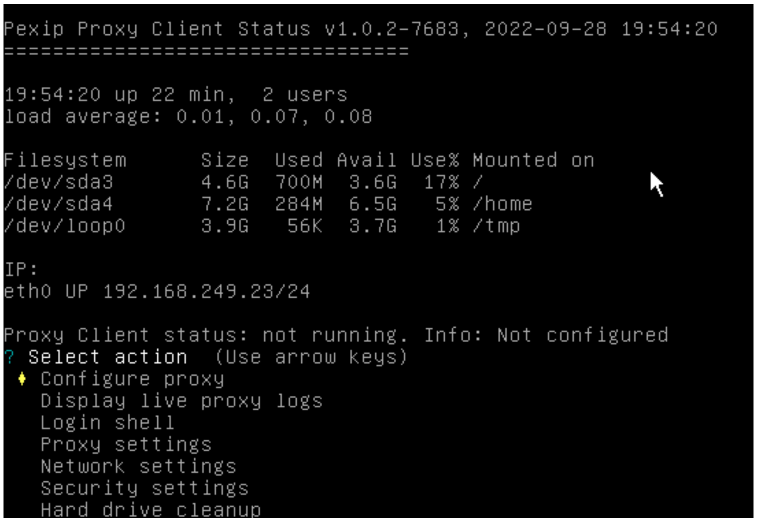
The options are:

Option	Description
Set password for admin system account	Here you create a password for the default system user (username: admin), which can then be used to log in to the Linux console, for example, to troubleshoot or change a specific setting (with guidance from Pexip support). After the password has been set, this option changes to allow the disabling or re-enabling of the admin account.
Disable SSH-login using password	Choose this option to disable login via SSH with a password. SSH is enabled with the use of SSH keys by default, and not by using a password. First, add your SSH key to the VM. To do this, temporarily activate SSH login using a password, add your SSH public key (to the **~/.ssh/authorized_keys** file) and then deactivate this option for increased security.
Disable further changes using boot console-wizard	If you select this option, you will no longer be able to access the terminal menu without first logging in. ⓘ If you have not enabled the admin system account, you will be locked out of the VM entirely and be unable to log in so will need to redeploy the appliance.

When you have chosen your options in this section, select **Continue** at the bottom of the list to proceed. As long as you have not selected **Disable further changes using boot console-wizard**, you can always return to these security choices later on to make additional changes.

CLI main ERM Proxy configuration menu

After the network and security steps of the installation wizard are complete, the main ERM Proxy configuration menu is displayed. Here, you can configure the main operation of the ERM Proxy to connect to an upstream ERM service:



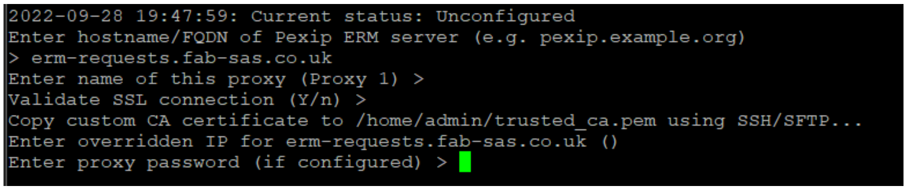
```
Pexip Proxy Client Status v1.0.2-7683, 2022-09-28 19:54:20
=================================

19:54:20 up 22 min,  2 users
load average: 0.01, 0.07, 0.08

Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3       4.6G  700M  3.6G  17% /
/dev/sda4       7.2G  284M  6.5G   5% /home
/dev/loop0      3.9G   56K  3.7G   1% /tmp

IP:
eth0 UP 192.168.249.23/24

Proxy Client status: not running. Info: Not configured
? Select action  (Use arrow keys)
 ♦ Configure proxy
   Display live proxy logs
   Login shell
   Proxy settings
   Network settings
   Security settings
   Hard drive cleanup
```

The options are:

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Configure proxy /
Update server status</td><td>

Initially, this option shows as **Configure proxy**, which allows you to configure the upstream ERM service connection for the ERM Proxy. After the proxy has been configured, this menu item changes to **Update server status**.

Within the Configure proxy menu, there are several sub-options:



```
2022-09-28 19:47:59: Current status: Unconfigured
Enter hostname/FQDN of Pexip ERM server (e.g. pexip.example.org)
> erm-requests.fab-sas.co.uk
Enter name of this proxy (Proxy 1) >
Validate SSL connection (Y/n) >
Copy custom CA certificate to /home/admin/trusted_ca.pem using SSH/SFTP...
Enter overridden IP for erm-requests.fab-sas.co.uk ()
Enter proxy password (if configured) >
```

<table>
<tr><td>Enter FQDN of the Pexip ERM server</td><td>

The details you enter in this field depend on whether you have configured your ERM service with one or two FQDNs, and how you have exposed those FQDNs:

- If your ERM service is configured with a single hostname / FQDN, then this should be used here.
- If your ERM server is configured to use the optional **Separate domain name for video conference system requests**, then typically you will expose this FQDN for remote inbound requests. Note that the main FQDN would technically work, however, when using separate domain names in this way, you would typically use the main FQDN only for access to the ERM web admin GUI.

</td></tr>
<tr><td>Enter the name of this proxy</td><td>This name can be human-readable to identify the proxy when it attempts a connection to the ERM server.</td></tr>
<tr><td>Validate SSL connection (Y/n)</td><td>

The default is **Yes** which ensures the ERM Proxy will validate the presented TLS certificate and chain from the ERM server or upstream infrastructure. Any certificate chain that has been issued from a public CA should be validated successfully using the built-in trusted root CA store.

If you use certificates from a private CA, then you should upload those root CA certificates in a PEM format into the **/home/admin/trusted_ca.pem** file (for example, using an SSH terminal, WinSCP or Filezilla).

</td></tr>
<tr><td>Enter overridden IP for (proxy FQDN)</td><td>Here you can define an IP to override the resolved FQDN of the ERM service (configured previously). For example, if the ERM service FQDN either doesn't resolve, or you want the request to be routed via some other infrastructure, or via an alternative route.</td></tr>
<tr><td>Enter proxy password</td><td>If you have configured a **Proxy client password** within the ERM module (**Admin > Settings > Security and privacy > Proxy client passwords**), you should enter a matching password here.</td></tr>
</table>

</td></tr>
<tr><td>Display live proxy logs</td><td>

Shows a real-time view of the ERM Proxy logged events. Press **Ctrl+C** to cancel this view, and after a couple of seconds, you are returned to the menu.

This option only works after the proxy has been configured and has started.

</td></tr>
<tr><td>Login shell</td><td>Allows you to log in to the VM terminal shell.</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Proxy settings</td><td>Allows you to configure additional settings for the proxy. There are several sub-options:
<table>
<tr><td>Configure proxy</td><td>As per the <b>Configure proxy</b> menu above. When the initial configuration of the ERM Proxy is complete, you can reconfigure it via this option.</td></tr>
<tr><td>Upgrade proxy</td><td>Lets you upgrade to the latest ERM Proxy image from the ERM registry portal. For this to occur, the ERM Proxy requires internet access to the <b>erm-registry.pexip.io</b> service.</td></tr>
<tr><td>Collect logs</td><td>Gathers the log files, compresses them, and saves them to a file in the /tmp folder. The file can then be SCPed off the box using an application like WinSCP, FileZilla or scp at the command line (OS dependent).</td></tr>
<tr><td>Clear settings</td><td>Removes the currently configured ERM Proxy settings.</td></tr>
</table></td></tr>
<tr><td>Network settings</td><td>Opens the network settings as described above.</td></tr>
<tr><td>Security settings</td><td>Opens up the security settings as described above.</td></tr>
<tr><td>Hard drive cleanup</td><td>This option lets you clean up data from your VM, including debug logs/raw call data, old versions and unused images.</td></tr>
</table>

Reverse proxy / load balancer for ERM

ERM can be deployed in your network in a number of different ways that suit your organization. See Network schematics for more information.

To help filter traffic for different services in different network zones, ERM allows the use of different domain names and/or URL prefixes for different types of services.

URL prefix guide – most often opened up beyond LAN/DMZ

If you have enabled **Separate domain name for Rooms Endpoint event requests** in the Installer, these services are already filtered for their respective domain name. Otherwise, the main management hostname should allow all traffic for regular users, and the following URL prefixes may be filtered for external systems and external edge nodes.

Enhanced Room Management	
(may use dedicated domain name)	
/tms/ /ep/	HTTP Feedback events, passive provisioning from Cisco video conferencing systems
/site_media/media/firmware/ /tms/firmware/download/ /ep/firmware/download/	Firmware files for Cisco video conferencing systems

Example – Reverse proxy for satellite offices, with local firmware cache

Prerequisites:

- Split DNS for the remote office with the domain names of the ERM-server overridden to the LB/RP
- Valid SSL certificates
- Replace 123.123.123.123 with the real IP of the server, and replace pexip.example.org with the fqdn for Pexip ERM installation
- If using “Separate domain name for video conference system requests” in your installation, replace endpoints.example.org with the configured fqdn. Otherwise remove the last server{}-block
- Example to start using docker, with the file below named pexip.conf and certificates in a directory named “ssl”:

```
docker run --rm -p 80:80 -p 443:443 -v `pwd`/pexip.conf:/etc/nginx/conf.d/default.conf -v
`pwd`/ssl/:/etc/nginx/ssl/:ro nginx
```

pexip.conf:

```
proxy_cache_path /var/cache/nginx keys_zone=pexip_static:100m inactive=10h max_size=30g;
limit_conn_zone $server_name zone=firmware:1m;

upstream pexipvm {
 server 123.123.123.123:443;
}

server {
 listen 80;
 server_name pexip.example.org;
 server_name endpoints.example.org;
 location / {
   rewrite ^/?(.*) https://$http_host/$1;
 }
}

server {
 listen 443 ssl http2;
 server_name pexip.example.org;

 ssl_certificate /etc/nginx/ssl/pexip.example.org.fullchain.crt;
 ssl_certificate_key /etc/nginx/ssl/pexip.example.org.key;

 # set_real_ip_from 234.234.234.234;  # Uncomment this to pass client IP from upstream proxies

 proxy_set_header Host pexip.example.org;
 proxy_set_header X-Real-IP $remote_addr;
 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 proxy_pass_request_headers on;
 underscores_in_headers on;

 proxy_http_version 1.0;
 proxy_ssl_session_reuse on;

 # Add your access rules here (ip/geoip etc)

 location / {
   proxy_pass https://pexipvm;
 }
 location ~ ^(/site_media/media/firmware/|/(tms|ep)/firmware/download/) {
   proxy_cache pexip_static;
   proxy_cache_valid 200 7d;
   proxy_cache_revalidate on;

   proxy_cache_lock on;
   proxy_cache_lock_age 60s;
   proxy_buffering off;

   limit_conn firmware 10;

   proxy_pass https://pexipvm;
 }
 location /site_media/ {
   proxy_cache pexip_static;
   proxy_cache_valid 200 60s;
   proxy_cache_revalidate on;

   proxy_cache_lock on;
   proxy_cache_lock_age 60s;
   proxy_buffering off;

   proxy_pass https://pexipvm;
 }
}

# Only needed if using "Separate domain name for Rooms Endpoint event requests" in your installation:

server {
 listen 443 ssl http2;
 server_name endpoints.example.org;

 ssl_certificate /etc/nginx/ssl/endpoints.example.org.fullchain.crt;
 ssl_certificate_key /etc/nginx/ssl/endpoints.example.org.key;

 # set_real_ip_from 234.234.234.234;  # Uncomment this to pass client IP from upstream proxies

 proxy_set_header Host $http_host;
 proxy_set_header X-Real-IP $remote_addr;
 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 proxy_pass_request_headers on;
 underscores_in_headers on;

 proxy_http_version 1.0;
 proxy_ssl_session_reuse on;

 # Add your access rules here (ip/geoip etc)

 location / {
   proxy_pass https://pexipvm;
 }
 location ~ ^(/site_media/media/firmware/|/(tms|ep)/firmware/download/) {
   proxy_cache pexip_static;
   proxy_cache_valid 200 7d;
   proxy_cache_revalidate on;

   proxy_cache_lock on;
   proxy_cache_lock_age 60s;
   proxy_buffering off;

   limit_conn firmware 10;

   proxy_pass https://pexipvm;
 }
}
```

Deploying ERM in Google Cloud Platform (GCP)

You can deploy ERM in Google Cloud Platform (GCP). Pexip publishes a disk image for the Pexip ERM Installer virtual machine that you can run on a VM instance in GCP.

In summary, you need to:

1. Prepare your GCP environment and SSH keys.
2. Obtain and prepare the ERM disk image.
3. Create a VM instance to host ERM.
4. Connect to the instance and run the ERM onboarding wizard.

Full details on how to perform these tasks are described below.

Deployment guidelines

This section provides information about what you need to prepare before you can deploy ERM in GCP.

We recommend that you deploy ERM in a dedicated GCP project.

Recommended instance types

GCP instances come in many different sizes. ERM is not compute intensive, it functions as a web server and database, and therefore a general purpose instance type such as the E2 machine series should suffice. We recommend:

- **e2-standard-4** for deployments with up to 500 endpoints
- **e2-standard-8** for deployments with more than 500 endpoints

Security and SSH keys

An SSH key must be applied to the VM instance that will host ERM (in order to complete the installation). Keys can be applied project wide or for a particular VM instance.

ⓘ The username element of the SSH key must be "admin" or "admin@<domain>" i.e. the key takes the format:
`ssh-rsa [KEY_VALUE] admin` or
`ssh-rsa [KEY_VALUE] admin@vc.example.com` for example.

You can create key pairs with third-party tools such as PuTTYgen, or you can use an existing SSH key pair but you will need to format the public key to work in Compute Engine metadata (and ensure the username is modified to "admin"). You can also use other key types than rsa, such as ed25519. For more information about using and formatting SSH keys for GCP, see https://cloud.google.com/compute/docs/instances/access-overview and https://cloud.google.com/source-repositories/docs/authentication#ssh.

Google Cloud IP addressing and VPN for private/hybrid cloud deployments

All GCE VM instances are allocated a Primary internal IP (i.e. private) address. For ERM, you typically also need to assign a static External IP (i.e. public) address to a GCE VM instance.

For a private or hybrid cloud deployment, you must configure the Google Cloud virtual private network (VPN) to connect your on-premises network to the Google Cloud Platform. For full information about how to configure the Google Cloud VPN, see https://cloud.google.com/compute/docs/vpn/overview.

Note that the VM starts up with default configuration running DHCP. You get or set a specific IP address during the VM deployment. When running in DHCP mode you cannot currently set and override the DNS server using the onboarding wizard. If you set the DNS servers while running in DHCP mode they will be overwritten on the next boot. The workaround in this case is to change from DHCP to static IP on the VM and configure your DNS servers again.

Configuring your Google VPC network and firewall rules

We recommend that you configure your Google VPC network (via **VPC network > Firewall** from the GCP project console in your dedicated Google project) to the firewall rules as described in ERM network port requirements. This ensures that access is locked down to just the required ports, and that all relevant ports are enabled.

Note that:

- While the default VPC network and firewall rules allow access to the VM instance running ERM, they do not enable access to the ERM Installer web interface (port 8999). Therefore, you must add a firewall rule for your VPC that allows access to port 8999 on the VM instance.
- The **default-allow-ssh** rule allows SSH access to the VM instance running ERM from any device on the Internet. You may want to limit the source IP addresses that can access this service.
- When configuring your VM instance you can ignore (leave as unselected) the **Allow HTTP traffic** and **Allow HTTPS traffic** options, as you will have already enabled HTTP(S) access as described in ERM network port requirements. (If they are selected, GCE will automatically add network tags to your instance and additional firewall rules to your VPC).

Assumptions and prerequisites

These deployment instructions assume that within GCP you have already:

- signed up to the Google Cloud Platform
- configured a Google Cloud VPN (for a private or hybrid cloud deployment)

For more information on setting up your Google Cloud Platform Virtual Machines, see https://cloud.google.com/compute/docs/instances/.

No changes should be made to any Pexip ERM system (other than as described within this documentation for installing and maintaining your deployment) unless directed to do so by Pexip support. This includes (but is not limited to) any changes to the operating system or the installation of any third-party code/applications. If you encounter any issues, please contact your Pexip authorized support representative.

Obtaining and preparing the disk image for GCE Virtual Machines

Pexip publishes Google Compute Engine (GCE) optimized disk images for ERM.

Before you can use the published ERM disk images, you must copy them to your storage bucket in the Google Cloud Platform (GCP). This guide refers to a disk image copied to your storage bucket as a **custom disk image**. All deployment operations use custom disk images.

Obtaining the Pexip disk images

To obtain your disk images, go to https://www.pexip.com/platform-downloads/enhanced-room-management-current-release, and select the **Direct .tar.gz file download** option for a **GCP deployment**. This downloads a **gce.tar.gz** file with a filename in the format **Pexip_ERM_<version>_generic_<build>_gce.tar.gz**.

Uploading disk images to Google Cloud Storage

The Pexip disk image packages must be uploaded to Google Cloud Storage.

1. Create a bucket to store the images:
   a. From the GCP project console, go to **Cloud Storage > Browser**.
   b. Select **Create Bucket**.
   c. Enter a **Name** (for example, "pexip-v1"), and then select an appropriate **Storage class** and **Location** for your deployment.
      For more information about storage buckets, see https://cloud.google.com/storage/docs/creating-buckets
   d. Select **Create**.
2. Upload the Pexip images to the new bucket:
   a. Select the new bucket e.g. pexip-v1.
   b. Select **Upload Files**.
   c. In the dialog that appears, select the ERM tar.gz file that you downloaded from Pexip.
   d. Select **Open**.

Preparing custom disk images

You must now prepare a custom disk image for ERM:

1. From the GCP project console, go to **Compute Engine > Images**.
2. Select **Create Image**.
3. Enter a **Name**, for example "pexip-erm-v1".
4. Select a **Source** of ***Cloud Storage file***.
5. Select **Browse** and select the ERM image package in your storage bucket e.g. pexip-v1.
6. Select **Create**.

You can now deploy ERM in Google Cloud Platform.

Creating a VM instance to host ERM

After you have prepared a custom disk image for ERM, you can deploy it on a Google Compute Engine VM:

1. From the GCP project console, go to **Compute Engine > VM Instances**.
2. Select **Create Instance**.

3. Complete the following fields (leave all other settings as default):

Name	Enter a unique name for the instance, for example "pexiperm".
Region / Zone	Select an appropriate **Region** and **Zone**. Typically you should choose a region and zone that is geographically close to the location from where it will be administered.
Series and Machine type	The E2 series and an **e2-standard-4** machine type should be sufficient. See Recommended instance types for more information.
Boot disk	Select the ERM custom disk image: a. Select **Change**. b. Select **Custom images**. c. Select your GCP project. d. Select the ERM custom disk image, e.g. "pexip-erm-v1". e. Select a **Boot disk type** of ***SSD persistent disk***. f. Select **Select**.
Identity and API access	For **Service account**, select ***No service account***.
Networking: External IP	In most deployment scenarios you need to assign a public (external) IP address to the instance. a. Expand the **Advanced options** section and open the **Networking** section. b. In the **Network interfaces** field, select the **default** interface to open the Network interface dialog. c. Select a **Subnetwork** if appropriate (e.g. if it is a private/hybrid deployment and you have created new subnets to avoid overlapping addresses in your corporate network). d. Select an appropriate **External IP**: ▪ ***None***: no external IP address will be assigned. Use this where the instance does not need to have a publicly-accessible IP address. ▪ ***Create IP address***: select this option to create a static external address. You can enter a **Name** for the address and GCP will allocate a static IP address. ▪ ***<external address>***: you can select a specific static external address if you have already created one in advance. Do **not** select ***Ephemeral*** — if you stop and restart the instance a new address will be assigned.
SSH keys	An SSH key must be applied to the instance so that you can access the console and run the setup wizard. The username element of the SSH key must be "admin" or "admin@<domain>". To apply an instance-level key: a. Open the **Security** section and then open the **Manage Access** section. b. Select **Add item** to add your own, existing SSH key. This produces a text box. Copy the contents of your public SSH key file and paste them into the text box. Modify the username element at the end of the key to "admin" or "admin@<domain>" if necessary. See Security and SSH keys for more information.

4. Select **Create** to create the instance.

Connecting to the instance and running the ERM onboarding wizard

You must now connect over SSH into the instance to run the ERM setup wizard.

1. Use a command window to connect to the instance via SSH:
   a. Open a command window on your local computer.
   b. Connect to the instance via ssh, using a command in the format: `ssh -i <path to private key> admin@<instance IP address>`
      For example:
      ```
      ssh -i .ssh\gcpprivkey admin@192.168.5.3
      ```
   For more information see https://cloud.google.com/compute/docs/instances/connecting-advanced#thirdpartytools

2. Run the ERM setup wizard. From the command prompt run:

```
sudo onboard_wizard
```

You can now follow the setup instructions as shown in Deploying the ERM Installer virtual machine.

Deploying ERM in Microsoft Azure

You can deploy ERM in Microsoft Azure. Pexip publishes a disk image for the Pexip ERM Installer virtual machine that you can run on a VM instance in Azure.

In summary, you need to

1. Follow the deployment guidelines to prepare your Azure environment and SSH keys.
2. Create your ERM variables initialization script.
3. Copy and save the ERM Azure deployment script.
4. Run the scripts to deploy the Pexip ERM Installer.

Full details on how to perform these tasks are described below.

Deployment guidelines

This section provides information about what you need to prepare before you can deploy ERM in Azure.

Assumptions and prerequisites

These deployment instructions assume that you already have an Azure subscription.

Recommended instance types

Azure instances come in many different sizes. ERM is not compute intensive, it functions as a web server and database, and therefore a general purpose instance type such as the Dsv4 series should suffice.

The deployment script is preconfigured to use a Standard_D4s_v4 instance type.

See https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general for more information.

Security and SSH keys

You can optionally assign an SSH key to the VM instance in Azure that will host ERM.

You can create key pairs with third-party tools such as PuTTYgen, or you can use an existing SSH key pair.

Azure virtual network, NSG and firewall rules

The deployment script automatically creates a suitable Azure virtual network and Network Security Group (NSG) to allow the appropriate access to the VM instance running ERM as described in ERM network port requirements, however you can nominate and use your own existing resources in Azure if required.

Azure IP addressing

The deployment script requests and reports a public IP address for your ERM instance in Azure by default, but you can configure this via the **$PxErmPublicIp** installation variable if you do not want to assign a public IP address to your ERM instance.

Note that the VM starts up with default configuration running DHCP. You get or set a specific IP address during the VM deployment. When running in DHCP mode you cannot currently set and override the DNS server using the onboarding wizard. If you set the DNS servers while running in DHCP mode they will be overwritten on the next boot. The workaround in this case is to change from DHCP to static IP on the VM and configure your DNS servers again.

ERM software disk image

You do not need to download any ERM software packages or prepare a disk image. Pexip publishes an ERM virtual hard disk (VHD) to Azure and the deployment script uses it to create an appropriate Azure image in your Azure subscription.

No changes should be made to any Pexip ERM system or the provided deployment scripts (other than as described within this documentation for installing and maintaining your deployment) unless directed to do so by Pexip support. This includes (but is not limited to) any changes to the operating system or the installation of any third-party code/applications. If you encounter any issues, please contact your Pexip authorized support representative.

Creating and specifying the ERM Azure variables initialization script

You need to specify a range of PowerShell variables that are used during the installation process.

1. Copy and save this variables initialization script on your local computer as, for example, **erm_variables.ps1**.
2. Edit the script and assign the appropriate values for your environment to each of the variables, as described in the table below.
3. Save your updated script.

The PowerShell variables initialization script is listed below. Note that this script does not produce any output. It only sets some variables for subsequent use in the installation script.

```
# The Azure Subscription ID for your ERM resources. This takes the GUID format "aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee".
$PxErmSubscriptionId = ""

# The name of the Azure region into which you are deploying the Pexip ERM resources, for example "westeurope", "southcentralus" etc.
$PxErmAzureLocation = ""

# Name prefix for all ERM resources, e.g. company name.
# PxErmBaseName can have a minimum of 2 and maximum of 10 characters
# It cannot contain dashes, spaces or other non a-z chars.
$PxErmBaseName = ""

# Name of the resource group to use for VM
$PxErmResourceGroupName = ""

# Deploy ERM using existing Virtual Network, Subnet and Network resource group resources
$PxErmDeployInExistingResources = $False # replace with $True or $False
# If $PxErmDeployInExistingResources = $True uncomment below lines to set the variables
#$networkName = ""
#$subnetName = ""
#$nsgName = ""
#$vnetResourceGroup = $PxErmResourceGroupName # If the resource groups is not the same specified above please enter the correct vnet resource
group in ''

# Deploy the ERM VM with a public IP address
$PxErmPublicIp = $True # replace with $True or $False

# Public-facing IP address of management networks used for SSH, Web UI, Installer Web UI, feedback events, CDR, API...
# If not specified (default) access is enabled from internet (should be only used for testing!)
# Any security scans should not come from these IPs
# Example:
# x.x.x.x - Management IP address #1
# y.y.y.y - Management IP address #2
# z.z.z.0/24 - Management subnet
# $PxMgmtSrcAddrPrefixes = @( "x.x.x.x", "y.y.y.y", "z.z.z.0/24" )
$PxMgmtSrcAddrPrefixes = @()

# VM Name
# Azure resource names cannot contain special characters \/""[]:|<>+=;,?*@&, whitespace, or begin with '_' or end with '.' or '-'.
# VM names may only contain letters, numbers, '.', and '-'.
$PxErmVmName = ""

# VM settings
# Below variables needs to follow the requirements of the Azure VM OS Profile:
# https://docs.microsoft.com/en-us/rest/api/compute/virtual-machines/create-or-update#osprofile
# Disallowed username values: "administrator", "admin", "user", "user1", "test", "user2", "test1", "user3", "admin1",
# "123", "a", "actuser", "adm", "admin2", "aspnet", "backup", "console", "david", "guest", "john", "owner",
# "root", "server", "sql", "support", "support_388945a0", "sys", "test2", "test3", "user4", "user5", "1".
$PxErmAdminUsername = ""
# The password must include at least 3 of the following: 1 lower case character,
# 1 upper case character, 1 number, 1 special character that is not "\" or "-" or "$"
# It must be between 6 and 72 characters
$PxErmAdminPassword = ""

# Optional (can be left empty)
# Optional public ssh key (can be left empty) https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-keys#supported-ssh-
key-formats
$PxErmAdminSshKey = ""
```

The variables initialization script contains the following variables:

<table>
<tr><th>Variable name</th><th>Description and example usage</th></tr>
<tr><td>$PxErmSubscriptionId</td><td>The Azure Subscription ID for your ERM resources. This takes the GUID format "<b>aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee</b>".
Example: <b>$PxSubscriptionId = "aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee"</b></td></tr>
<tr><td>$PxErmAzureLocation</td><td>The name of the Azure region into which you are deploying the ERM resources, for example "<b>westeurope</b>", "<b>southcentralus</b>" etc.
Example: <b>$PxErmAzureLocation = "westeurope"</b></td></tr>
<tr><td>$PxErmBaseName</td><td>This is a prefix used when naming all ERM resources. We recommend using your own company name.
<b>PxErmBaseName</b> can have a minimum of 2 characters and a maximum of 10 characters. It cannot contain dashes, spaces or other non a-z characters.
Note that if you are setting up multiple test environments within the same Azure subscription, ensure that each ERM deployment has a unique $PxErmBaseName.
Example: <b>$PxErmBaseName = "pexample"</b></td></tr>
<tr><td>$PxErmResourceGroupName</td><td>The name of the resource group to use for ERM resources. We recommend setting this variable to something in the format <company name>-erm-RG.
Example: <b>$PxErmResourceGroupName = "pexample-erm-RG"</b></td></tr>
<tr><td>$PxErmDeployInExistingResources</td><td>Controls whether to use the existing resources in your Azure subscription.
When set to <b>$False</b> (the default) the deployment script will create and use new resources in Azure.
If you have existing resources in Azure that you want to use for your ERM deployment, change the setting to <b>$True</b> and then remove the comment (#) markers from the following lines and specify the additional resource variables:
<table>
<tr><td>$networkName</td><td>The name of the Azure virtual network to use.</td></tr>
<tr><td>$subnetName</td><td>The name of the Azure virtual network subnet to use.</td></tr>
<tr><td>$nsgName</td><td>The name of the Azure network security group (NSG) to use.</td></tr>
<tr><td>$vnetResourceGroup</td><td>The name of the Azure resource group used to host the virtual network. This defaults to the same value as specified in <b>$PxErmResourceGroupName</b> but you can change it to a different resource group is required, for example: <b>$vnetResourceGroup = "pexample-ermvnet-RG"</b></td></tr>
</table></td></tr>
<tr><td>$PxErmPublicIp</td><td>Controls whether to deploy the ERM VM with a public IP address or not. You can set this value to <b>$True</b> (the default) or <b>$False</b>.
Example: <b>$PxErmPublicIp = $True</b></td></tr>
</table>

Variable name	Description and example usage

$PxMgmtSrcAddrPrefixes	Specifies the public-facing IP addresses of any management workstations/networks that may be required to administer ERM.
	You should not perform any security scans from these addresses.
	For example to allow access from:
	`x.x.x.x     Management IP address #1`
	`y.y.y.y     Management IP address #2`
	`z.z.z.0/24  Management subnet`
	you would specify **$PxMgmtSrcAddrPrefixes = @("x.x.x.x", "y.y.y.y", "z.z.z.0/24")**
	ⓘ If no addresses are specified i.e. **$PxMgmtSrcAddrPrefixes = @( )** then all access via the internet is enabled.
	Example: **$PxMgmtSrcAddrPrefixes = @("192.168.7.4", "192.168.3.0/24")**

$PxErmVmName	The name of the virtual machine used to run ERM: • It can be up to 64 characters long. • Azure resource names cannot contain special characters \/""[]:|<>+=;,?*@&, whitespace, or begin with '_' or end with '.' or '-'. • VM names may only contain letters, numbers, '.', and '-'. Example: **$PxErmVmName = "PexipERM"**
$PxErmAdminUsername	The account username for the VM that will be created in Azure. This is used if you need to connect over SSH into the VM. See https://docs.microsoft.com/en-us/rest/api/compute/virtual-machines/create-or-update#osprofile for details about account name restrictions. Example: **$PxErmAdminUsername = "PexAdmin"**
$PxErmAdminPassword	The associated password for $PxErmAdminUsername for the virtual machine. (You are asked at the end of the process to specify the password for the ERM Installer admin account.) See https://docs.microsoft.com/en-us/rest/api/compute/virtual-machines/create-or-update#osprofile for details about password restrictions. Example: **$PxErmAdminPassword = "Pexip123!"**
$PxErmAdminSshKey	An optional SSH public key to assign to the VM. Example: **$PxErmAdminSshKey = "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDkxR4blOhK0okFHu7Nmnu9xEtktjGAQh/zxugTRnUdkLx7AN2QZSqNf6oJjSC0SY2BFN6kCTsFeiDTxNJ4bHBc7EtlIghqJPP3LvgCv1Q82o+xgVY/L8P6ojglLA44YcPgqh8F74v5aKoiqIY2vevJqS+tUes0kfcjKwz4LH9GZUj6toA6VOqvkyQSSkGl8xazucpsZtlT0Sw7T1lLSPvUIrIqbs80mZGmqIb5mIDsqve4GMTQyr3P admin"**

Copying and saving the ERM Azure deployment script

You need to copy and save the ERM Azure deployment PowerShell script:

1. Copy the ERM Azure deployment script listed below into a plain text editor.
2. Save the script as **deploy_pexip_erm_vm.ps1** into the same folder as your variables initialization script.

ⓘ Do not change the contents of this script.

This is the ERM Azure deployment script:

```
param(
    [Parameter(Mandatory = $True)]
    [ValidateNotNullOrEmpty()]
    [string] $PxErmSubscriptionId,

    [Parameter(Mandatory = $True)]
    [ValidateNotNullOrEmpty()]
    [string] $PxErmAzureLocation,

    [Parameter(Mandatory = $True)]
    [ValidateNotNullOrEmpty()]
    [string] $PxErmResourceGroupName,

    [Parameter(Mandatory = $True)]
    [ValidateNotNullOrEmpty()]
    [ValidatePattern('^[a-z]{2,10}$')]
    [string] $PxErmBaseName,

    [Parameter(Mandatory = $True)]
    [ValidateNotNullOrEmpty()]
    [System.Management.Automation.PSCredential] $PxErmVmAdminCredential,

    [Parameter(Mandatory = $False)]
    [ValidateNotNullOrEmpty()]
    [string]  $PxErmVmName,

    [Parameter(Mandatory = $False)]
    [string] $PxErmAdminSshKey,

    [Parameter(Mandatory = $False)]
    [string] $PxErmDeployInExistingResources,

    [Parameter(Mandatory = $False)]
    [string] $networkName,

    [Parameter(Mandatory = $False)]
    [string] $subnetName,

    [Parameter(Mandatory = $False)]
    [string] $nsgName,

    [Parameter(Mandatory = $False)]
    [string] $vnetResourceGroup,

    [Parameter(Mandatory = $True)]
    [string] $PxErmPublicIp,

    [Parameter(Mandatory = $False)]
    [string[]] $PxMgmtSrcAddrPrefixes = @()
)

$PxErmVmSize = 'Standard_D4s_v4'
$PxStorageContainerName = 'erm'

# Version info
$sourceVersion = "1.0.7"
$sourceBuildNumber = "9497"
$ermOsDiskCopy = "pexip-erm-osDisk-$sourceVersion-$sourceBuildNumber.vhd"
$ermOsDiskSrc = "https://pexipas.blob.core.windows.net/erm/1-0-7/Pexip_ERM_v$($sourceVersion)_generic_$($sourceBuildNumber).0.0_azure.vhd"

$ErrorActionPreference = "Stop"
Set-Item Env:\SuppressAzurePowerShellBreakingChangeWarnings "true"

function Get-UniqueString {
    param(
        [Parameter(Mandatory = $True)]
        [string]$Id,

        [Parameter(Mandatory = $False)]
        [int]$Length
    )

    $hashArray = (New-Object System.Security.Cryptography.SHA512CryptoServiceProvider).ComputeHash($Id.ToCharArray())
    -join ($hashArray[1..$Length] | ForEach-Object { [char]($_ % 26 + [byte][char]'a') })
}

function Take {
    param(
        [Parameter(Mandatory = $True)]
        [string]$Id,
        [Parameter(Mandatory = $True)]
        [int]$Length
    )
    return $(if ($Id.length -gt $Length) { $Id.substring(0, $Length) } else { $Id })
}

$randomId = Get-UniqueString -Id $PxErmResourceGroupName -Length 10

Import-Module Az -MinimumVersion 7.0.0
Connect-AzAccount

Write-Host "Using the subscription with id: $PxErmSubscriptionId"
Set-AzContext -Subscription $PxErmSubscriptionId

# Create RG if it doesn't exist
if (!(Get-AzResourceGroup $PxErmResourceGroupName  -ErrorAction SilentlyContinue)) {
    Write-Host "Creating resource group: $PxErmResourceGroupName"
    New-AzResourceGroup -Name $PxErmResourceGroupName -Location $PxErmAzureLocation
}
else {
    Write-Host "Using the existing resource group: $PxErmResourceGroupName"
}

# StorageAccount - For boot diagnostics and image import
$storageAccountName = -join ($(Take -Id $( -join ($PxErmBaseName, $randomId).toLower()) -Length 14), "ermstorage")

$storageAccount = Get-AzStorageAccount -Name $storageAccountName -ResourceGroupName $PxErmResourceGroupName -ErrorAction SilentlyContinue
if (!$storageAccount) {
    Write-Host "Creating storage account: $storageAccountName"
    $storageAccount = New-AzStorageAccount -ResourceGroupName $PxErmResourceGroupName -Name $storageAccountName -Location $PxErmAzureLocation -
SkuName Standard_LRS -Kind StorageV2
}
else {
    Write-Host "Using the existing storage account: $storageAccountName"
}


# Network
if ($PxErmDeployInExistingResources -eq $True -And $networkName) {
# use set parameter from variable script
}
else {
$networkName = -join ($PxErmBaseName, "-", $randomId, "-VNET")
}

if ($PxErmDeployInExistingResources -eq $True -And $vnetResourceGroup) {
$virtualNetwork = Get-AzVirtualNetwork -ResourceGroupName $vnetResourceGroup -Name $networkName -ErrorAction SilentlyContinue
}
else {
$virtualNetwork = Get-AzVirtualNetwork -ResourceGroupName $PxErmResourceGroupName -Name $networkName -ErrorAction SilentlyContinue
}


if (!$virtualNetwork) {
    Write-Host "Creating virtual network: $networkName"
    $virtualNetwork = New-AzVirtualNetwork -ResourceGroupName $PxErmResourceGroupName -Location $PxErmAzureLocation -Name $networkName -
AddressPrefix 10.0.0.0/24
}
else {
    Write-Host "Using the existing virtual network: $networkName"
}

if ($PxErmDeployInExistingResources -eq $True -And $subnetName) {
# use set parameter from variable script
}
else {
$subnetName = "Default"
}

$subnet = Get-AzVirtualNetworkSubnetConfig -Name $subnetName -VirtualNetwork $virtualNetwork -ErrorAction SilentlyContinue
if (!$subnet) {
    Write-Host "Creating subnet: $subnetName"
    $virtualNetwork = Add-AzVirtualNetworkSubnetConfig -Name $subnetName -AddressPrefix 10.0.0.0/24 -VirtualNetwork $virtualNetwork | Set-
AzVirtualNetwork
    $subnet = Get-AzVirtualNetworkSubnetConfig -Name $subnetName -VirtualNetwork $virtualNetwork
```

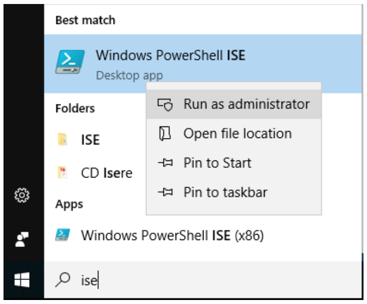
```
}
else {
    Write-Host "Using the existing subnet: $subnetName"
}

if ($PxErmDeployInExistingResources -eq $True -And $nsgName) {
# use set parameter from variable script
}
else {
# Network security group
$nsgName = -join ($PxErmBaseName, "-", $randomId, "-NSG")
}

if (!$PxMgmtSrcAddrPrefixes) {
    $PxMgmtSrcAddrPrefixes = "Internet"
}

if ($PxErmDeployInExistingResources -eq $True -And $vnetResourceGroup) {
$nsg = Get-AzNetworkSecurityGroup -Name $nsgName -ResourceGroupName $vnetResourceGroup -ErrorAction SilentlyContinue
}
 else {
$nsg = Get-AzNetworkSecurityGroup -Name $nsgName -ResourceGroupName $PxErmResourceGroupName -ErrorAction SilentlyContinue
}


if (!$nsg) {
    Write-Host "Creating network security group: $nsgName"
    $rule1 = New-AzNetworkSecurityRuleConfig -Name ssh-rule -Description "Allow SSH" `
        -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix `
        $PxMgmtSrcAddrPrefixes -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 22
    $rule2 = New-AzNetworkSecurityRuleConfig -Name http-rule -Description "Allow HTTP" `
        -Access Allow -Protocol Tcp -Direction Inbound -Priority 101 -SourceAddressPrefix `
        Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 80
    $rule3 = New-AzNetworkSecurityRuleConfig -Name https-rule -Description "Allow HTTPS" `
        -Access Allow -Protocol Tcp -Direction Inbound -Priority 102 -SourceAddressPrefix `
        Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 443
    $rule4 = New-AzNetworkSecurityRuleConfig -Name installer-rule -Description "Allow Pexip installer" `
        -Access Allow -Protocol Tcp -Direction Inbound -Priority 103 -SourceAddressPrefix `
        $PxMgmtSrcAddrPrefixes -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 8999
    $nsg = New-AzNetworkSecurityGroup -ResourceGroupName $PxErmResourceGroupName -Location $PxErmAzureLocation -Name `
        $nsgName -SecurityRules $rule1 , $rule2, $rule3, $rule4
}
else {
    Write-Host "Using the existing network security group: $nsgName"
}

# Download
# Obtain the access key for the storage account
$storageAccountKey = Get-AzStorageAccountKey -ResourceGroupName $PxErmResourceGroupName -Name $storageAccountName
$storageAccountKey = $storageAccountKey[0].Value
# Create the storage access context
$ctx = New-AzStorageContext -StorageAccountName $storageAccountName -StorageAccountKey $storageAccountKey
if (!(Get-AzStorageContainer -Name $PxStorageContainerName -Context $ctx -ErrorAction SilentlyContinue)) {
    Write-Host "Creating blob storage container: $PxStorageContainerName"
    New-AzStorageContainer -Name $PxStorageContainerName -Context $ctx | Out-Null
}
else {
    Write-Host "Using the existing blob storage container: $PxStorageContainerName"
}

$osDisk = Get-AzStorageBlob -Container $PxStorageContainerName -Blob $ermOsDiskCopy -Context $ctx -ErrorAction Silent
$osDiskCopy = $null
if (!$osDisk) {
    # Start copying the OS Disk Image
    Write-Host "Going to copy ERM disk from $ermOsDiskSrc to $ermOsDiskCopy"
    $osDiskCopy = Start-AzStorageBlobCopy -AbsoluteUri $ermOsDiskSrc -DestContainer $PxStorageContainerName -DestBlob $ermOsDiskCopy -
DestContext $ctx
}
else {
    Write-Host "OS disk $ermOsDiskCopy has been already copied to $PxStorageContainerName blob container"
    $osDisk = $osDisk[0].ICloudBlob
}
if ($osDiskCopy) {
    # Wait for the OS Disk to finish copying
    $status = Get-AzStorageBlobCopyState -Blob $osDiskCopy.Name -Container $PxStorageContainerName -Context $ctx
    While ($status.Status -eq "Pending") {
        $status
        $status = Get-AzStorageBlobCopyState -Blob $osDiskCopy.Name -Container $PxStorageContainerName -Context $ctx
        Start-Sleep 10
    }
    $status
    $osDisk = $osDiskCopy.ICloudBlob
}

$diskImage = Get-AzImage -ResourceGroupName $PxErmResourceGroupName -ImageName $ermOsDiskCopy -ErrorAction SilentlyContinue
if (!$diskImage) {
    # Create Azure images from the vhd files
    Write-Host "Creating Azure images from the vhd file"
    $osImageConfig = New-AzImageConfig -Location $PxErmAzureLocation
    Set-AzImageOsDisk -Image $osImageConfig -OsType "Linux" -OsState "Generalized" -StorageAccountType "Premium_LRS" -BlobUri
$osDisk.Uri.AbsoluteUri | Out-Null
    $diskImage = New-AzImage -Image $osImageConfig -ImageName $ermOsDiskCopy -ResourceGroupName $PxErmResourceGroupName
    $diskImageId = $diskImage.Id
    Write-Host "Created Pexip ERM Disk image with resource ID: $diskImageId"
}
else {
    $diskImageId = $diskImage.Id
    Write-Host "Using the exisiting Pexip ERM Disk image with resource ID: $diskImageId"
}

# Public IP
# If the $PxErmPublicIp parameter is set to True create a public IP
if ($PxErmPublicIp -eq $true) {
$pipName = -join ($PxErmBaseName, "-", $randomId, "-PIP")
$pip = Get-AzPublicIpAddress  -ResourceGroupName $PxErmResourceGroupName -Name $pipName -ErrorAction SilentlyContinue
if (!$pip) {
    Write-Host "Creating public IP address: $pipName"
    $pip = New-AzPublicIpAddress `
        -ResourceGroupName $PxErmResourceGroupName `
        -Location $PxErmAzureLocation `
        -AllocationMethod Static `
        -IdleTimeoutInMinutes 4 `
        -Name $pipName
}
else {
    Write-Host "Using the existing public IP address: $pipName"
}
}

# NIC
$nicName = -join ($PxErmBaseName, "-", $randomId, "-NIC")
$nic = Get-AzNetworkInterface -Name $nicName -ResourceGroupName $PxErmResourceGroupName -ErrorAction SilentlyContinue
if (!$nic) {
    Write-Host "Creating network interface: $nicName"
    # if $PxErmPublicIp is set to True set the public IP on the nic
    if ($PxErmPublicIp -eq $true) {
    $nic = New-AzNetworkInterface `
        -Name $nicName `
        -ResourceGroupName $PxErmResourceGroupName `
        -Location $PxErmAzureLocation `
        -SubnetId $subnet.Id `
        -PublicIpAddressId $pip.Id `
        -NetworkSecurityGroupId $nsg.Id
    } else {
    $nic = New-AzNetworkInterface `
        -Name $nicName `
        -ResourceGroupName $PxErmResourceGroupName `
        -Location $PxErmAzureLocation `
        -SubnetId $subnet.Id `
        -NetworkSecurityGroupId $nsg.Id
    }
$getprivip = Get-AzNetworkInterface -Name $nicname -ResourceGroupName $PxErmResourceGroupName -ErrorAction SilentlyContinue
$PrivateIP = $getprivip.IpConfigurations.PrivateIpAddress
}
else {
    $PrivateIP = $nic.IpConfigurations.PrivateIpAddress
    Write-Host "Using the existing network interface: $nicName with private IP: $PrivateIP"
}

# VM
# Create a virtual machine configuration
$vmConfig = New-AzVMConfig `
    -VMName $PxErmVmName `
    -VMSize $PxErmVmSize | `
    Set-AzVMOperatingSystem `
    -Linux `
    -ComputerName $PxErmVmName `
    -Credential $PxErmVmAdminCredential | `
    Set-AzVMSourceImage `
    -Id $diskImageId | `
    Set-AzVMBootDiagnostic `
    -Enable -StorageAccountName $storageAccountName -ResourceGroupName $PxErmResourceGroupName | `
    Add-AzVMNetworkInterface `
    -Id $nic.Id

# Configure the SSH key
if ($PxErmAdminSshKey) {
    $vmConfig = $vmConfig | Add-AzVMSshPublicKey `
        -KeyData $PxErmAdminSshKey `
        -Path "/home/$($PxErmVmAdminCredential.UserName)/.ssh/authorized_keys" | `
        Set-AzVMOperatingSystem -Linux -DisablePasswordAuthentication -ComputerName $PxErmVmName -Credential $PxErmVmAdminCredential
}

Write-Host "Deploying Pexip ERM VM: $PxErmVmName"
$vm = New-AzVM -ResourceGroupName $PxErmResourceGroupName -Location $PxErmAzureLocation -VM $vmConfig
if ($vm.IsSuccessStatusCode) {
    Write-Host "Successfully deployed Pexip ERM VM (version: $sourceVersion, build number: $sourceBuildNumber)."
    Write-Host ""
    if ($PxErmPublicIp -eq $true) {
    Write-Host "******************************************************************************************"
    Write-Host "To start your Pexip ERM installer configuration, browse to:"
    Write-Host "https://$($pip.IpAddress):8999"
    Write-Host ""
    Write-Host "When you connect with SSH, you must use the username: $($PxErmVmAdminCredential.UserName)@$($pip.IpAddress)"
    Write-Host ""
    Write-Host "******************************************************************************************"
    } else {
    Write-Host "******************************************************************************************"
    Write-Host "To start your Pexip ERM installer configuration, browse to:"
    Write-Host "https://$($PrivateIP):8999"
    Write-Host ""
    Write-Host "When you connect with SSH, you must use the username: $($PxErmVmAdminCredential.UserName)@$($PrivateIP)"
    Write-Host ""
    Write-Host "******************************************************************************************"
    }
    if ($PxErmDeployInExistingResources -eq $true) {
    Write-Host "You deployed ERM in an existing virtual network and Network security group. Make sure to open up the correct ports described in
the documentation:"
    Write-Host "https://docs.pexip.com/erm/installation/vm-deployment/network-ports.htm"
    Write-Host ""
    Write-Host "******************************************************************************************"
    }
}
else {
    Write-Host "Deployment failed."
}
Set-Item Env:\SuppressAzurePowerShellBreakingChangeWarnings "false"
```

Running the scripts to deploy the Pexip ERM Installer in Azure

You can now deploy the Pexip ERM Installer in your Azure subscription — this section describes the PowerShell commands used to install ERM.

Deploying the Pexip ERM Installer

1. From your PC, run PowerShell ISE as Administrator by right-clicking on it and selecting **Run as Administrator**.



2. If you are connecting to Azure Resource Manager from your Windows PC for the first time, you must run the following PowerShell command:

```
Install-Module -Name Az -MinimumVersion 7.0.0 -MaximumVersion 8.3.0 -AllowClobber -Scope AllUsers
```

   To check your installed version you can run:

```
Get-InstalledModule -Name Az -AllVersions
```

3. Change directory to the folder (`cd <path>`) into which you have saved the variables initialization script and deployment script.

   You must ensure that the folder containing your scripts is in your PowerShell PATH environment variable (you can use `$env:path` to check this).

4. Open and run your **erm_variables.ps1** variables initialization script.
5. Copy and run the following installation commands.
   - It sets the execution policy for the current PowerShell process — when prompted type A (Yes to All).
   - It prepares the credentials to apply to the VM (based on what you supplied in the variables initialization script).
   - Then it runs **deploy_pexip_erm_vm.ps1** to deploy the Pexip ERM Installer.

   These are the installation commands:

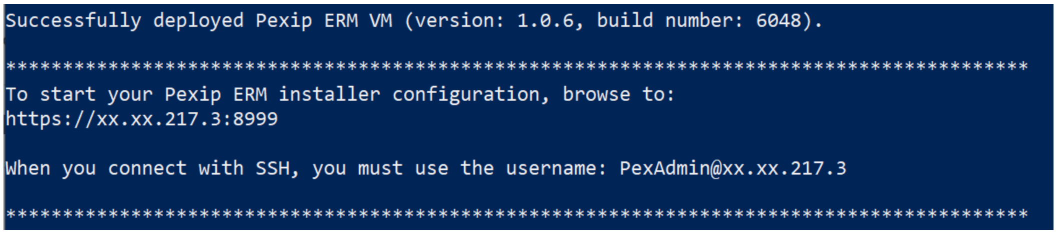
```
# ERM installation script. Do not modify the contents of this script

# Set execution policy for the current PowerShell process, when prompted type A (Yes to All)
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope Process

# Prepare the credentials to apply to the VM
$securePassword = ConvertTo-SecureString $PxErmAdminPassword -AsPlainText -Force
$PxErmVmAdminCredential = New-Object System.Management.Automation.PSCredential ($PxErmAdminUsername, $securePassword)

# Call the deployment script
./deploy_pexip_erm_vm.ps1 -PxErmSubscriptionId $PxErmSubscriptionId `
    -PxErmAzureLocation $PxErmAzureLocation `
    -PxErmBaseName $PxErmBaseName `
    -PxErmVmName $PxErmVmName `
    -PxErmResourceGroupName $PxErmResourceGroupName `
    -PxMgmtSrcAddrPrefixes $PxMgmtSrcAddrPrefixes `
    -PxErmVmAdminCredential $PxErmVmAdminCredential `
    -PxErmAdminSshKey $PxErmAdminSshKey `
    -PxErmDeployInExistingResources $PxErmDeployInExistingResources `
    -networkName $networkName `
    -subnetName $subnetName `
    -nsgName $nsgName `
    -PxErmPublicIp $PxErmPublicIp `
    -vnetResourceGroup $vnetResourceGroup
```

6. At the start of this process you are asked to sign in to Azure — follow the prompts to do this.

   ℹ The sign-in window may not automatically appear on top of your existing windows. If your PowerShell session appears to be hanging, check that the Azure sign-in window is not being obscured by any other windows.

7. While the script runs it outputs several messages stating what is being created. Wait for the script to finish. This may take several minutes.

   When the script completes, a "Successfully deployed Pexip ERM VM" message is displayed, for example:



```
Successfully deployed Pexip ERM VM (version: 1.0.6, build number: 6048).

******************************************************************************************
To start your Pexip ERM installer configuration, browse to:
https://xx.xx.217.3:8999

When you connect with SSH, you must use the username: PexAdmin@xx.xx.217.3

******************************************************************************************
```

(A different message is displayed if you decided to use your own existing resources in Azure.)

8. Follow the instructions presented on the screen: browse to the specified address with the given username to access your Pexip ERM Installer.
9. At the Welcome screen you can define the password you want to use to access the ERM Installer (you will use this in the future along with the admin username you specified in your variables initialization script) and then enter your license key.

   See ERM Installer: initial setup and license management for full details.

ERM release notes

This section lists the new features, changes in functionality, fixed issues and security improvements in the Pexip Enhanced Room Management (ERM) product and installer.

- ERM product changelog
  - Version 1.0.2
  - Version 1.0.1
- ERM Installer changelog
  - Version 1.0.7
  - Version 1.0.6

ERM product changelog

This section lists the new features and changes in the ERM product.

Version 1.0.2

Added

- Include number of seats in system Excel export
- Add support for automatic cleanup/redaction of debug logs and call statistics, set through backend admin (beta)
- Display per endpoint based history for people count
- Start storing sensor data from touch panels - temperature, noise level
- Add support to set overridden address book for a specific endpoint
- Display all tasks that will be repeated in provision dialog
- Display warning if dial settings/system name have been changed on system
- Apply dial settings from chained provisioning service
- Fix saving setting to automatically adding incoming endpoints
- Initial support for repeating provisioning
- Display warning if passive provision events have stopped coming in while live events still are
- Display information about CA certificate validation in Dashboard provisioning widget
- Add option to validate SSL-connection to systems (require trusted CA in installer)
- Add API endpoint filter for online and warning-status
- Display hostname and MAC-address on system dashboard
- Add support to match LDAP user to a customer using DN path (using "dn" as matching field in installer)

Fixed

- Use inline pagination in backend admin to allow updating calendar connections for large room lists
- Fix room list sync for rooms with invalid email address as name

- Make sure to stop non-finished concurrent status updates when task timeout is reached
- Fix updating dial info for Webex systems
- Fix potential lock race condition during object update
- Don't set passive system to online status when displaying cached status data
- Allow connecting Proxy client to separate ERM hostname
- Use correct help text for active screen - branding logo field
- Fix browser freeze-up when setting zero-value in required, number-based command arguments
- Handle connection error during re-activationg of HttpFeedback slot
- Fix logging for background tasks
- Don't display system meeting status in list except for when in head count view
- Fix endpoint API data type for warning about missing live events
- Only allow .cop.sgn and .pkg-files in firmware upload

Changed

- Use secure flag for cookies
- Use ed25519 cipher for Proxy tunnel for new deployments
- Connect to external systems in the following order (if set): API host, hostname, IP instead of API host, IP, hostname
- Retry failed API-requests to video systems
- Use Monday as first day of week in date picker dropdown
- Stop display uuid in call history for spark/webex-calls
- Hide non-approved proxy clients for non-admin users
- Include created provision task id in API response
- Use file upload for CA root certificate setting
- Display information about TlsVerify on dashboard
- Stop trying to connect to incoming endpoints using external remote IP if internal IP connection failed
- Only fill SIP proxy password value when default password is set
- Don't pass default SIP proxy-password or Proxy client password to non-admin
- Return HTTP 403 when proxy registration fails
- Use debian ca-certificates instead of Mozilla as default trusted CA list
- Hide permissions from user backend admin due to not being used elsewhere
- Use locally stored call history for active endpoints as well if system could not be contacted
- Increase concurrency when updating active endpoint status
- Stop allowing proxy connections without password by default for new installation
- Brute force lockout for proxy client registration attempts
- Remove deprecated SSH algorithms for proxy client tunnels

Version 1.0.1

Added

- Add support to bulk provision saved dial settings from ERM to endpoints
- Add support to bulk provision chained passive provisioning
- Display loading errors on dashboard
- Support for getting provisioning data from external passive provisioning server
- Display license information on Dashboard
- Display call history from local call statistics for passive endpoints
- Support for syncing external sources to nested subgroup (delimited by >)
- Merge folders with the same name from multiple sources in addressbook search
- Add API endpoint to force addressbook sync
- Log TMS address book sync error, force UTF-8 encoding

Fixed

- Fix database initialization if using FQDN with over 100 characters
- Fix translation in policy views and macro dialog
- Don't display full html page as error message if raw error is passed to frontend
- Strip XML namespace from chained passive provision services using tandberg CUIL namespace
- Better connection/response error-handling when updating endpoint status
- Better error handling of disconnecting participants in ongoing meeting list
- Fix using prefilled default SIP proxy password when bulk-provisioning endpoint dial settings
- Fix saving endpoints if changing it from backend admin
- Fix freetext search for address book items in root folder
- Fix rescheduling tasks for next night when last task in particular timezone had errors
- Better error handling for connection errors when updating call statistics from previously offline endpoints
- Reset user session if currently selected customer is removed
- Remove console log for missing favicon
- Remove console warning in organization tree view
- Fix endpoint proxy-client empty password in multi-tenant ERM installations
- Prefill default sip proxy settings when provisioning multiple endpoints
- Bulk provisioning missing endpoint device aliases to Pexip Infinity
- Remove empty columns from endpoint debug view error log
- Use password input for new password field in provisioning view
- Better error message on chained provisioning errors

Security

- Upgrade libgmp, zlib1g, libssl, libexpat, gzip, liblzma5
- Upgrade django
- Related CVEs: CVE-2022-0778 CVE-2021-43618 CVE-2018-25032 CVE-2022-23852 CVE-2022-25235 CVE-2022-25236 CVE-2022-25313 CVE-2022-25315 CVE-2022-22818 CVE-2022-23833 CVE-2022-1271

Changed

- Increase log verbosity for ldap logins
- Allow multiple reverse proxy/load balancer hops when resolving client ip
- Log firmware version when called endpoint commands fail
- Don't set endpoint status to "in call" when display endpoint status until call is connected
- Always display mac address and serial field in endpoint form to be able to replace it with a new one
- Open endpoint web admin interface in new window
- Set default passive provision heartbeat to 7 minutes (activated endpoint still use < 1 min)
- Display password indicator in provision dialog if default sip proxy password is set
- Only allow selecting one endpoint when filtering statistics instead of silently ignoring extra ones
- Disable change password functionality for passive endpoints - not supported
- Hide add new organization unit from system list, empty groups are hidden

ERM Installer changelog

This section lists the new features and changes in the ERM installer.

Version 1.0.7

Added

- Add support for Hyper-V environments
- Add support to enable external database from license file
- Add support to importing and converting binary certificates (beta)

- Add support to export private keys with encryption, and importing encrypted keys
- Add support for external redis server
- Add support for enabling LDAP referral chasing
- Add support to lookup LDAP servers using SRV records
- Add more inline documentation for LDAP-settings
- Mark certificates in use in lists
- Add field for validating SSL handshake against remote port using network tools
- Validation of database and LDAP settings when saving configuration
- Display information about last component metadata refresh time and add link to force refresh

Fixed

- Clear certificate existing CA chain when updating public key
- Fix TLS validation for LDAP test connection
- Validate line before removing volumes
- Fix version ordering for x.y.z-dev builds
- Fix permission to run ping in network tools
- Fix certificate chain warnings if CA lacks common name information
- Reset offline mode if online license validation was successful
- Increase length of LDAP filter
- Remove warning in load balancer logs about SNI host
- Stop validating values in optional forms marked for deletion
- Fix offline export if "check for update"-checkbox is not set
- Fix offline export if any components are marked for uninstallation
- Remove console log warnings about HostSNI
- Fix installing multiple ERM on the same VM without getting 500 error
- Fix home link from product details view
- Lock postgres version for LDAPAdmin deployed with old version of deploy file
- Stop re-deploying load balancer on installer upgrade if not necessary
- Remove warning about missing volumes when removing component
- Fix service deploy problems when using setting values (e.g. passwords) starting with quotes (")

Security

- Upgrade django, openssl, libssl1.1, sqlite3
- Related CVEs: CVE-2022-28346, CVE-2022-28347, CVE-2022-0778
- Limit system permissions for load balancer container, run more services with read only root file system

Changed

- Only display first certificate chain warning, hide warning if three or more certificates are included
- Increase log verbosity for LDAP tests
- Set LDAP connection timeout
- List any unknown/not fully uninstalled container services
- Add pagination and search to certificate lists
- Use direct API for fetching service logs instead of subprocesses for better performance
- Escape special characters in authentication to external services
- Change deploy mode for some shared services to allow Installer upgrades in the future with less downtime
- Increase number of workers for each component based on available memory
- Always try to start Installer based on script from the currently running version when using other than the official latest version
- Remove letsencrypt option from certificate

ERM OS

Added

- Add CLI command ("cli") with support to, among other things, reset passwords and dump database content
- Allow ICMP echo requests ("ping")
- Allow overriding DNS when using DHCP
- Install traceroute
- Add support for EFI and Secure Boot (beta, new VM installations only)

Fixed

- Fix host security update files when upgrading system using offline bundle
- Set static routes after all interfaces are up
- Install systemd-timesyncd if the initial VM version did not include it
- Fix returning to menu after setting hostname

Security

- Upgrade host packages for bind9-libs, curl, dpkg, grub-common, grub-pc, grub2, hyperv-daemons, libc-bin, libexpat1, libssl1.1, libtasn1-6, libxml2, linux-image-cloud-amd64, linux-image-cloud-amd64 bind9-host, openssl, qemu-guest-agent, rsyslog, zlib1g
- Related CVEs: CVE-2021-22945, CVE-2021-22946, CVE-2021-30560, CVE-2021-3697, CVE-2021-3999, CVE-2021-4197, CVE-2021-4206, CVE-2021-4207, CVE-2021-46828, CVE-2021-46848, CVE-2022-0358, CVE-2022-1012, CVE-2022-1158, CVE-2022-1292, CVE-2022-1353, CVE-2022-1586, CVE-2022-1587, CVE-2022-1652, CVE-2022-1664, CVE-2022-1679, CVE-2022-1729, CVE-2022-1786, CVE-2022-20368, CVE-2022-20422, CVE-2022-20566, CVE-2022-20568, CVE-2022-2068, CVE-2022-22576, CVE-2022-2327, CVE-2022-24903, CVE-2022-2509, CVE-2022-2585, CVE-2022-2588, CVE-2022-2601, CVE-2022-2602, CVE-2022-26353, CVE-2022-27404, CVE-2022-27405, CVE-2022-27406, CVE-2022-27666, CVE-2022-27775, CVE-2022-27781, CVE-2022-27782, CVE-2022-2795, CVE-2022-28733, CVE-2022-28734, CVE-2022-29155, CVE-2022-29162, CVE-2022-29581, CVE-2022-29582, CVE-2022-2959, CVE-2022-2977, CVE-2022-30594, CVE-2022-3080, CVE-2022-31676, CVE-2022-3176, CVE-2022-32207, CVE-2022-32250, CVE-2022-34918, CVE-2022-3524, CVE-2022-3565, CVE-2022-3594, CVE-2022-3625, CVE-2022-3635, CVE-2022-36946, CVE-2022-3775, CVE-2022-38177, CVE-2022-38178, CVE-2022-40303, CVE-2022-40304, CVE-2022-40674, CVE-2022-41222, CVE-2022-4139, CVE-2022-42896, CVE-2022-43680, CVE-2022-43750, CVE-2022-4378, CVE-2022-47518, CVE-2022-47519, CVE-2018-13405

Changed

- Limit access for logs and system files, fix some CIS benchmark warnings, enable console timeout
- Install host security upgrades just after upgrading Installer, stop docker from potentially being upgraded automatically
- Discard some recurring kernel log messages about virtual container network interfaces
- Allow more userdata in cloud-init config
- Rotate log files more often
- Increase log file partition size (for new VMs)
- Decrease console log verbosity
- Change docker internal IP series to 100.64.10[3-5].0/16 to limit risk of conflicts (new VMs only)
- Change to GPT based partitions
- Add docker/-prefix to syslog tag, write container logs to separate files in /var/log/docker/
- Prepare for support for external syslog servers. Manual configuration should be moved to /etc/rsyslog.d/50-remote.conf
- Enable SSH login by default for new installation, enable fail2ban to lock logins after too many logins

Version 1.0.6

Added

- Add support for deployment as a cloud service in Microsoft Azure and Google Cloud Platform.
- Add support to override DNS entries for specific hosts
- Warn about missing CA/Intermediaries from certificate chain
- Add support for trusting load balancers using whole networks
- Support validating SSL CA trust against external server using network tools

- Improve error message when trying to browse to invalid FQDN/using IP to access services
- Add info about using offline mode until CA has been trusted when using HTTPS proxy
- Add support to export manually upgraded Installer version
- Add support to test HTTP requests in network tools
- Add choice to either uninstall component or remove it completely
- Display shortcuts to importing offline bundles when running in offline mode
- Display notice about required re-deploy after configuration change
- Display notice about required re-deploy after CA-change
- Validate uploaded private key/certificate and display warnings for mismatches
- Use global CA trust instead of dedicated CA bundle file for each component
- Support to remove not installed products from list

Fixed

- Fix upgrading Installer from CLI before setting license key
- Remove warning from load balancer logs about missing port
- Clearer error display of some forms visible in separate tabs
- Allow using domain names using leading digits
- Fix subject alt names in CSR generation, use meaningful filename
- Limit number of characters for fqdn-based service name and remove trailing special characters
- Don't try to output ldap metadata result
- Apply custom CA settings directly after save
- Fix offline bundle export of Installer
- Fix registry name for offline upgrades
- Use trusted custom CA in Installer as well as components
- Fix change password success message/redirect

Security

- Upgrade gzip
- Upgrade zlib1g, libssl
- Upgrade libexpat
- Related CVEs: CVE-2022-1271, CVE-2021-43618, CVE-2018-25032, CVE-2022-23852 CVE-2022-25235 CVE-2022-25236 CVE-2022-25313 CVE-2022-25315

Changed

- Indent each individual certificate in certificate bundle
- Display full chain in certificate textarea
- Separate general server settings form from network related settings
- Use separate virtual network for Installer load balancer
- Redirect to certificate details view after generating new certificate
- Include CSR generation in form header
- Replace self-signed server default certificate if component certificate uses the same FQDN
- Increase max length of LDAP filter
- Display select all-checkbox at top of Log view as well as at bottom
- Prepare offline export and display log before file download
- Improve help texts for CA certificates
- Pre-populate server IP/hostname on first boot

Using the ERM Installer

ERM Installer: initial setup and license management

The ERM Installer is used to install and configure the Enhanced Room Management suite of products. This topic describes how to set up the password for the installer and activate your license key.

It assumes that you have already followed and completed the set up of the ERM Installer virtual machine in your server network. If not, please see Deploying the ERM Installer virtual machine before proceeding.

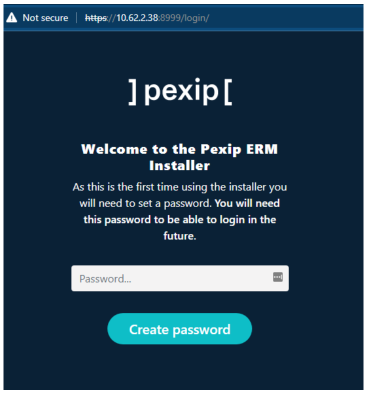
After completing the set up of the ERM Installer virtual machine, the VM's IP address and URL is displayed via the machine’s command line. Using a computer with access to the server’s network, enter the displayed URL into your browser to access the ERM Installer interface.

Note that browsing to the machine hostname requires correct records in your DNS. The ERM Installer can also be reached by IP address in the format `https://<IP address>:8999`.

Setting a password (on first time use)

The first time you access the ERM Installer via the browser you are asked to choose a password for your installation. This password is used for all future access to the installer, so it is important that you securely save this information.

Enter your desired password and click **Create password** to proceed.



Not secure | ~~https~~://10.62.2.38:8999/login/

Welcome to the Pexip ERM Installer

As this is the first time using the installer you will need to set a password. **You will need this password to be able to login in the future.**

After entering the password you are now logged in to the installer and the next step is to activate your license key.

Activating your license key

This section describes how to activate your license key if your server has access to the internet. If your server does not have internet access, see Installing and upgrading ERM in an offline environment instead.

If you have not yet entered a license key, there is a notice stating that you do not currently have an active license key. Click **Set license key** in the notice to proceed.

Note that the **Ignore verification errors and save anyway** option is primarily used in offline environments. Where the virtual machine has access to the internet, leave this option unselected so that it can validate the license and get a list of licensed components.

Enter the license key you received from your distributor and click on **Submit** to proceed.

If this is the first time you have used the installer and entered your license key, you are next taken to the general server settings.

Viewing your active license

You can see an overview and status of your current license key by going to **Settings > Active license**. This shows which products the license key applies to, and when the license key expires for each product.

Changing/updating a license key

You can change or update your license key by going to **Settings > Change license key**, and then selecting **Submit** to activate the new licenses.

However, the license will not be pushed to the ERM product until you **Deploy Changes** via the **Installation** menu. Please complete these steps to ensure the new licence becomes active within ERM.

Certificate management

TLS/SSL certificates are crucial for private information exchange and to validate that the received information has not been altered. The ERM Installer includes tools to help deal with these seemingly complex technologies.

Sometimes it can take a while to get access to valid certificates, which is why ERM Installer has tools to generate test certificates while waiting for the valid ones to arrive. To simulate a real environment, both a root CA issuer and an intermediate CA issuer is generated. Note that these should only be used in tests or proof of concept environments.

Certificate management tools

The certificate management tools are accessed by selecting **Certificates** which is located in the header navigation of the ERM Installer.

Use this tool to upload your certificate pairs and check certificate information. To help with demo-setups a self signed CA and certificate generation service is also included.

When first navigating to certificate management you get an overview which shows all of the available certificates. You can review information including the expiration date, upload date, and Issuer. You also have the choice to delete selected certificates.

Clicking on the title of a certificate from the overview brings you to the certificate details page for the specific certificate, where there are tools such as `update certificate`, `create CSR request` or `export private key`. For more information, see Certificate details below.

General information about certificates

Certificates files should use Base 64-encoded PEM format, and the public certificate should always include the full certificate chain for better compatibility with different services, video conferencing systems and web browsers i.e. the public certificate file should include the certificate for the service followed by intermediate certificate(s) and the root CA. If the file contains only one certificate some devices or services may not work correctly even if everything looks ok in the administrator's web browser.

Use external tools, e.g. https://www.ssllabs.com/ssltest/ or openssl from the command line `openssl s_client -connect pexip-erm.example.org:443` to validate your installation.

Example of a public key for pexip-erm.example.org opened in a text editor:

```
—-BEGIN CERTIFICATE—-
(pexip-erm.example.org content)
—-END CERTIFICATE—-
—-BEGIN CERTIFICATE—-
(Intermediate CA content)
—-END CERTIFICATE—-
—-BEGIN CERTIFICATE—-
(Root CA content)
—-END CERTIFICATE—-
```

Upload or generate certificates

Further down the certificate overview page are some tools for uploading new certificates, and to get the ERM Installer to generate temporary self-signed certificates for all products without assigned certificates. Lastly, there is an option to generate new certificates.

Certificate details

The certificate details page shows more information and tools for a specific certificate.

You reach this view by going to **Certificates** located in the header navigation of the ERM Installer, then clicking on the title of your desired certificate from the certificates overview.

Certificate general information

This shows a table with general information about the specific certificate. Scrolling down shows tools and actions for the certificate.

Update certificate

Use the form to update the certificate, choose a name and select your private key and public certificate and click **Update**. You also have the choice to delete the certificate.

Public certificate

You see the public certificate in the text field and also have the option to download the public certificate by clicking on **Download**.

Generate CSR

Create a CSR request, fill in the form and click **Generate CSR request**.

Export private key

Lastly you have the option to export the certificate private key, by clicking **Export**.

Using the ERM Installer to install and upgrade components

This topic explains how to upgrade the ERM Installer, upgrade an ERM module, and how to uninstall a module.

Upgrading the ERM Installer

If your primary ERM VM runs in online mode with direct access to the ERM docker image registry and OS update service then the latest installer images are automatically downloaded. The new installer version will start either when the VM is rebooted or when the administrator forces an upgrade via **Settings → Upgrade Installer** and selecting **Start upgrade**, followed by clicking reload in the terminal panel.

Note that the installer services will be unavailable for a short period as the upgrade completes and the services restart.

If the primary ERM VM is used offline, then an offline bundle must be prepared from the online ERM VM:

1. On the online ERM VM, go to **Settings > Upgrade Installer** and select **Export offline bundle of installer** to prepare the installer image.

   ℹ The offline file can be large and take several minutes to prepare. Please be patient and do not navigate away from the page.
2. Transfer the exported file using your preferred method (for example, a USB stick) to the second offline (air-gapped) VM.
3. Using the Installer on the second VM, go to **Settings > Handle offline bundle** and **Import** the file that was just exported.

For full details about offline bundles, see Installing and upgrading ERM in an offline environment.

ERM module upgrades/downgrades

If the ERM VM runs in online mode with direct access to the ERM docker image registry and OS update services, new versions of the licensed modules will show as available in the **Upgrade** dropdown box via **Installation > Installed Product > Details**. When a more recent (or a previous) version of the module is selected, you should click **Deploy changes** to complete the process.

ℹ The module's services will be unavailable for a short period as the changes are applied, and the services restart.

If the primary ERM VM is used offline, then an offline bundle must be prepared from the online ERM VM:

1. On the online VM, go to **Installation > Installed Product > Details**, select the version to upgrade (or downgrade) to via the **Upgrade** dropdown box, and then select **Export offline bundle** to prepare the module image.

   ℹ The offline file can be large and take several minutes to prepare. Please be patient and do not navigate away from the page.
2. Transfer the exported file using your preferred method (for example, a USB stick) to the second offline (air-gapped) VM.
3. Using the Installer on the second VM, go to **Settings > Handle offline bundle** and **Import** the file that was just exported.

For full details about offline bundles, see Installing and upgrading ERM in an offline environment.

Uninstalling a module

To uninstall a module, select the **Uninstall** option from the bottom of the version selection box, and select **Deploy changes**.

Installing and upgrading ERM in an offline environment

This topic describes how to deploy Enhanced Room Management when your primary ERM deployment has no direct Internet access.

If you have set up the ERM Installer virtual machine in an environment with internet access you may skip this article.

Overview

As outlined in the planning and prerequisites section, configuring your primary ERM deployment that has no direct Internet access requires two separate ERM virtual machines:

- A **primary** (main) VM that provides the main ERM functions, and is "air-gapped" from the secondary VM and the internet.
- A **secondary** ERM VM that has access to the Internet to activate licenses and fetch upgrades. The secondary VM plays no part in endpoint management — its sole purpose is to provide a simple way to activate or update your licence and fetch upgrades.

There is no difference in the images you deploy to each VM, just in how you configure and use them.

The license key is installed on both the secondary and primary VMs, however, it is only activated on the secondary server with Internet access. Therefore, while installing the license on the primary VM without Internet access, you should select the **Ignore verification errors and save anyway** option before proceeding.

In summary, to activate your primary ERM VM you have to export an "offline bundle" from the secondary ERM VM (after the license key has been activated and the ERM modules have been configured), then import that offline bundle into the primary ERM VM. The offline bundle contains the activated license authorization and all software components associated with the configured module available for that license key. The offline bundle is in the form of a large .bin file.

You may require several offline bundles depending on the options associated with your license key and the configuration of the primary ERM VM. For example, you may need an offline bundle for the ERM module(s) and a separate offline bundle for the ERM Installer.

The offline file can be large and take several minutes to prepare. Please be patient and do not navigate away from the page.

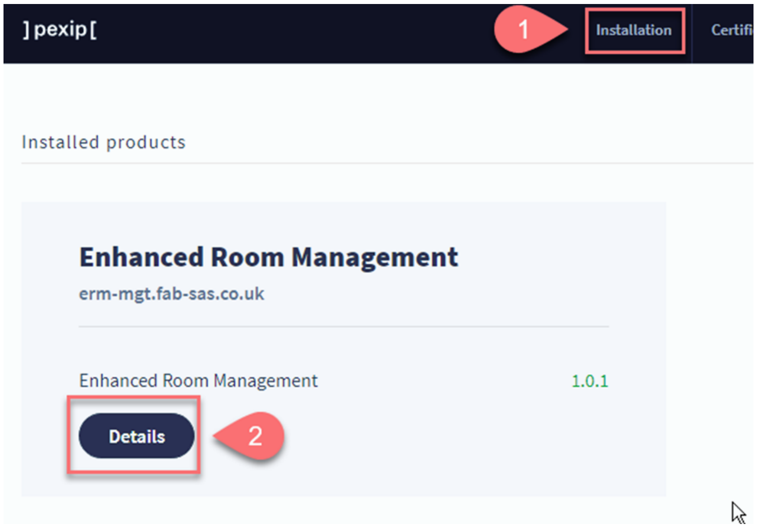
Procedure

This section describes the steps in detail to Install and upgrading ERM in an offline environment.

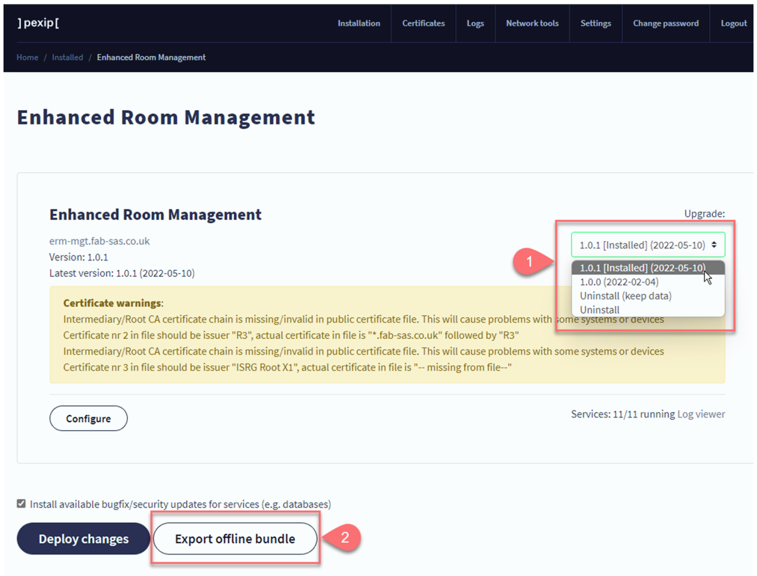
Install the secondary VM and export the bundle

On the secondary VM:

1. Follow the instructions to install an ERM virtual machine in an environment **with** internet access. See Deploying the ERM Installer virtual machine.
2. Enter your license key, ensuring you **do not select** the **Ignore verification errors and save anyway** option.
3. Install and configure the ERM module you want to use (as per normal for setting up a standalone ERM deployment, but using details that would apply to the offline environment, such as FQDN of the offline VM), then export the module bundle package(s) associated with your license key:
   a. On the secondary VM, configure the module you intend to bundle for offline. Please see Using the ERM Installer and Installing the ERM module for device management.
      You only need to specify the mandatory fields. The settings you configure will need to be re-entered when you configure the modules in your offline environment.
   b. On the secondary VM, in the ERM Installer menu, go to the **Installation** menu and click the **Details** button for the module you want to package.



c. Select the version of the module you want to export from the drop-down, then select **Export offline bundles**.



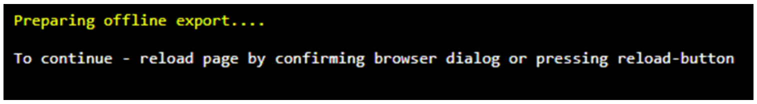
erm-mgt.fab-sas.co.uk
Version: 1.0.1
Latest version: 1.0.1 (2022-05-10)

Certificate warnings:
Intermediary/Root CA certificate chain is missing/invalid in public certificate file. This will cause problems with some systems or devices
Certificate nr 2 in file should be issuer "R3", actual certificate in file is "*.fab-sas.co.uk" followed by "R3"
Intermediary/Root CA certificate chain is missing/invalid in public certificate file. This will cause problems with some systems or devices
Certificate nr 3 in file should be issuer "ISRG Root X1", actual certificate in file is "-- missing from file--"

Services: 11/11 running Log viewer

☑ Install available bugfix/security updates for services (e.g. databases)

d. A new browser tab opens, and you see the following prompt:



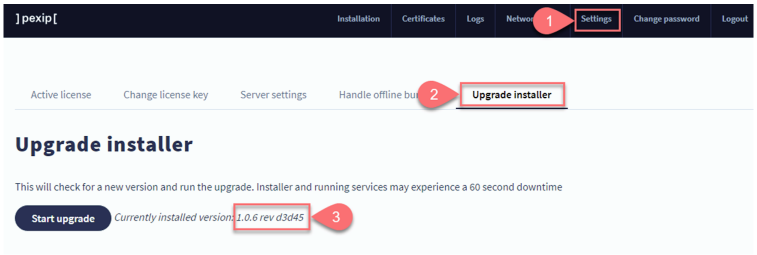
```
Preparing offline export....

To continue - reload page by confirming browser dialog or pressing reload-button
```

Do not close the tab. Wait for the offline bundle (in the form of a bin file) to start downloading.

ℹ The offline file can be large and take several minutes to prepare. Please be patient and do not navigate away from the page.

You can close the tab when the download is complete.

4. Optional. Export the offline bundle for the installer itself. This is only required if the installer version on the primary VM differs from the installer version on this secondary VM.
   a. First, you should check the ERM Installer versions on both primary and secondary ERM VMs by going to **Settings > Upgrade installer**. Review the versions on both systems and if the primary VM installer is at a lower version than the secondary VM installer, you should export the installer as an offline bundle and update the primary VM.

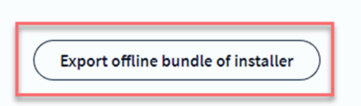


Upgrade installer

This will check for a new version and run the upgrade. Installer and running services may experience a 60 second downtime

Currently installed version: 1.0.6 rev d3d45

b. On the online secondary VM, select **Export offline bundle of installer**.



c. A new browser tab opens, although this will not show any information.

Do not close this tab. Wait for the offline bundle (in the form of a bin file) to start downloading. This can take 5 minutes, depending on the underlying host hardware, at which point the tab will close automatically.

d. Copy the exported file to your chosen media (such as a USB drive) for transfer to the primary ERM VM.

After completing these steps, the online secondary ERM VM can be switched off until the next upgrade. Its sole purpose is to enable you to activate or update your licence, and compile the correct version of software associated with your license key. It plays no role in the management of endpoints.

Install the primary VM and import the bundle

After exporting a bundle from the secondary VM, you can import it into the primary VM.

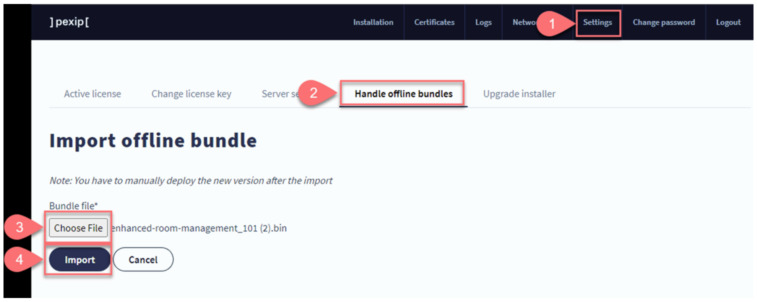
1. Follow the instructions to install an ERM virtual machine in an environment **without** internet access. See Deploying the ERM Installer virtual machine.
2. Enter your license key, ensuring you **select** the **Ignore verification errors and save anyway** option.
3. Enter the relevant server settings for your environment. See ERM Installer server settings.
4. Import into the primary VM the offline bundle(s) created previously:

   You can use this method to import either offline bundles created for the ERM module or the ERM Installer.

   a. On the primary offline VM, in the ERM Installer, go to **Settings > Handle offline bundle**.

   b. Select **Choose File**, and select the file you exported previously.

   c. Select **Import** to proceed.



Import offline bundle

Note: You have to manually deploy the new version after the import

Bundle file*

enhanced-room-management_101 (2).bin

5. After the offline bundle has been imported, you will have access to the new modules or installer functions.

ERM Installer server settings

The server settings configured in the ERM Installer (**Settings > Server settings**) are used as the default settings for all of the ERM modules that you later choose to install.

General server settings

This section contains the general settings for your server:

Setting	Description
Internal IP address of server	This IP address should be the same as for the virtual machine you set up for the Pexip ERM Installer. It is automatically filled in with the same value as on the server.
Internal hostname of server	Enter the hostname to use for your server, preferably the same hostname as the one you entered when you set up Pexip virtual machine (see VM deployment for more information).
Server is running on SSD / SAN instead of hard drive	This setting is for database management which will be optimized based on the selection you make here.
Allow sending traceback of unhandled errors to Pexip	This option enables the products to send traceback of unhandled errors back to Pexip for troubleshooting.
Trusted HTTP load balancer / reverse proxy IPS	It is common to have a firewall or load balancer that first receives calls and then forwards them to the server. By entering the IP address of the load balancer here, the actual IP addresses from the calls are stored in the logs instead of the IP address of the load balancer.
Timezone and default language	Choose which timezone and language to set as default for your upcoming product installations.

SSL settings

In the SSL settings section you can upload the various certificates that should be used by default when someone connects to the server.

The ERM Installer also has tools for creating certificates that are mainly used for testing or while waiting for the valid certificates. See Certificate management for more information.

ERM troubleshooting tools

To simplify the process of troubleshooting settings and installation, Pexip ERM Installer comes with tools to be able to test in your environment directly from Pexip ERM Installer.

You can access these tools by clicking on **Network tools** in the top navigation.

LDAP test

For troubleshooting your LDAP connection, this tool lets you quickly and easily test lookups in your LDAP. Simply fill in the fields and click on **Test LDAP query** and the result will appear for your request.

Network tools

Use these tools to verify DNS lookups and try connecting to different IP/TCP-ports directly from the server to check firewall and route settings.

Installing the ERM module for device management

This describes how to use the ERM Installer to install the ERM module for device management.

As a prerequisite you must have already deployed an ERM virtual machine, and set up the ERM Installer.

To get started, use your browser to go the URL of the ERM Installer. The ERM Installer start screen shows all the products that you have access to via your license key. Currently this is limited to just the ERM module.

On first use you need to **Configure** the module, and if you later return to the page you can view the current **Details** of the module, such as the software version number and also review any warnings that might exist, such as with its certificates, and make changes to the primary configuration.

This topic covers:

Installation settings

The installation settings are a combination of required and optional settings.

Hostname

In this section you specify the **Hostname / FQDN** of the product and select the SSL certificate to use.

See Certificate management for information about generating and uploading certificates.

Locale

The locale settings let you specify the default language (currently English or Swedish) and which timezone to use.

ERM uses the language setting in the web browser for the user interface, if that language is available. Otherwise it uses the nominated default language instead.

Other settings

The other settings let you specify the port on which to listen for proxy clients, and allow you to disable the proxy service.

LDAP authentication settings

You can optionally use an external LDAP / Active Directory database to authenticate users accessing ERM.

Overview

The ERM LDAP configuration includes the following elements:

- Access to a service account with read access to the Organizational Units (OUs) used to find user and security group objects.
- A base Distinguished Name (DN) path to provide the starting point for the LDAP search query.
- An LDAP user filter to provide a way to match users within the base DN path who should be provided access to the ERM interface.
- Security groups that can be used to provide permissions for two of the three types of ERM users (Admins and Superusers) and are defined using their LDAP Distinguished Names (DNs).

Three types of users can be granted access to ERM via LDAP with different permissions:

- **Support**: these users provide day-to-day ERM support and operations. They can add, remove and configure systems, schedule conferences, monitor call operations and statistics, perform firmware upgrades to the endpoints, etc.

  By default, users are granted this permission by simply existing within the defined base DN.
- **Admins**: these users have all the permissions of Support personnel plus additional permission to configure the ERM core application settings (such as setting base provisioning details and default endpoint passwords), plus the ability to check on proxy clients' connection statuses.

  By default, users are granted this permission through a specific Security Group.
- **Superusers**: These users have all the permissions of Admins plus the ability to manage the ERM backend system.

  By default, users are granted this permission through a specific Security Group.

Configuration

You can configure the following settings:

Setting	Description
Server	The address of the LDAP server.

Setting	Description
Service account DN/username	The distinguished name (DN) or username of the service account, for example **CN=Svc_ Pexip,OU=ServiceAccounts,DC=example,DC=org** or **user@example.org**
Password	The password for the service account / username. Use dash "-" to set an empty password.
Use LDAPS-connection	Select this option to use a secure connection. TLS may be used both with and without an LDAPS connection.
Ignore TLS/SSL verification errors	Select this option if you want to ignore TLS/SSL verification errors.
Base dn	Specify where in the tree the initial search for results should begin.
User filter	You can define how users are filtered out and displayed. ⓘ The default user filter allows any user object within the base DN path access to the ERM interface with a minimum of ERM support permissions. While you can control access to the ERM interface at the network level, it is generally considered good practice to ensure access permissions are only granted to users that require them. The default LDAP user filter may not, therefore, suit all enterprises. Please see the example below as to how you could provide more granular access.
Admin group DN	Specify which group in the tree has access to admin rights in the system (which enables additional settings and functions for the logged in user).
Superuser group DN	Specify which group in the tree has access to superuser status. Use this with caution as these users have full control over the system and should only be assigned to users with high technical knowledge.
Customer attribute	Enter attributes for the customer's shared key in multi-tenant installations.
Enable local accounts	Controls whether to allow login access to users in the local user database: ***Yes***: if the LDAP connection fails or is misconfigured then only local users that were manually added can log in. ***No***: if the LDAP connection fails or is misconfigured then nobody, including "pexip_fallback", can log in. Administrators can use the ERM Installer to test and reconfigure the connection. ***Unknown***: please ignore this option. Note that local users are managed by Superusers through Backend admin settings.
Read only	Select this option if you want to disable access to functions such as changing passwords, emails or other user information.
Remove optional setting	Select this option to remove this LDAP configuration i.e. to revert to local account access only.

The Pexip ERM Installer has tools to test your LDAP or AD settings to make it easier for you to troubleshoot and get started — see ERM troubleshooting tools for details.

We have also provided a worked example below to help explain how to use the settings in your environment.

Separate domain name for video conference system requests

This is an optional set of configuration for a separate domain name for video conference system requests. Enter the hostname and any settings for the certificates to be used.

Initial deployment

After you have gone through and filled in the necessary settings during the configuration and clicked on **Configure**, you are redirected to the step to deploy your ERM installation.

Start by selecting which version of ERM to install in the drop-down list to the right then click on **Deploy changes** to start the installation. You can now follow the installation process in a terminal that appears under the deploy button. When the installation is complete, you may reload the page and then you should see the correct version displayed for ERM.

The next step is to complete the onboarding wizard as described below.

Onboarding wizard

Open a web browser and go to the hostname that you entered for the installation. Note that the hostname you selected for your installation must be a valid record in your DNS.

You are met by the ERM onboarding wizard which takes you through the following configuration steps.

Organization

Enter a name and click continue. This is used as the default organization for your ERM installation.

Add Pexip cluster

The next step is to set up a Pexip video cluster. Start by filling in a description for the cluster followed by choosing Pexip Infinity and specifying the SIP address to use for the cluster.

Note that you can subsequently update the cluster configuration via **Backend admin > Clusters** (requires superuser permissions).

ℹ Adding a Pexip cluster and a Pexip Management Node only applies to self-hosted Pexip customers. Please skip this step if you are a Pexip Service customer.

Pexip Management Node

Add the details of your Pexip Management Node to your cluster:

Option	Description
Description	A short description for the Management Node.
IP address	The IP address for the node.
Ev. separate IP/host for API calls	Choose if you want network separation for all API calls, so that traffic goes through a separate hostname if, for example, you want to add firewall rules.
DNS Name	The DNS name of the Management Node.
Username and password	The username and password that ERM needs to use to connect to the Management Node.
Prepare event sink and external policy	These options are currently unused and should not be configured.

Note that you can subsequently update the Management Node configuration via **Backend admin > Meeting platforms** (requires superuser permissions).

Choose password

Here you may enter a password for the fallback user "pexip_fallback". We recommend that you set a password so you always have a fallback user for recovering the platform. You may skip this step, but you will then have to use one of your LDAP users for future access.

ℹ If the password for the fallback user is non-existent or forgotten, and the LDAP integration is down, password recovery is only available via the virtual machine. In this case please contact support for further assistance. **A password recovery in this way is a time-consuming process and that is why we always recommend setting a password for the fallback user which you then store in a safe place.**

Note that you can subsequently update the fallback user via **Backend admin > Users** (requires superuser permissions).

All done!

After completing the onboarding wizard you are now ready to start managing all your video conferencing systems.

Note that the onboarding wizard settings can be updated via the **Backend admin** options (requires superuser permissions).

Updating settings after deployment

After the installation of Enhanced Room Management is complete, you still have the option to change settings. To do this:

1. Select the installation you want to change from the Pexip ERM Installer start screen.
2. Click on **Configure** for the product whose settings you want to change.
3. When you have made your changes, click **Save**. This takes you back to the deployment of the product.
4. Click on **Deploy changes** to apply the new settings to your installation.

   ⓘ The module's services will be unavailable for a short period as the changes are applied, and the services restart.

After the installation process is complete you may now reload the page and your update is completed.

Online versus offline mode

If the primary ERM VM runs in online mode with direct access to the license activation services then the **Deploy changes** button completes the process.

If the primary ERM VM is used offline, then an offline bundle must be prepared from the online ERM VM:

1. On the online VM, go to **Installation > Installed Product > Details** and select **Export offline bundle** to prepare the module image.

   ⓘ The offline file can be large and take several minutes to prepare. Please be patient and do not navigate away from the page.
2. Transfer the exported file using your preferred method (for example, a USB stick) to the second offline (air-gapped) VM.
3. Using the Installer on the second VM, go to **Settings > Handle offline bundle** and **Import** the file that was just exported.

For full details about offline bundles, see Installing and upgrading ERM in an offline environment.

Example LDAP usage

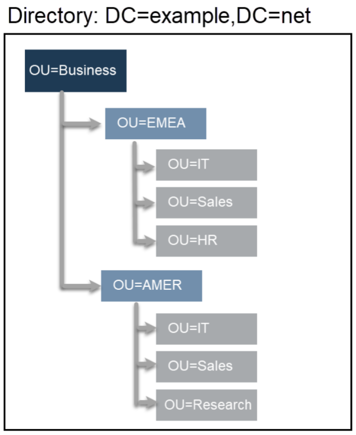
Here is a worked example of LDAP usage that you can use as a guide and adapt for your own organization.

Worked example

The following example is an enterprise using Microsoft Active Directory and a directory domain of **example.net**. This domain translates into the LDAP root path as being:

```
DC=example,DC=net
```

They have created a directory structure that maps their real-world organization and subdivides their users by geographical region and business function. In addition, they have created a base Organizational Unit (OU) called "Business" that contains all the sub-OUs. Their example structure is seen below:



ERM support personnel are located within the IT business function OUs, in the different regions. Their base DN path is therefore:

```
OU=Business,DC=example,DC=net
```

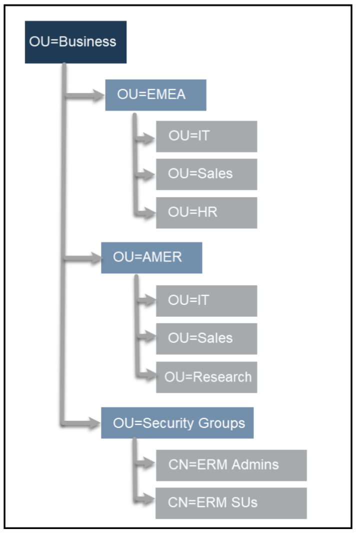
The default LDAP user filter is:

```
(&(|(sAMAccountName=%(user)s)(userPrincipalName=%(user)s)(uid=%(user)s))(objectClass=person))
```

This filter allows any user within the Base DN search path access to the ERM interface with ERM Support permissions. Therefore, sales, HR, and research users could technically access the ERM interface using the LDAP credentials. You could block these users' access at the network level, however, we will discuss how access permissions can be tightened by adjusting the LDAP user filter and creating an additional security group later.

Two security groups can be defined within ERM to provide additional permissions for ERM user access. Security groups allow users across different OUs to be gathered together, and permissions can be applied at the group level. For example, our organization uses a separate OU (named “Security Groups”) to contain all of its security groups. It then created two groups for its ERM Admin and ERM Superusers. We can, therefore, extend the directory diagram to show these groups:

Directory: DC=example,DC=net



The Distinguished Names (DNs) of these groups are then:

```
ERM Admins: CN=ERM Admins,OU=Security Groups,OU=Business,DC=example,DC=net
ERM Super Users: CN=ERM SUs,OU=Security Groups,OU=Business,DC=example,DC=net
```

We could limit user access to the ERM interface to users that exist solely within these security groups by extending the LDAP user filter by adding a `memberOf` property. For example, the LDAP search filter could become:

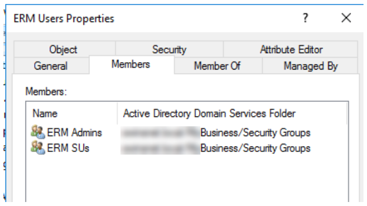
```
(&(|(sAMAccountName=%(user)s)(userPrincipalName=%(user)s)(uid=%(user)s))(objectClass=person)(|(memberOf=CN=ERM Admins,OU=Security Groups,DC=example,DC=net)(memberOf=CN=ERM SUs,OU=Security Groups,DC=example,DC=net)))
```

So, users within the base DN path but are only members of the ERM Admins, or ERM SUs security groups are allowed access.

The LDAP user filter currently has a limitation of **255 characters**. The above filter is 215 characters, so it is permissible. However, filters greater than 255 characters are truncated, therefore, will likely give erroneous results.

The result seems OK, however, the organization would like to give some users access to the ERM interface with only the support user permission. We could create an additional security group for ERM Support, but, applying another `memberOf` property to the LDAP filter would mean that the filter is greater than 255 characters and would be truncated. In addition, the `memberOf` property does not allow for wildcard matching, so an alternative method is required.

Security groups can be nested, so one group can be added as another group member. For example, our organization creates a general ERM Support Users security group, then adds the ERM Admin and ERM SUs groups to its members list, for example:

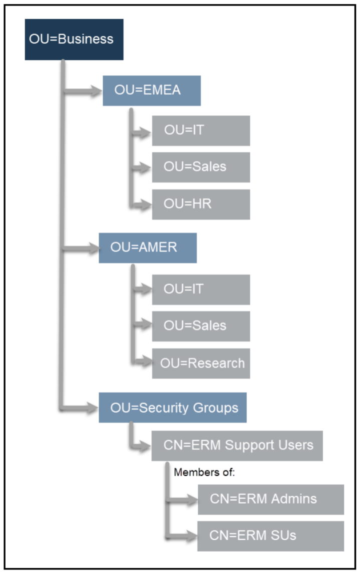


Members:

Name	Active Directory Domain Services Folder
ERM Admins	[redacted]Business/Security Groups
ERM SUs	[redacted]Business/Security Groups

We can further extend the directory diagram to show these group relationships:

Directory: DC=example,DC=net



Lastly, we can modify the LDAP Search filter to extend the `memberOf` property to search within the ERM Support User groups and any nested group. The numbers added to the `memberOf` property are an OID called LDAP_MATCHING_RULE_IN_CHAIN, which extends the match to provide a recursive lookup of nested objects within the given DN (see Ldapwiki: LDAP_MATCHING_RULE_IN_CHAIN), so the `memberOf` property needs to be exactly as shown below:

```
(&(|(sAMAccountName=%(user)s)(userPrincipalName=%(user)s)(uid=%(user)s))(objectClass=person)
(memberOf:1.2.840.113556.1.4.1941:=CN=ERM Support Users,OU=Security Groups,DC=example,DC=net))
```

The result is a filter which is 186 characters long, so it meets the current ERM LDAP user filter requirements. In addition, it allows access to users across multiple OUs but who only exist within the ERM Support Users group and its nested group siblings. Further, users are granted additional permissions within the nested ERM Admins or ERM SUs groups.

ERM dashboard

The ERM dashboard provides a summary of the current status of your system.

The top of the dashboard provides a summary of the different video conferencing systems that are connected to yourERM installation.

- **Total systems**: total number of your managed room systems.
- **Queued actions**: total number of queued actions for your room systems. Go to **Systems > Queue / history** for a list of all queued actions. See Queue / History for more information.
- **Non-approved systems**: number of non-approved room systems. Go to **Systems > Approve new systems** to get a list of the systems that need to be accepted before they are managed by ERM. See Approving new systems for more information.
- **Systems in calls**: total number of room systems that are currently in a call.
- **Systems online**: total number of the managed room systems that are currently online.
- **System with warnings**: total number of systems that currently have one or more warnings.

You can click any of the panels to get more details.

See ERM systems overview for more information about your managed systems.

ERM version

The panels on the right of the dashboard shows the current version of your ERM installation and its status:

- ◜ Status is loading.
- ✅ Everything is OK.
- ✔ The version has warnings.
- ❗ There are version errors.

By clicking on the version, you get more detailed information such as which version build that is currently in use and more information about any warnings and errors.

ℹ Always include this version information in your support tickets to enable faster troubleshooting.

Provisioning

The provisioning panel shows the passive provisioning settings to be configured in your video conferencing systems (found under **Setup > Configuration > Provisioning** in your system settings):

- **Address**: the current address for your Enhanced Room Management installation.
- **Path** : the provisioning path to use.
- **Type** : type of provisioning.
- **Protocol** : the protocol used when provisioning.
- **xConfiguration CLI**: click **View** to get all details as xConfiguration CLI which you can copy from the dialog that appears.

Enhanced Room Management: systems

This provides management of all video conferencing systems connected to your Enhanced Room Management installation.

ERM systems overview

From within ERM, select **Systems** via the main navigation in the left sidebar to get an overview of all of the currently available video conferencing systems. From this page you can also add new systems, approve systems that have been entered with a passive url, and view the actions that have already been, or are queued to be, applied to systems.

It has three main tabs:

- Overview
- Queue / History
- Approving new systems

You can use the actions at the top of the page to add either a single room system, or add multiple room systems at once:

- + Add a new room system.
- Add multiple room systems at once.

See Adding and approving new systems in ERM for more information.

Overview (search) tab

The default overview/search tab shows summary counts of your systems and highlights any with warnings or communication errors.

The list shows detailed information about all your managed room systems. The list is sortable by clicking on the heading for each specific column. It shows:

- **Name**: the name and model of the system. Clicking on the name takes you to the management of that system (see Viewing details of a system in ERM). It also shows the current status of the system:
  - ✓ the system is online (direct connection)
  - ✓ the system is online (passive connection)
  - ✓ the system is online (proxied connection)
  - ○ the system is offline (direct connection)
  - ○ the system is offline (passive connection)
  - ○ the system is offline (proxied connection)
  - ? unknown status
  - ☎ the system is in a call
  - 📅 the system has an active meeting
  - ⚠ error retrieving system status
- **URI**: shows which URI is used for the system.
- **IP**: the IP address of the system.
- **Other details**: this column is selectable. You have the following options: Serial number, Model, Group, Firmware, MAC address, E.164, H323 and Place are selectable.
- **System warning**: the final column indicates any warnings ⚠ .

Searching, filtering and grouping

You can search, filter and group the list.

Search

You can search the list by using the search field at the top left of the table.

Filter

Select the **Filter** button ▼ to display the filtering options:

- Firmware
- Status
- New systems only
- Webex-registered systems only
- Only Pexip service-registered systems
- Only system with warnings

When you have chosen your filters, click **Apply** to update the list.

Grouping

Select the **Grouping** button ▦ to display the grouping options:

- Per organization
- Per location
- Per model
- Per status
- Per connection

When you have chosen your groups, select **Apply** to update the list. (On larger screen resolutions the room system list is updated directly when changing your selection in the grouping form.)

Bulk editing

When you select one or more systems in the table using the checkbox, you can make changes to all of those systems at the same time. After selecting the systems, the available actions appear in a dialog at the bottom right of the screen:

Edit

Opens a dialog box for editing the selected systems with the following options:

- Password
- Number of seats in rooms
- Place
- Organizational unit

Provisioning

Opens a dialog to provision settings to the selected systems (this contains the same options as when provisioning an individual system). See ERM provisioning overview for more information.

Export

Exports the selected systems to Excel.

Delete

Removes the selected systems from ERM.

Queue / History

This table in the **Queue / History** tab lists upcoming and previous actions for the systems with an indicator of whether the action has been completed. Use the search and filtering functions to quickly find what you are looking for, e.g. you can filter on queued backup events.

Directly from the table, you can re-run actions by clicking ↻. You can also get more information about a specific action by clicking on ●.

If something went wrong, ⚠ is displayed as status; you can hover the mouse over the symbol to get more information, or click the ⓘ icon to show more details in a dialog.

Approve new systems

Video conference systems that have been entered with a passive URL need approval before the system is added to ERM.

See Approving new systems for details.

Adding and approving new systems in ERM

This topic describes how to add your video conferencing systems to be managed by Enhanced Room Management, including how to import endpoint details in bulk from TMS, and how to approve new systems.

ⓘ If Cisco TMS and Enhanced Room Management co-exist during a trial process or migration, you should disable the **Enforce management settings on systems** option in the **TMS Services** section on Cisco TMS. Otherwise, TMS may overwrite various settings.

From within ERM, select **Systems** via the main navigation in the left sidebar to get an overview of all of the currently available video conferencing systems.

In the top right of the page you can:

- + Add a single room system
- Adding multiple room systems at once / bulk TMS import
- ↻ Refresh the current page.

For more details on how to manage all your video conferencing systems, see ERM systems overview, and to change a system's dialing properties see Modifying a system's dialing properties.

Add a single room system

When adding a room system you should complete the following information (mandatory fields marked with *):

Setting	Description
Name	The system unit name displayed in the ERM list of endpoints and in the address book.
Username *	The username for the endpoint. Note that Webex registered endpoints require that an additional user with administrator privileges is created as the Webex admin password is not disclosed and any direct HTTPS access is by default only possible through Webex Control Hub. Default: admin
Sign in with default password *	If this option is selected, ERM will try to add the system with one of the passwords specified under **Admin > Settings** in ERM. If you clear the option you can manually add a specific password for the system. Default: selected.
IP address	The IP address enables ERM to connect directly to the endpoint.
Port to web interface	The port to use for the system’s web interface. Default: 443
Full DNS hostname	Optionally, enter the system’s DNS hostname. The hostname takes precedence over the IP address.
Automatically update IP data when sent from the system	Select this option if you want ERM to acknowledge and track IP address changes for the selected endpoint.

Setting	Description
Type of connection	Select how the endpoint is accessed: • Direct connection from ERM • By Pexip ERM proxy-client • Passive / behind firewall Default: Direct connection
MAC address	You can either specify the MAC address directly in advance so that the correct system is connected to ERM for passive provisioning, or to switch to another system. When the connection is active, this is retrieved automatically. If a passive connection is used the MAC address is received first after the system has been approved from the incoming list.
Place	Select a place (location) of the endpoint, e.g. headquarters, sales office, London office. This can be used for filtering and analytics.
Organizational unit	Select an organizational unit (OU) for the endpoint, e.g. IT-department or Sales. This can be used for filtering and analytics.
Number of seats in rooms	Enter the number of seats/chairs in the physical meeting room. This value is used for analytics and to show the efficiency of that particular room.
Personal system	Select this option to disable people count for the system, for instance, to not track if employees are at their desks. Default: not selected.

After adding your system you are automatically redirected to provisioning settings for the new system. See ERM provisioning overview for more details.

Adding multiple room systems at once / bulk TMS import

This option provides a form where you can specify many systems at the same time, and that have a few shared characteristics such as the connection type. Most settings are similar to adding a single endpoint as described above.

You can also select the **From Excel** tab to add multiple systems from an Excel file (.csv, .xls, .xlsx) and choose the appropriate columns as you import endpoints.

Endpoints can be exported from Cisco TMS (Tandberg Management System) and imported to ERM.

After adding your systems, a provisioning dialog automatically appears for provisioning settings to your newly added systems. See ERM provisioning overview for more details.

Approving new systems

Video conference systems that have been entered with a passive URL need approval before the system is added to ERM.

The table of systems in the **Systems > Approve New Systems** tab has these available details:

- **ID**: the system ID.
- **Name** : the name of the system.
- **IP** : the system's IP address.
- **Created** : date when the system was added.

Select **Approve** to approve the new system or select 🗑 to remove it from the list.

Viewing details of a system in ERM

You can view a system's details by selecting the system's name from the ERM **Systems** overview page.

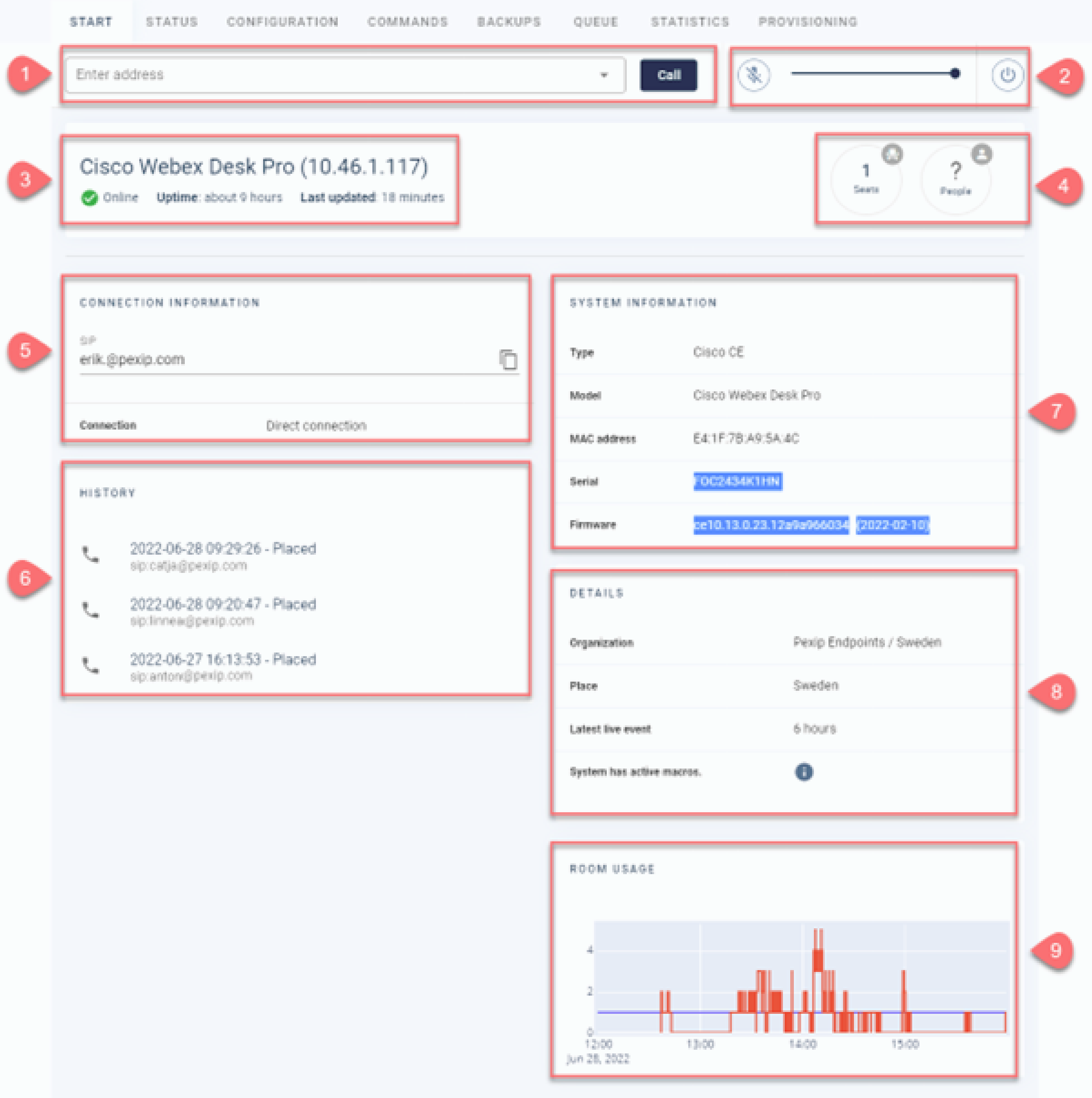
The initial view (also known as the system's dashboard) provides an overview of the system’s current status and settings, and further options are available such as to call addresses, change volume, restart the system or provision new settings.

From the top of the page you can:

- ✎ Edit system settings (see Adding and approving new systems in ERM)
- 🗑 Remove the system from ERM.
- ⚙ Go to a debug view for the system.
- ↻ Refresh the current page.

Start

The initial view is the **Start** tab and is broken up into the following elements:



Cisco Webex Desk Pro (10.46.1.117)
Online **Uptime**: about 9 hours **Last updated**: 18 minutes

SIP
erik.@pexip.com

Connection Direct connection

2022-06-28 09:29:26 - Placed
sip:catja@pexip.com

2022-06-28 09:20:47 - Placed
sip:linnea@pexip.com

2022-06-27 16:13:53 - Placed
sip:anton@pexip.com

Type	Cisco CE
Model	Cisco Webex Desk Pro
MAC address	E4:1F:7B:A9:5A:4C
Serial	FOC2434K1HN
Firmware	ce10.13.0.23.12a9a966034 (2022-02-10)

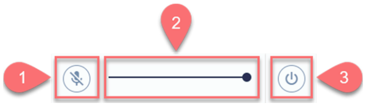
Organization	Pexip Endpoints / Sweden
Place	Sweden
Latest live event	6 hours
System has active macros.	ⓘ

1. Call control

The **Enter address** drop-down box allows a remote support person to dial another device or service from this system. By default, the list is populated with the names of the other systems managed by this ERM instance but it can also be overridden with any valid dial string.

For example, to make this system dial into a VMR service, you could use a SIP URI: **vmr@pexample.net**, or to dial into a VMR service that requires a PIN code of 1234, the you could extend this URI using the # option: **vmr#1234@pexample.net**.

2. System control



These controls allow you to control some aspects of the system remotely:

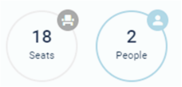
1. Mute/unmute the system.
2. Set the output volume of the system.
3. Restart the system.

3. System title and connection status

This displays the title of the system, its IP address, connection status, uptime, and last update time stamp. Hovering over the connection status icon gives further detail on this status. The icon varies depending on the type of connection the endpoint has to the ERM instance (direct, passive, or proxied) and the status of the connection:

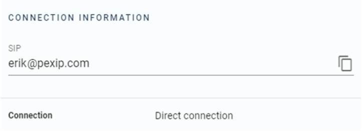
- ✓ the system is online (direct connection)
- ✓ the system is online (passive connection)
- ✓ the system is online (proxied connection)
- ○ the system is offline (direct connection)
- ○ the system is offline (passive connection)
- ○ the system is offline (proxied connection)
- ? unknown status
- ☎ the system is in a call
- 📅 the system has an active meeting
- ⚠ error retrieving system status

4. System seat and people count (dependent on the features being available on the system):



- **Seats**: refers to the maximum number of users that would typically use this system.
- **People**: refers to the number of people detected in front of the camera by the system.

5. Connection information



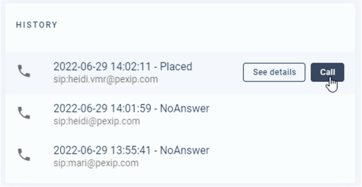
CONNECTION INFORMATION

SIP
erik@pexip.com

Connection Direct connection

This shows the aliases (SIP, email, H.323 etc) that are assigned to the system, which can also be copied to the user clipboard by clicking the copy button (⧉) . The type of connection from the system to ERM can also be seen, i.e. Direct connection, Passive behind firewall, or Proxy,

6. Historical call list



HISTORY

2022-06-29 14:02:11 - Placed
sip:heidi.vmr@pexip.com

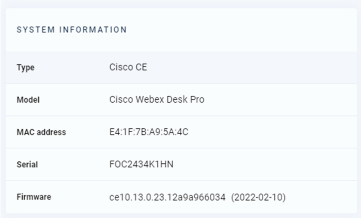
2022-06-29 14:01:59 - NoAnswer
sip:heidi@pexip.com

2022-06-29 13:55:41 - NoAnswer
sip:mari@pexip.com

The historical call list shows the last few calls to or from the system. You can hover over a call to view further details (which for Cisco systems could also be retrieved by issuing an xCommand CLI API call). This CDR data from the endpoint outlines items including; the call protocol, bandwidth signaled, and media statistics.

In addition, the **Call** button lets you easily re-dial the previous device or service.

7. System information

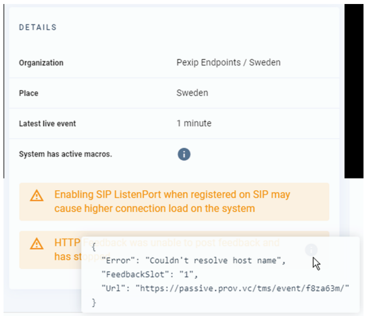


SYSTEM INFORMATION

Type	Cisco CE
Model	Cisco Webex Desk Pro
MAC address	E4:1F:7B:A9:5A:4C
Serial	FOC2434K1HN
Firmware	ce10.13.0.23.12a9a966034 (2022-02-10)

This section shows general system information, such as the make and model, MAC address, serial number and currently installed firmware version.

8. Details



DETAILS

Organization	Pexip Endpoints / Sweden
Place	Sweden
Latest live event	1 minute
System has active macros.	🛈

⚠ Enabling SIP ListenPort when registered on SIP may cause higher connection load on the system

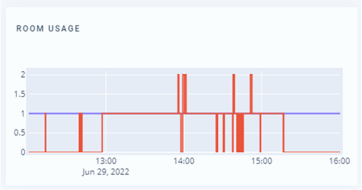
⚠ HTTP Feedback was unable to post feedback and has stopped

```
{
  "Error": "Couldn't resolve host name",
  "FeedbackSlot": "1",
  "Url": "https://passive.prov.vc/tms/event/f8za63m/"
}
```

This shows further system details, such as the Organization Unit where the system is deployed, its location, last live event status update, any system warnings or errors, and whether the system has active macros.

Hovering over the informational icons (🛈) shows additional information.

9. Room stats (dependent on the features being available on the system)



Shows a graph outlining the available seat and total occupancy for the last day.

Status

Shows a detailed view of the current status of each setting for the system. For a Cisco system, this is the same as viewing the Setting > Statuses page directly from the endpoint.

You can navigate between the different setting areas via the tabs to the left, or use the search function to find what you are looking for quickly.

By clicking on **Create report** (🗎) you can then choose which different types of settings that you want to generate a report for in the status list. When you are ready with your choices click **Select system** (☰) to compare the selected settings with other managed room systems in your installation.

Configuration

This is similar to status, but shows all of configurable items available for a system. This is the same as viewing the Setting > Configurations page directly from a Cisco endpoint.

You can adjust multiple settings and apply them to the endpoint directly, or save them as a template to be reused (e.g. when a new system is added or creating a system-wide default configuration).

Similar to status, you get the various settings available for the system. The difference is that you can choose to provision new settings or save a number of different settings as templates for which can be reused e.g. when a new system is added.

See Provisioning configurations to an ERM system for more information on how to work with configurations.

Commands

This provides a GUI interface to issue API commands to a system. You can execute individual commands or create a queue to run multiple commands simultaneously. You can also save a queue of commands as a template to reuse later.

Get an overview of all available commands for the system. You can quickly run specific commands directly, or run multiple commands from a queue. You can also save a queue of commands as a template to reuse at a later time.

For more information on how to work with configurations in Enhanced Room Management, please see getting started documentation for provisioning commands.

Backups

Here you can manage system backups.

The table gives you an overview of previously created backups where you can directly download, restore and delete backups.

You can create new backups by clicking on the + icon located at the top right of the page. This starts a backup process in the background which will be automatically added to the list as soon as it is complete.

Queue

This table lists upcoming and previous actions for the system with an indicator of whether the action has been completed. Use the search and filter functions to find specific actions.

You can use the icons to rerun actions or find out more information:

↻ — rerun the action.

ⓘ — get more information about a specific action.

⚠ — an error occurred; hover over the symbol to get more information about what might have gone wrong.

Statistics

Call statistics of "hours used per day" are available for all systems by default, while systems that support people count show several other graph types.

Provisioning

Provisions new settings for the system. See ERM provisioning overview for more information.

Enhanced Room Management: provisioning

Enhanced Room Management supports provisioning configurations, commands, firmware, branding and macros/panels to one or multiple room systems.

ERM provisioning overview

ERM supports the provisioning of configurations, commands, firmware, branding and macros/panels to one or more room systems.

Each room system in ERM has its own provisioning view, which is reached by selecting the system you want to provision and then clicking the **Provisioning** tab located under the heading on the room system’s start screen.

For detailed information about the types of system connections and provisioning options that are available within ERM, see ERM system connections and provisioning details.

Provisioning options

Inside the provisioning view you have the option of provisioning a number of different types of settings:

Update configuration

You can update different configurations for the room system. You have a choice of options:

- **From a template**: if you have already saved templates, you can load the settings here by clicking **Load** for the desired template. You can click on the information icon next to the **Load** button to get an overview of all the configurations of the template.
- **From a system**: you can load an entire configuration that applies to another room system. Select the system you want from the system list and click on **Load settings**.
- **Edit manually**: change the configurations manually. All configurations for the selected system are displayed here and you can select the required configurations by clicking each checkbox. When you are ready, click on the **Review** tab to get an overview of your choices.
- **Review**: after you have loaded configurations from a template, an existing system or have manually selected configurations yourself, an overview of your choices is always displayed under the **Review** tab. You can check all values before they are provisioned to the system.

Run custom commands

You can run custom commands from a template against a system.

Subscribe to live updates

This sends commands to the room system to start subscribing to live updates. The slot used for this is determined by the setting in **Admin > Settings > HTTP Feedback Slot**.

Next to this option, a notice is also displayed about when the system last received a message from live updates.

Change password

This changes the password for the room system. You can either choose to set the default password (as defined in **Admin > Settings > Default password**). If several passwords have been entered under the settings, the first password is used.

You can also choose to set a completely different password by clearing **Use default password** option and then entering your own password.

Change passive room analysis

Controls which type of passive room analysis should apply.

- **People count out of call**: if activated, the system will send information about people count even when the system is not in a call.
- **Detect presence**: if activated, the system will send events if it senses that a person is in the room.

Note that these features are not supported for all types of systems.

Get previous statistics

If this option is selected, the room system will send all its previous statistics to ERM.

Set up passive provisioning

Sets up the system to use passive provisioning.

Use address book

Provisions an address book for the room system. By selecting this option you can then choose which address book you want to provision via the drop-down list. These address books are created and managed through **Address books**.

Use branding

Provisions the branding the room system should use. By selecting this option you can then choose which branding you want to provision via the drop-down list. These branding profiles are created and managed via **Admin > Branding profiles**.

Upgrade firmware

Provisions new versions of the room system's firmware. Which firmware is selectable in the dropdown list depends on what is stored under **Firmware**.

Apply macros/panels

Provisions room controls to a room system. You create and manage all your room controls under **Panels and macros**. See Panels, macros, room controls and collections for more information.

Dialing properties

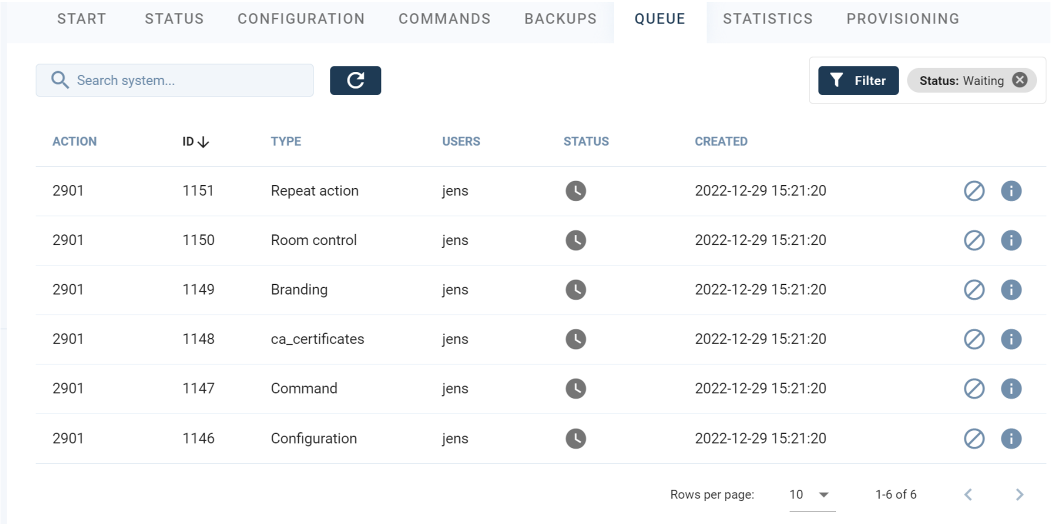
Changes the dialing properties that apply to the room system. If the room system has been edited and new information has been entered, these are shown here, but they are updated in the room system only after the provisioning has been applied.

For Pexip use cases, you can add the system to the Pexip's device registration by selecting the **Register new aliases in Pexip** option.

Applying the changes

When you are ready, you can either click **Apply** to provision the new settings immediately, or click **Schedule** to select whether to schedule the provisioning actions to happen ***One night only*** or ***Every night***.

Every night means that the provisioning actions you choose will be executed once every day. Scheduled actions can be found under the **Queue** tab on each system:



ACTION	ID ↓	TYPE	USERS	STATUS	CREATED	
2901	1151	Repeat action	jens	◷	2022-12-29 15:21:20	⊘ ⓘ
2901	1150	Room control	jens	◷	2022-12-29 15:21:20	⊘ ⓘ
2901	1149	Branding	jens	◷	2022-12-29 15:21:20	⊘ ⓘ
2901	1148	ca_certificates	jens	◷	2022-12-29 15:21:20	⊘ ⓘ
2901	1147	Command	jens	◷	2022-12-29 15:21:20	⊘ ⓘ
2901	1146	Configuration	jens	◷	2022-12-29 15:21:20	⊘ ⓘ

If you want to cancel an ***Every night*** scheduled repeated action you need to find the event with the type **Repeat action** and press the Cancel button ⊘.

Provisioning multiple room systems

The same provisioning form is used to provision to several room systems simultaneously. Start by navigating to the list of all systems and In the list view you can then select one or more systems by clicking in the checkbox for the systems you want to select.

A dialog appears in the lower right corner where you can select **Provisioning** to open a provisioning dialog. In this case everything that you choose to provision is sent to all selected systems.

ERM system connections and provisioning details

This topic provides detailed information about the types of system connections and provisioning options that are available within ERM.

It covers the following areas:

- Provisioning terminology
- Understanding TLS certificates within the provisioning and connection processes
- Understanding TLS certificates for a Cisco endpoint
- Provisioning and connection types
    - Direct connection
    - Direct provisioning with a direct connection
    - Passive connection (and passive provisioning)
    - Differences in functionality when using a passive connection as opposed to a direct connection
    - Passive provisioning combined with a direct connection
    - Chained provisioning (technical preview)

Provisioning terminology

The following table contains a list of many of the terms used in the context of ERM connections and provisioning.

Term	Definition
System	A videoconferencing endpoint or room added to ERM. Currently, Cisco endpoints are supported as outlined here.

Term	Definition
Provisioning	The ability for an administrator to apply centrally defined and managed configuration sets for systems within an estate. These configuration sets can be applied in two ways: • **Direct provisioning**: ERM pushes configuration changes towards a system. • **Passive provisioning**: a system pulls configuration changes from the ERM service.
Chained provisioning	In addition to the provisioning types mentioned above, ERM allows an administrator to use provisioning from the Pexip Service. A system uses passive provisioning towards ERM, and ERM then proxies those provisioning requests towards the Pexip Service. The provisioning responses are then sent from the Pexip Service to ERM and back to the system.
Connection	For a system to obtain provisioning information, there must be a network connection to ERM: • **Active connection**: ERM can send new requests to a system. This is required for direct provisioning. An active connection in itself can be achieved in two ways: ○ **Direct**: the connection from ERM to a system is directly routable. ○ **Via ERM Proxy Client**: the connection from ERM to a system is routed via an ERM Proxy instance. • **Passive/behind a firewall**: the system is not routable from ERM, however, the system is able to send new requests to an ERM service. This is required for passive and chained provisioning.
Live event updates	A system can send updates to ERM regarding various processes (such as call details or presence information). While similar to passive provisioning requests, these updates are sent using separate new requests.

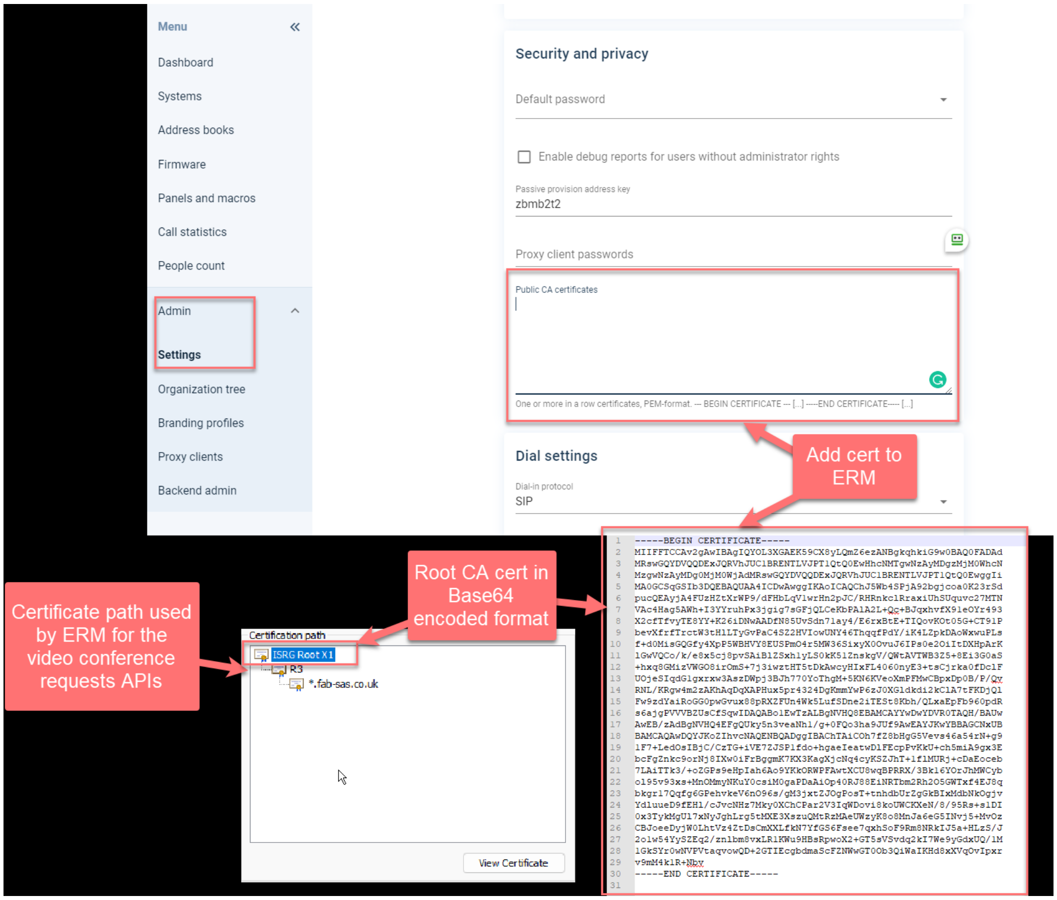
Understanding TLS certificates within the provisioning and connection processes

To understand how the provisioning of Cisco endpoints and live event updates work, you need to know how TLS certificates work within these processes.

Understanding TLS certificates within ERM

An ERM VM contains the management GUI and the videoconferencing system request API endpoints. You can use a single FQDN for both services, or (more commonly), you can add an optional FQDN to use specifically for the video conference system requests. These are configured via the ERM Installer interface in the **Installation > (ERM Installation) Details > Configure** options. The **Hostname** page shows the FQDN applied to the ERM management interface; if the optional setting under **Separate domain name for video conference system requests** is **not** configured, then the Cisco endpoints will also use this FQDN when they connect to ERM for provisioning information.

Alternatively, if you want the endpoints to use a separate FQDN for the provisioning service, then you can specify that in the optional **Separate domain name for video conference system requests** setting.



Security and privacy

Default password

□ Enable debug reports for users without administrator rights

Passive provision address key: zbmb2t2

Proxy client passwords

Public CA certificates

One or more in a row certificates, PEM-format. — BEGIN CERTIFICATE — [...] ----END CERTIFICATE---- [...]

Dial settings

Dial-in protocol: SIP

Add cert to ERM

Root CA cert in Base64 encoded format

Certificate path used by ERM for the video conference requests APIs

```
-----BEGIN CERTIFICATE-----
MIIFFTCCAv2gAwIBAgIQYOL3XGAEK59CX8yLQmZ6ezANBgkqhkiG9w0BAQ0FADAd
MRswGQYDVQQDExJQRVhJUClBRENTLVJPT1QtQ0EwHhcNMTgwNzAyMDgzMjM0WhcN
MzgwNzAyMDg0MjM0WjAdMRswGQYDVQQDExJQRVhJUClBRENTLVJPT1QtQ0EwggIi
MA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQChJ5Wb4SPjA92bgjcoa0K23rSd
pucQEAyjA4FUzHZtXrWP9/dFHbLqV1wrHn2pJC/RHRnklRraxiUhSUquvc27MTN
VAc4Hag5AWh+I3YYruhPx3jgig7sGFjQLCeKbPAlA2L+Qc+BJqxhvfX91eOYr493
X2cfTfvyTE8YY+K26iDNwAADfN85UvSdn7lay4/E6rxBtE+TIQovKOt05G+CT91P
bevXfrfTrctW3tH1LTyGvPaC4SZ2HVIowUNY46ThqqfPdY/iK4LZpkDAoWxwuPLs
f+d0MisGQGfy4XpP5WBHVY8EUSPmO4r5MW36SixyX0OvuJ6IPs0e2OiItDXHpArK
1GwVQCo/k/e8x5cj8pvSAiBlZSxhlyLS0kK5lZnskgV/QWtAVTWB3Z5+8Ei3G0aS
+hxq8GMizVWGO8irOmS+7j3iwztHT5tDkAwcyHIxFL4060nyE3+tsCjrka0fDclF
UOjeSIqdG1gxrxw3AszDWpj3BJh770YoThgM+5KN6KVeoXmPFMwCBpxDp0B/P/Qv
RNL/KRgw4m2zAKhAqDqXAPHux5pr4324DgKmmYwP6zJ0XGldkdi2kClA7tFKDjQl
Fw9zdYaiRoGG0pwGvux88pRXZFUn4Wk5LufSDne2iTESt8Kbh/QLxaEpFb960pdR
s6ajgPVVVBZUsCfSqwIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUw
AwEB/zAdBgNVHQ4EFgQUky5n3veaNhl/g+0FQo3ha9JUf9AwEAYJKwYBBAGCNxUB
BAMCAQAwDQYJKoZIhvcNAQENBQADggIBAChTAiCOh7fZ8bHgG5Vevs46a54rN+g9
1F7+LedOsIBjC/CzTG+iVE7ZJSPlfdo+hgaeIeatwDlFEcpPvKkU+ch5miA9gx3E
bcFgZnkc9orNj8IXw0iFrBggmK7KX3KagXjcNq4cyKSZJhT+1flMURj+cDaEoceb
7LAiTTk3/+oZGPs9eHpIah6Ao9YKkORWPFAwtXCU8wqBPRRX/3Bk16YOrJhMWCyb
o195v93xs+MnOMmyNKuY0csiM0gaPDaAiOp40RJ88EiNRTbm2Rh2O5GWTxf4EJ8q
bkgrl7Qqfg6GPehvkeV6nO96s/gM3jxtZJOgPosT+tnhdbUrZgGkBIxMdbNkOgjv
YdluueD9fEHl/cJvcNHz7Mky0XChCPar2V3IqWDovi8koUWCKXeN/8/95Rs+s1DI
0x3TykMgUl7xNyJghLrg5tMXE3XszuQMtRzMAeUWzyK8o8MnJa6eG5INvj5+MvOz
CBJoeeDyjW0LhtVz4ZtDsCmXXLfkN7YfGS6Fsee7qxhSoF9Rm8NRkIJ5a+HLzS/J
2olw54YySZEq2/znlbm8vxLRlKWu9HBsRpwoX2+GT5sVSvdq2kI7We9yGdxUQ/1M
1GkSYr0wNVPVtaqvowQD+2GTIEcgbdmaScFZNWwGT0Ob3QiWaIKHd8xXVqOvIpxr
v9mM4klR+Nbv
-----END CERTIFICATE-----
```

You can then assign a TLS certificate to each of these services. Assuming you are using PKI (consisting of a Root Certificate Authority and potentially one or more Intermediate Certificate Authorities), then the certificate file uploaded to ERM should be in the format of a PEM bundle. For example, this file would contain the actual TLS certificate for the ERM service, concatenated with any intermediate CA certificates used in the signing process. You do **not** need to append the root CA certificate to the bundle (and you can ignore the error shown in the ERM Installer interface suggesting that the root is missing).

You do, however, need to add the root CA certificate used to terminate the chain of trust for the ERM TLS certificate to the ERM management GUI via the **Admin > Settings > Trusted CA Root Certificates** setting. These root certificate(s) then need to be pushed to the Cisco endpoint (either automatically or manually) so that it can terminate the TLS chain and form a trust relationship with the ERM service.

Note that alternative certificate chains may be used if there is some intermediate infrastructure between the Cisco endpoint and ERM (such as a reverse proxy or load balancer). In this case, adding all CA root certificates that terminate these chains to the ERM **Trusted CA Root Certificates** setting is practical.

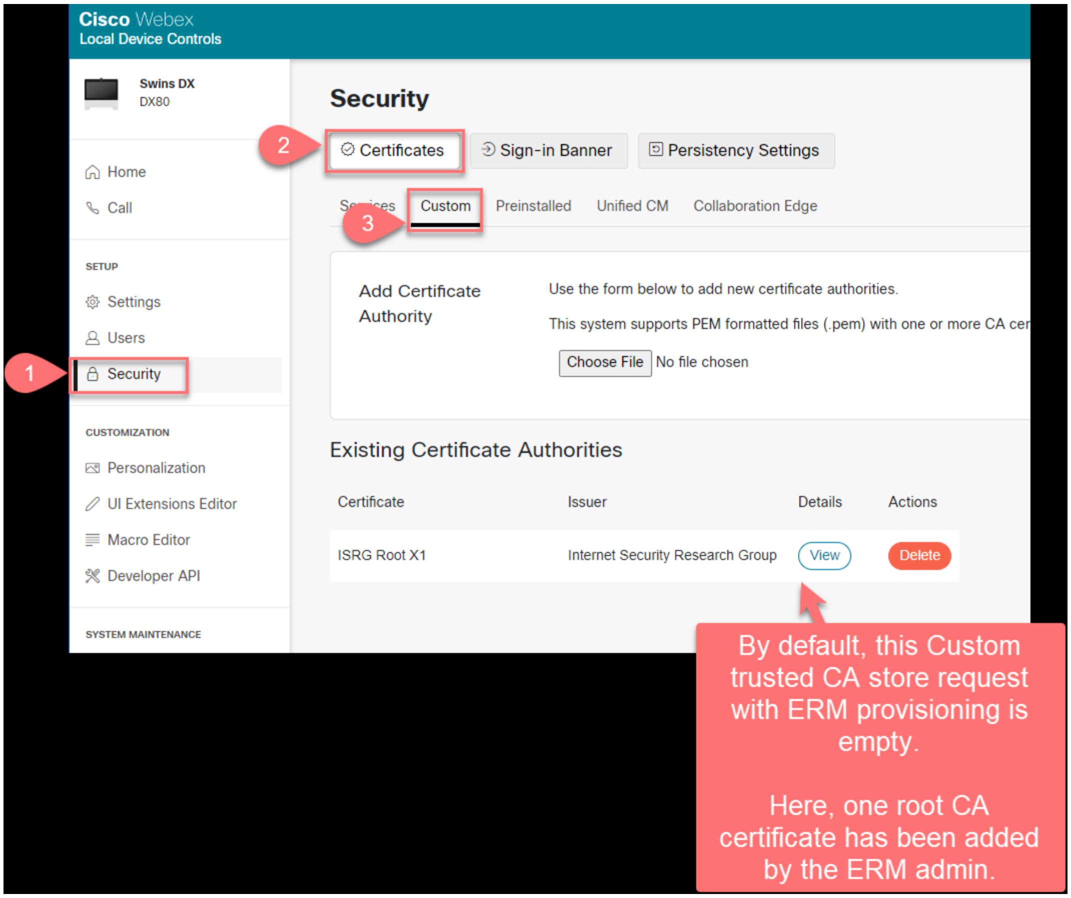
Understanding TLS certificates for a Cisco endpoint

Why do you need to add CA root certificates to the Cisco endpoints?

A Cisco endpoint has multiple trusted CA stores that are pre-populated with public roots, and different HTTP request types made from an endpoint are associated with the different trusted CA stores, which can cause some confusion. Two of these default Trusted CA stores on an endpoint are populated with a typical list of public root CA certificates, which means that the endpoint will trust some HTTP services that have publicly issued TLS certificates assigned to them. For example, one of these stores is used for provisioning. However, it is only used when provisioning occurs via CUCM and the Expressway. ERM uses the passive provisioning system from TMS (Telepresence Management Server), and for this HTTP request, the endpoint relies on its **Custom trusted CA store**, which by default is empty. Therefore by default, a Cisco endpoint will **not** trust any certificate chain presented to it from ERM when it connects to the provisioning service, be it from a private or public PKI.

Therefore, you must ensure that the endpoint has the correct root CA certificate(s) uploaded to its Custom trusted CA store so that it will trust the TLS certificate presented by ERM or any intermediate proxy.

Note that you can bypass the certification validation by switching off the **TlsVerify** settings on the endpoint, however, this is not recommended.



Add Certificate Authority

Use the form below to add new certificate authorities.

This system supports PEM formatted files (.pem) with one or more CA cer

Choose File No file chosen

Existing Certificate Authorities

Certificate	Issuer	Details	Actions
ISRG Root X1	Internet Security Research Group	View	Delete

By default, this Custom trusted CA store request with ERM provisioning is empty.

Here, one root CA certificate has been added by the ERM admin.

Additional information

- For passive provisioning, you can check the configuration on a Cisco endpoint within **Settings (or Status) > Provisioning** (or by running `xStatus Provisioning` against the endpoint's API).
- ERM typically subscribes to **Live Event Updates** from an endpoint, allowing that endpoint to update ERM regarding call usage and other statistical information. A Cisco endpoint uses multiple **HTTP feedback slots** to connect to various HTTP event sink servers. By default, ERM configures HTTP feedback slot 4 to enable the endpoint to send live updates of call events towards ERM (using similar information such as the ERM URL and path used for the passive provisioning configuration). Again, the Cisco endpoint uses its Custom trusted CA store to terminate the TLS chain presented by the ERM service when it sends these live updates. You can reconfigure the HTTP feedback slot used by ERM via the **Admin > Settings > Base > HTTP Feedback slot** option.
- You can check the status of the HTTP Feedback slots configured on a Cisco endpoint by viewing the HttpFeedback configuration from the **Settings > Status > HttpFeedback page** in the HTTP GUI. Alternatively, you can run the `xStatus HttpFeedback` API command on the endpoint.

Provisioning and connection types

Direct connection

With direct connections, the ERM server connects directly to the Cisco endpoint’s API and immediately pushes configuration information that the endpoint will use. You can also directly control the endpoint (by pushing commands such as dial strings or mute/unmute options), providing a facility for white glove operators to manage the endpoint directly from ERM.

To enable the endpoint to feed back live updates to ERM regarding call details, occupancy etc. ERM can push configuration to the endpoint to update one of its HttpFeedback slots (four are available on a Cisco endpoint) used to send event data to a listening server. By default, ERM configures HttpFeedback slot 4 on the endpoint. To enable this, ERM pushes its URL (based on the ERM FQDN) that directs the endpoint to connect to the ERM server. In addition, it should push the Root CA certificates as added via the ERM Management GUI in the **Admin > Settings > Trusted CA Root Certificates** setting (as described above).

If you do not configure ERM to subscribe to live updates from an endpoint, or you fail to provision the correct root CA certificate on an endpoint, you will likely see system errors and warnings in the ERM management GUI status dashboard.

Ensure that you select the following options in the **Systems > (System to update) > Provisioning** tab (and we recommend ensuring they are set even if there is a green "Active" box next to the option):

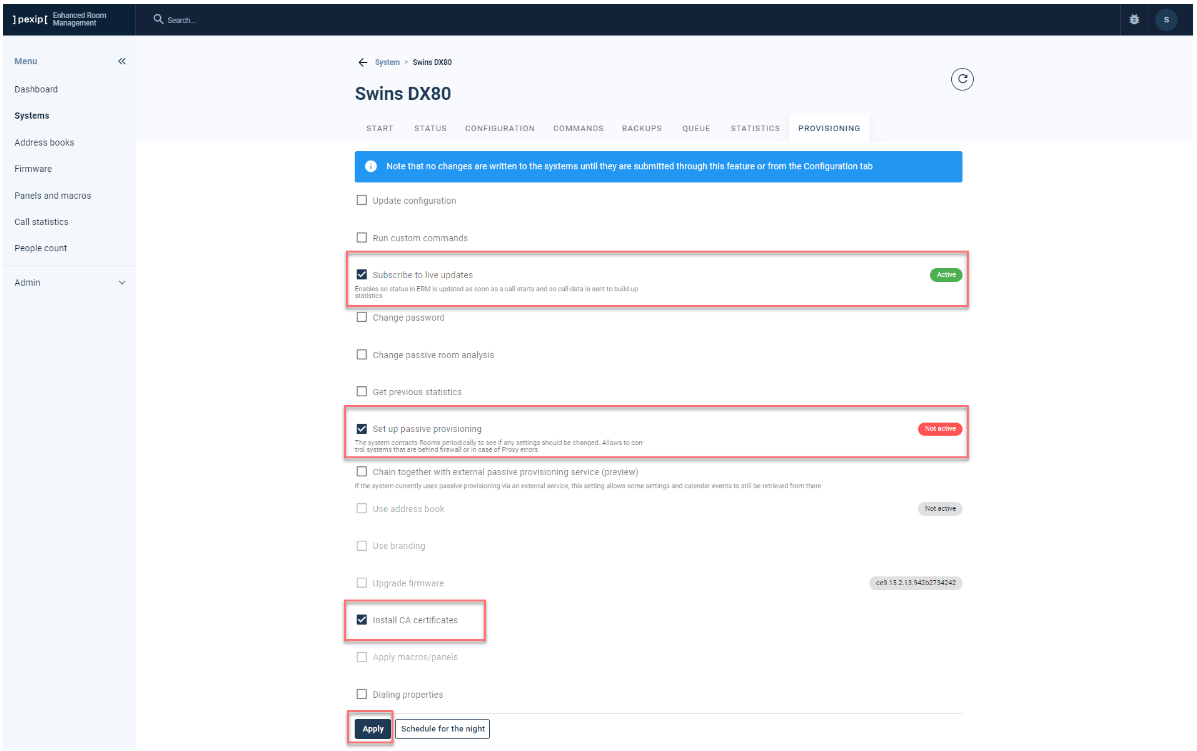
- Ensure that you select the **Subscribe to live updates** check box.

  This will raise a system warning in ERM if it is not enabled or configured correctly.
- Optionally, select the **Set up passive provisioning** check box (see more about passive provisioning below).

  Even with a direct connection, you can enable passive provisioning on an endpoint so it will create new requests to ERM to obtain provisioned information every few minutes (this can range between 45-420 seconds depending on activity within ERM). This configuration is generally used as a fallback mechanism in conjunction with the Proxy VM. If it is not enabled, a red "Not Active" message is displayed next to the setting within the provisioning tab. ERM will not raise a system warning as direct provisioning provides you with all the control needed. (Also, see Passive provisioning combined with a direct connection below).
- Ensure that you select the **Install CA certificates** check box.

  This option is unavailable if no certificates have been added via **Admin > Settings > Trusted CA Root Certificates**. If the CA root certificate is not installed on the Cisco endpoint, the endpoint will not form a trust relationship with the ERM service, and you will see errors on the endpoint and in the ERM dashboard.

Finally, click **Apply** to push these settings to the endpoint immediately.



Swins DX80

Note that no changes are written to the systems until they are submitted through this feature or from the Configuration tab

☐ Update configuration

☐ Run custom commands

☑ Subscribe to live updates — Active

Enables so status in ERM is updated as soon as a call starts and so call data is sent to build up statistics

☐ Change password

☐ Change passive room analysis

☐ Get previous statistics

☑ Set up passive provisioning — Not active

The system contacts Rooms periodically to see if any settings should be changed. Allows to control systems that are behind firewall or in case of Proxy errors

☐ Chain together with external passive provisioning service (preview)

If the system currently uses passive provisioning via an external service, this setting allows some settings and calendar events to still be retrieved from there

☐ Use address book — Not active

☐ Use branding

☐ Upgrade firmware — ce9.15.2.13.942b2734242

☑ Install CA certificates

☐ Apply macros/panels

☐ Dialing properties

Apply | Schedule for the night

Direct provisioning with a direct connection

As noted above, a direct connection means that ERM connects out to an endpoint. Direct provisioning implies that ERM will use this connection to push provisioning information, such as endpoint configuration items. For example, when you click the **Apply** button in the Provisioning tab for a system, or change an item in the Configuration tab and then **Review** and **Apply** that change, ERM immediately pushes those configuration changes via the direct connection.

Passive connection (and passive provisioning)

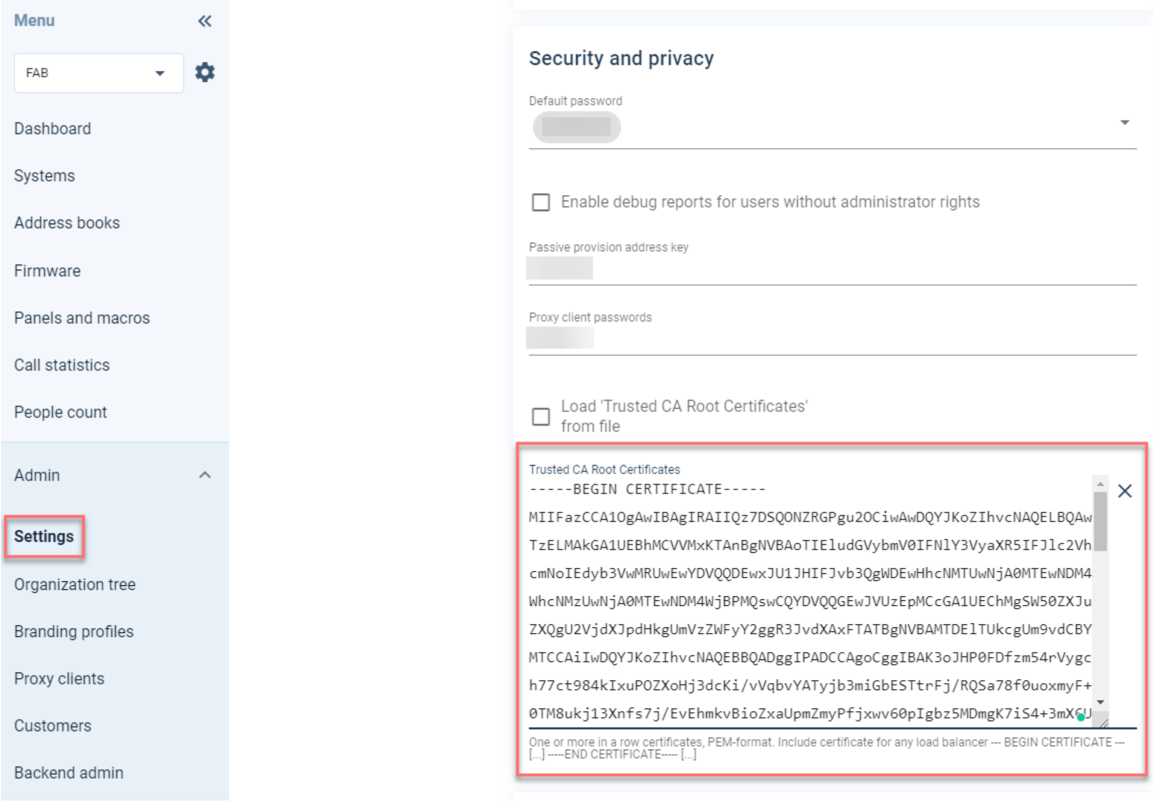
A passive connection enables a Cisco endpoint to create new outbound requests to the ERM video conference system request services to retrieve provisioning data every few minutes (between 45 and 420 seconds). This passive provisioning allows Cisco devices installed behind firewalls or NATed routers that would otherwise prevent ERM from connecting directly to the endpoint to obtain provisioning information.

Without any direct mechanism for ERM to push the necessary details to the endpoint, you need a way to inject that information onto a remote endpoint. This configuration is often applied via the endpoint’s API, either using its HTTP GUI or an SSH terminal session.

To add a passively provisioned device to ERM, you can either add a system placeholder or simply run the relevant CLI commands on the endpoint allowing a new system to be created automatically. Adding a system placeholder is beneficial when using chained provisioning.

The commands required to configure the endpoint are obtained via the **xConfiguration CLI** button in the ERM dashboard. The commands that are shown depend on whether you have added a Trusted CA Root Certificates in the ERM settings (as seen above). We recommend ensuring that the correct Trusted CA Root Certificates are added to this setting in ERM.

If you have included a certificate in the Trusted CA Root Certificate settings, then the `TlsVerify` option shows as `On` in the xConfiguration CLI commands list, and you see a notice indicating that `TlsVerify` *could* be set to `On` or `Off`. In addition, the trusted certificate(s) will appear within the xConfiguration CLI commands list.



Security and privacy

Default password

□ Enable debug reports for users without administrator rights

Passive provision address key

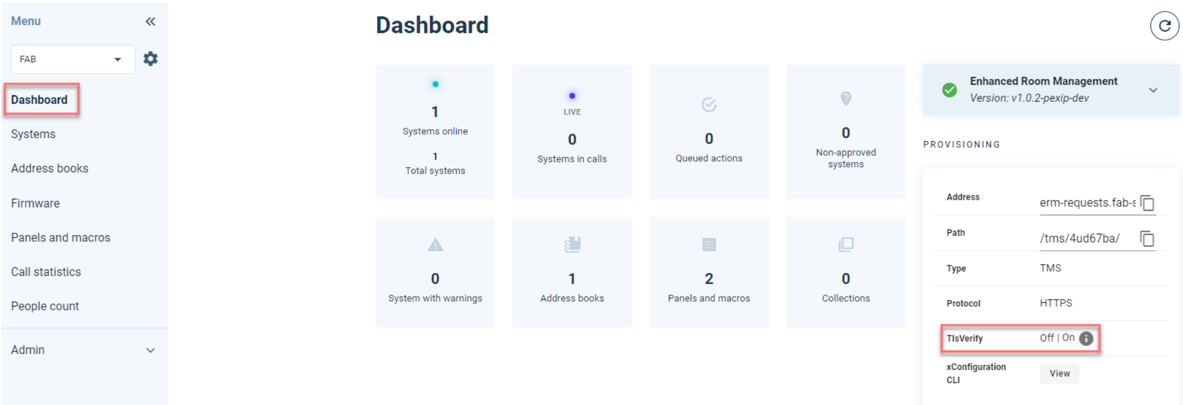
Proxy client passwords

□ Load 'Trusted CA Root Certificates' from file

Trusted CA Root Certificates

```
-----BEGIN CERTIFICATE-----
MIIFazCCA1OgAwIBAgIRAIIQz7DSQONZRGPgu2OCiwAwDQYJKoZIhvcNAQELBQAw
TzELMAkGA1UEBhMCVVMxKTAnBgNVBAoTIEludGVybmV0IFNlY3VyaXR5IFJlc2Vh
cmNoIEdyb3VwMRUwEwYDVQQDEwxJU1JHIFJvb3QgWDEwHhcNMTUwNjA0MTEwNDM4
WhcNMzUwNjA0MTEwNDM4WjBPMQswCQYDVQQGEwJVUzEpMCcGA1UEChMgSW50ZXJu
ZXQgU2VjdXJpdHkgUmVzZWFyY2ggR3JvdXAxFTATBgNVBAMTDElTUkcgUm9vdCBY
MTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAK3oJHP0FDfzm54rVygc
h77ct984kIxuPOZXoHj3dcKi/vVqbvYATyjb3miGbESTtrFj/RQSa78f0uoxmyF+
0TM8ukj13Xnfs7j/EvEhmkvBioZxaUpmZmyPfjxwv60pIgbz5MDmgK7iS4+3mX6U
```

One or more in a row certificates, PEM-format. Include certificate for any load balancer --- BEGIN CERTIFICATE --- [...] -----END CERTIFICATE----- [...]



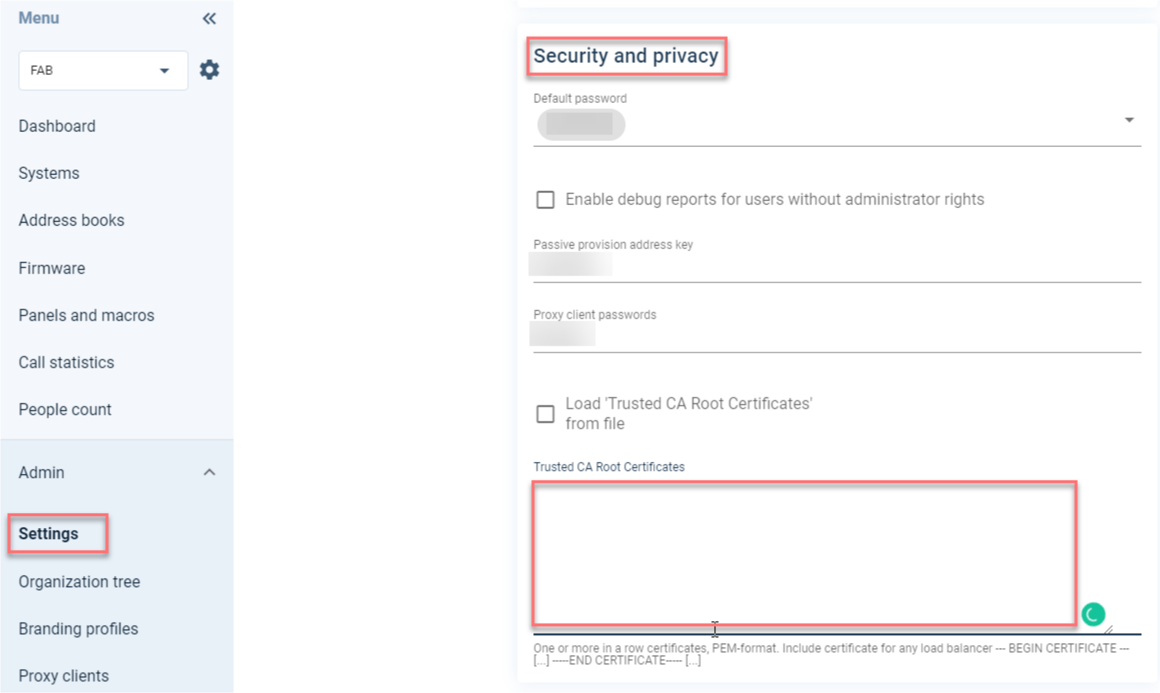
1	Systems online
1	Total systems
0	Systems in calls
0	Queued actions
0	Non-approved systems
0	System with warnings
1	Address books
2	Panels and macros
0	Collections

Enhanced Room Management
Version: v1.0.2-pexip-dev

PROVISIONING

Address	erm-requests.fab-s
Path	/tms/4ud67ba/
Type	TMS
Protocol	HTTPS
TlsVerify	Off | On
xConfiguration CLI	View

If you have not added a trusted CA root certificate into the ERM settings, then the `TlsVerify` option will not appear in the xConfiguration CLI command list, and you see a notice indicating that `TlsVerify` *could* be set to `Off`. The command is not part of the xConfiguration CLI command list as it is best to maintain the current state of the endpoint, but you would therefore need to manually upload any root CA certificates to the endpoint when this setting is still set to `On`.



Security and privacy

Default password: [redacted]

☐ Enable debug reports for users without administrator rights

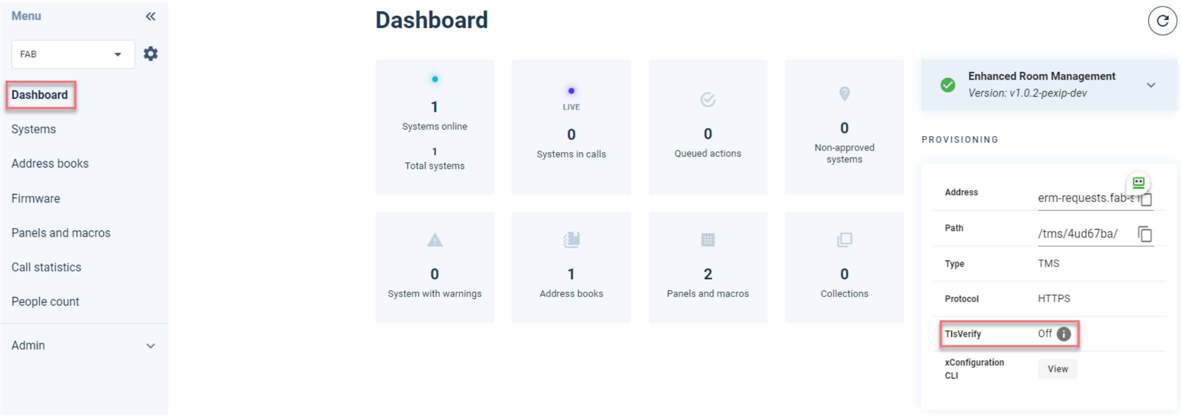
Passive provision address key: [redacted]

Proxy client passwords: [redacted]

☐ Load 'Trusted CA Root Certificates' from file

Trusted CA Root Certificates

One or more in a row certificates, PEM-format. Include certificate for any load balancer --- BEGIN CERTIFICATE --- [...] -----END CERTIFICATE----- [...]



1	Systems online
1	Total systems
0	Systems in calls
0	Queued actions
0	Non-approved systems
0	System with warnings
1	Address books
2	Panels and macros
0	Collections

Enhanced Room Management
Version: v1.0.2-pexip-dev

PROVISIONING

Address	erm-requests.fab-s
Path	/tms/4ud67ba/
Type	TMS
Protocol	HTTPS
TlsVerify	Off
xConfiguration CLI	View

You can also use passive provisioning with a direct connection. Note that there is only one set of configuration options on a Cisco endpoint for passive provisioning. Therefore, configuring ERM as the passive provisioning server will overwrite any currently configured passive provisioning setting. For example, your endpoint may be provisioned via CUCM, WebEx, TMS, or the Pexip Service. In the case of provisioning via the Pexip Service, you may want to look at chained provisioning.

TlsVerify option

It is important to understand what the TlsVerify option is and how it affects new outbound requests from a Cisco endpoint to various upstream services. By default, new or factory reset endpoints with a software version of CE9.9 or above, have this value set to ***On***. Endpoints that were upgraded from CE9.8 to CE9.9 (or above) will have this value set to ***Off***, provided that the device has not been factory reset after the upgrade, and that the old NetworkServices HTTPS VerifyServerCertificate setting was not explicitly set to ***On***. It is therefore difficult to say with certainty what the current value might be on any given Cisco endpoint within the estate.

We would generally recommend that this is set to ***On***, as outlined above. However, the endpoint's custom CA store needs to contain the relevant CA root certificates that are used to sign the certificate chains presented to the endpoint when it attempts a new request to the various services (such as provisioning, event updates and phonebook requests). Potentially, other infrastructure in the path (such as a load balancer or reverse proxy) may use certificate chains that are different to those used within ERM, so those roots should also be added to the Trusted CA Root Certificates setting. Thus, setting this to ***On*** when it was previously set to ***Off***, may result in the device losing communication with the provisioning service.

Differences in functionality when using a passive connection as opposed to a direct connection

The primary difference in the functionality of system manipulation when using a passive connection to ERM compared with a direct connection is a reduction in "white glove" operation. As a direct connection enables ERM to push commands in real-time towards a system, you could control an endpoint remotely on behalf of the local users. For example, calls can be placed or answered, the device could be muted/unmuted, and passcodes could be entered.

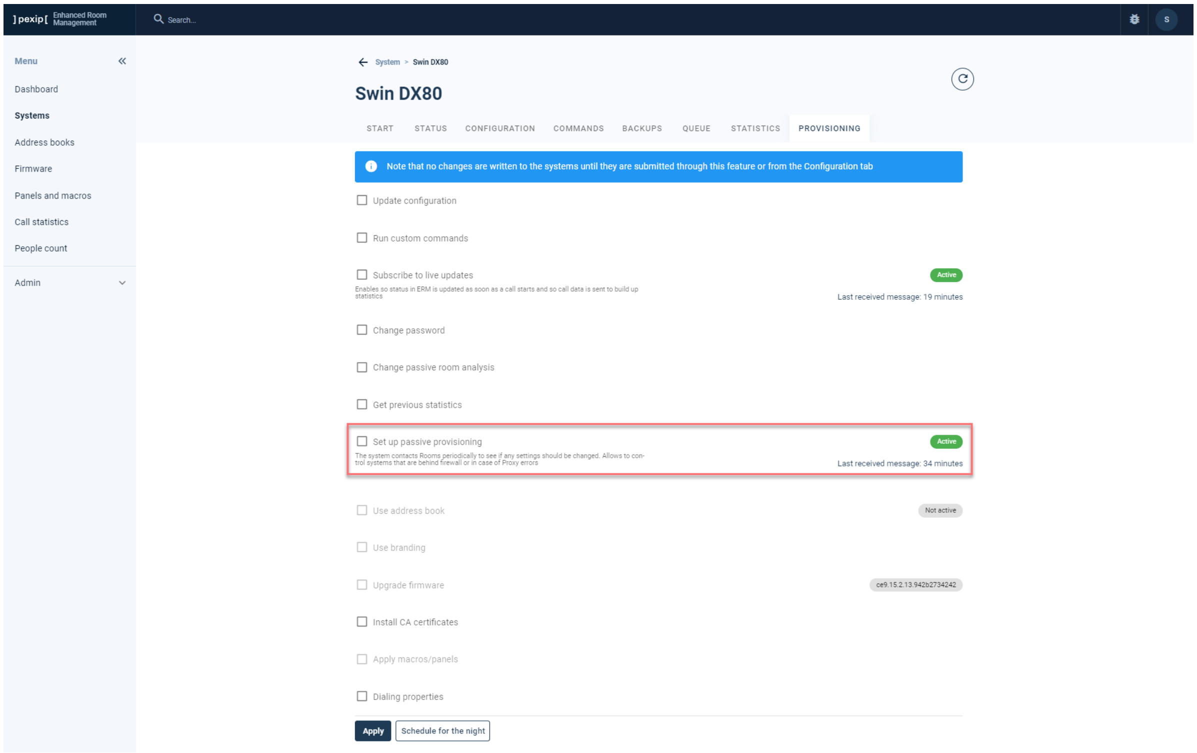
Technically, a passive connection could still allow for such system manipulation, but as the commands are simply queued within ERM and actioned only when the system calls home, they are therefore disabled within ERM. A system may take up to 420 seconds (7 minutes) to request an update from ERM, making such operations impracticable.

Passive provisioning combined with a direct connection

You can enable passive provisioning on the endpoint to provide a fallback provisioning mechanism for direct connections, although this is generally intended when the ERM Proxy VM is used. Passive provisioning configures the endpoint to call home to the ERM service every few minutes (which can vary between 45 and 420 seconds) to see if there are any configuration changes.

This configuration can be beneficial if, for example, the IP address of the Cisco endpoint changes, thus breaking the direct connection from ERM. Then, during the next passive provisioning update, as the Cisco endpoint connects to the ERM server, it can update its IP address details held by ERM, and ERM could re-establish a direct connection.

Alternatively, using passive provisioning with a direct connection could be undesirable. For example, if you have added a system into ERM that was provisioned to an external service (such as WebEx, CUCM or the Pexip Service). In that case, the original endpoint configuration will get overwritten. In this instance, chained provisioning may be appropriate.



Swin DX80

Note that no changes are written to the systems until they are submitted through this feature or from the Configuration tab

☐ Update configuration

☐ Run custom commands

☐ Subscribe to live updates — Active
Enables so status in ERM is updated as soon as a call starts and so call data is sent to build up statistics
Last received message: 19 minutes

☐ Change password

☐ Change passive room analysis

☐ Get previous statistics

☐ Set up passive provisioning — Active
The system contacts Rooms periodically to see if any settings should be changed. Allows to control systems that are behind firewall or in case of Proxy errors
Last received message: 34 minutes

☐ Use address book — Not active

☐ Use branding

☐ Upgrade firmware — ce9.15.2.13.942b2734242

☐ Install CA certificates

☐ Apply macros/panels

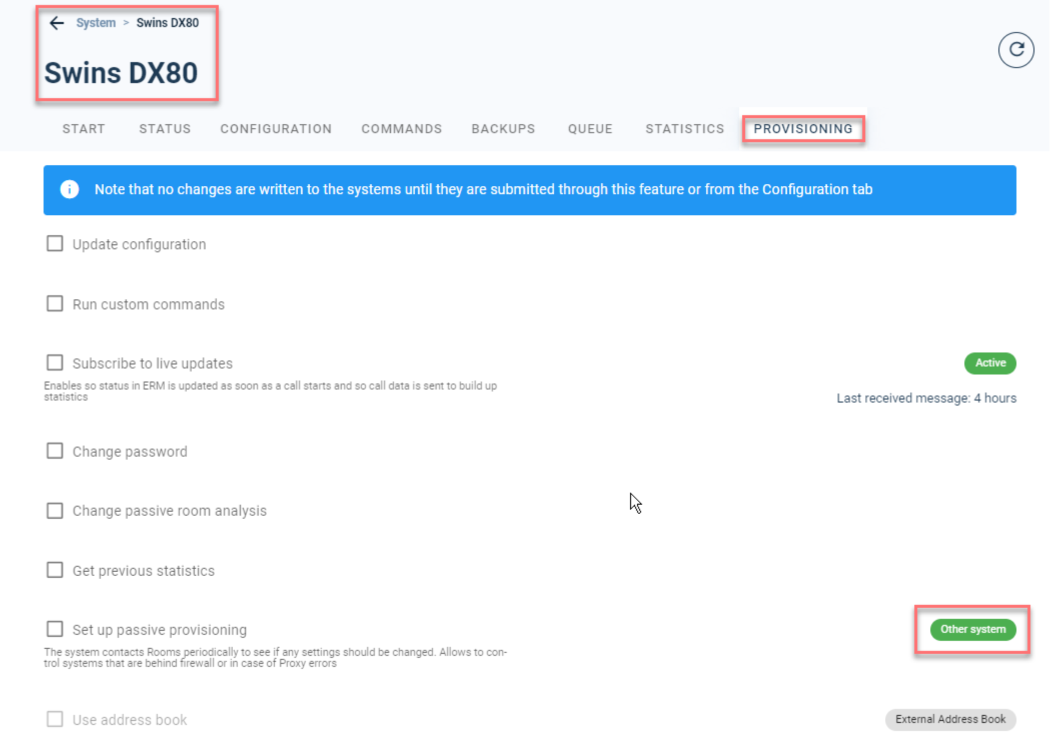
☐ Dialing properties

Chained provisioning (technical preview)

Chained provisioning allows a Cisco endpoint that already uses passive provisioning from the Pexip Service to be added to ERM as a managed device yet retain the provisioning information from the Pexip Service. You can configure chained provisioning for both directly connected and passively connected devices.

Chained provisioning for endpoints with a direct connection (or via the ERM Proxy) to ERM

When you add a Cisco endpoint as a directly connected device (or via the ERM Proxy) to ERM, you can also set the endpoint's passive provisioning configuration (as seen in Passive provisioning combined with a direct connection). However, you can configure only one set of passive provisioning options. By reviewing the **Passive provisioning** option in the **Provisioning** tab for a system, you can see if another third-party service is already being used to provision that system.



Swins DX80

Note that no changes are written to the systems until they are submitted through this feature or from the Configuration tab

□ Update configuration

□ Run custom commands

□ Subscribe to live updates
Enables so status in ERM is updated as soon as a call starts and so call data is sent to build up statistics
Active
Last received message: 4 hours

□ Change password

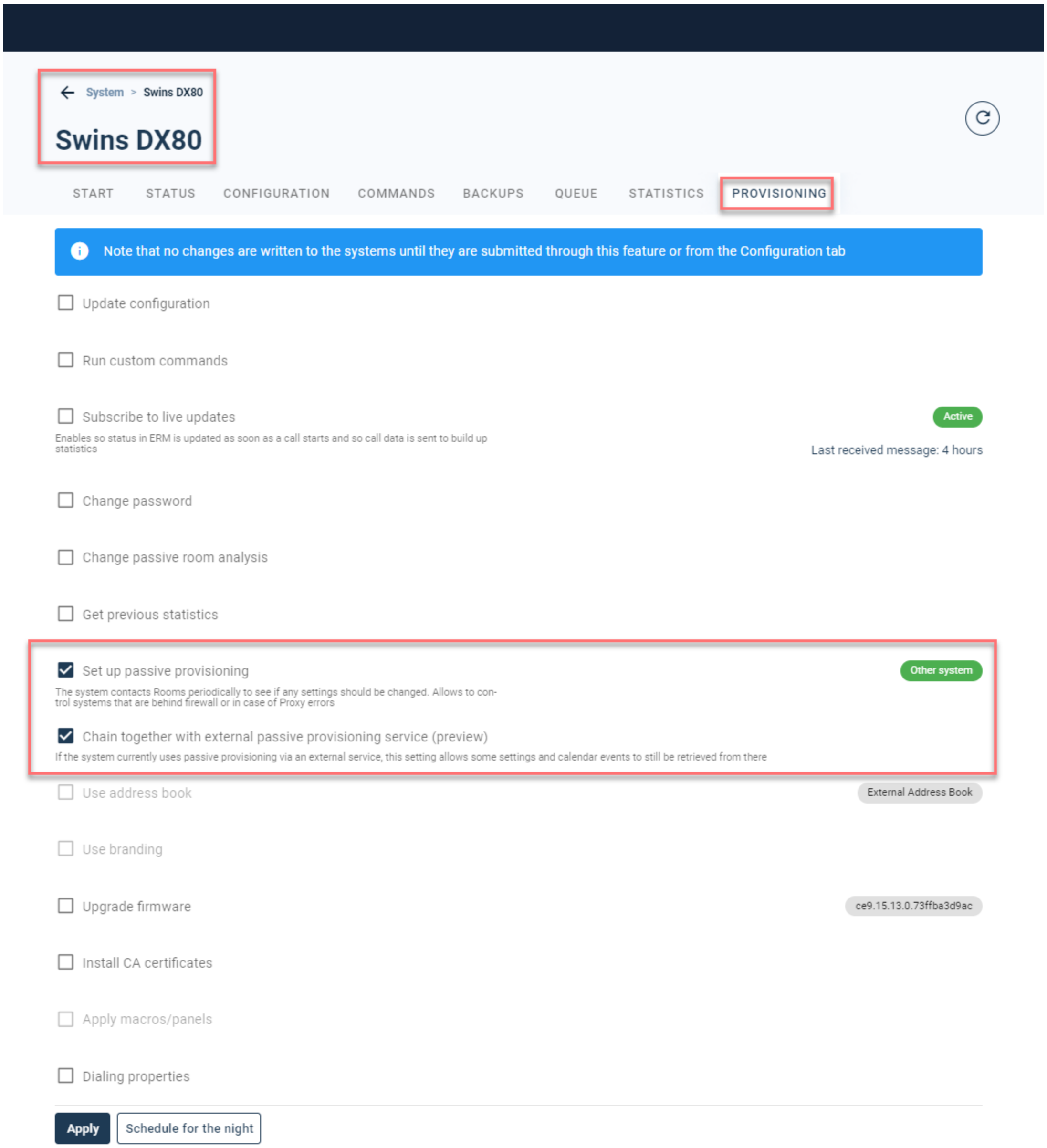
□ Change passive room analysis

□ Get previous statistics

□ Set up passive provisioning
The system contacts Rooms periodically to see if any settings should be changed. Allows to control systems that are behind firewall or in case of Proxy errors
Other system

□ Use address book
External Address Book

Setting passive provisioning to use ERM can override the original configuration. However, a second option to **Chain together with external passive provisioning service** appears when you select the **Set passive provisioning** option in the **Provisioning** tab for a system.



System > Swins DX80

Swins DX80

Note that no changes are written to the systems until they are submitted through this feature or from the Configuration tab

☐ Update configuration

☐ Run custom commands

☐ Subscribe to live updates — Active

Enables so status in ERM is updated as soon as a call starts and so call data is sent to build up statistics

Last received message: 4 hours

☐ Change password

☐ Change passive room analysis

☐ Get previous statistics

☑ Set up passive provisioning — Other system

The system contacts Rooms periodically to see if any settings should be changed. Allows to control systems that are behind firewall or in case of Proxy errors

☑ Chain together with external passive provisioning service (preview)

If the system currently uses passive provisioning via an external service, this setting allows some settings and calendar events to still be retrieved from there

☐ Use address book — External Address Book

☐ Use branding

☐ Upgrade firmware — ce9.15.13.0.73ffba3d9ac

☐ Install CA certificates

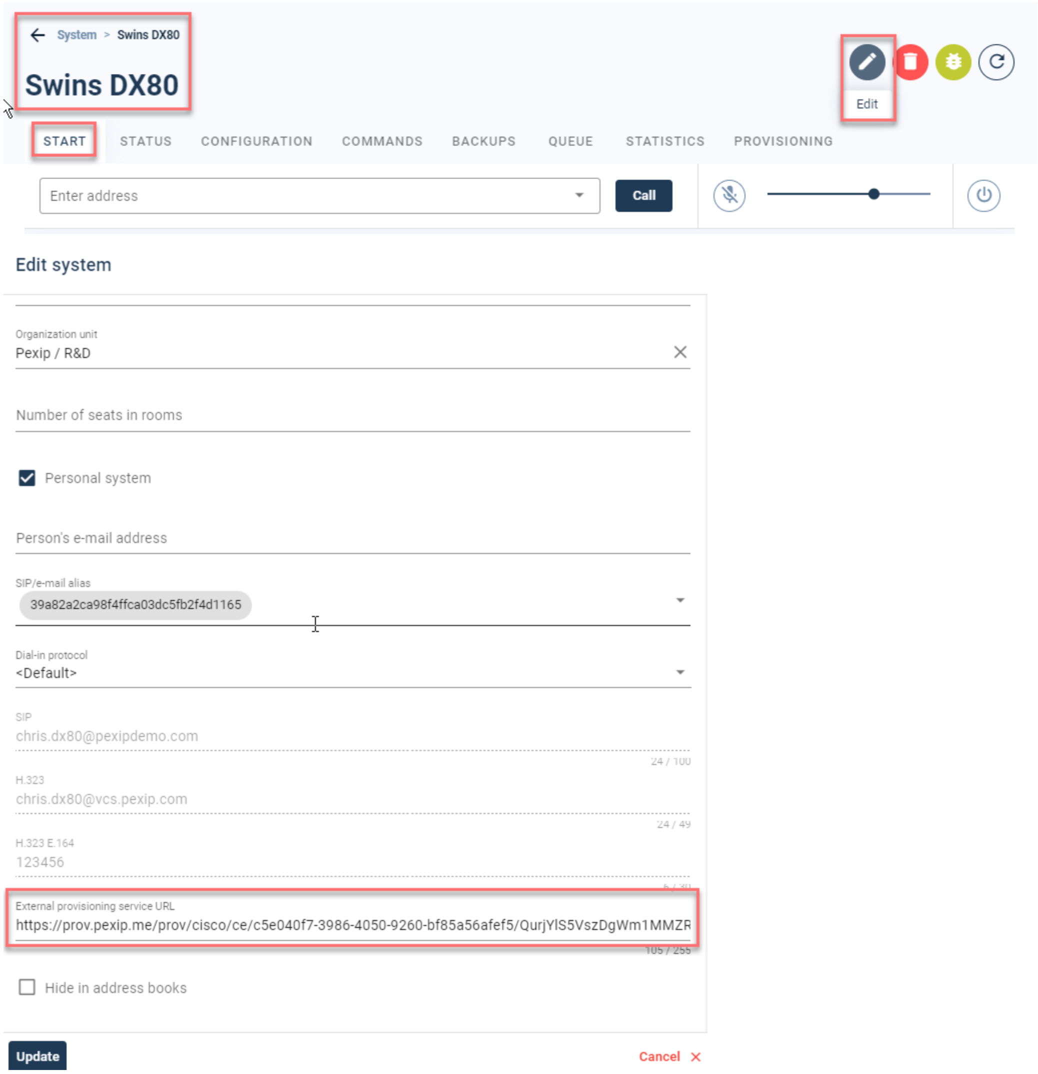
☐ Apply macros/panels

☐ Dialing properties

Chained provisioning operation process for a directly connected endpoint

When chained provisioning is applied, the following operations occur:

1. ERM queries the endpoint (using the direct connection) to obtain the currently configured passive provisioning settings and transfers these to the ERM system. You can see this information within the **System** settings in ERM (click on a System in the Dashboard, then in the **Start** tab, click the pencil to **Edit**); you see some basic settings, including the **External provisioning service URL**.



Edit system

Organization unit
Pexip / R&D

Number of seats in rooms

☑ Personal system

Person's e-mail address

SIP/e-mail alias
39a82a2ca98f4ffca03dc5fb2f4d1165

Dial-in protocol
<Default>

SIP
chris.dx80@pexipdemo.com
24 / 100

H.323
chris.dx80@vcs.pexip.com
24 / 49

H.323 E.164
123456
6 / 30

External provisioning service URL
https://prov.pexip.me/prov/cisco/ce/c5e040f7-3986-4050-9260-bf85a56afef5/QurjYlS5VszDgWm1MMZR
105 / 255

□ Hide in address books

Update
Cancel ✕

2. ERM then configures the passive provisioning on the Cisco endpoint to point to itself (i.e. the ERM system).
3. ERM queries the initially configured passive provisioning server, impersonating the Cisco endpoint, thus obtaining the provisioning data for the endpoint.
4. ERM relays this information to the Cisco endpoint when it next requests a provisioning update.

Chained provisioning for endpoints with a passive connection to ERM

Extra care, and some manual steps, need to be taken when configuring chained provisioning with those endpoints that can only have a passive connection to ERM. As seen in the passive connection section, setting up a passive connection from a Cisco endpoint requires you to run several xConfiguration API commands via the CLI. If the endpoint is already provisioned by a third-party service, such as the Pexip Service, running these API commands will **overwrite** the original provisioning information.

Note that:

- Chained provisioning in ERM is only designed to work with the Pexip Service. Therefore, it will **not** work when the system is provisioned via CUCM or WebEx.
- The Pexip Service is still the primary provisioning source for the endpoint (which may include phonebooks), not ERM. Changes to configuration items within ERM will be overwritten during the next provisioning request cycle. Should configuration updates be required, ensure they are completed on the Pexip Service.

Please contact your Pexip authorized support representative for more information if you want to set up chained provisioning.

Modifying a system's dialing properties

Changing a video conferencing system’s dialing properties in ERM can be done in three different ways: editing the system details directly, direct provisioning, or bulk provisioning.

Edit system details

You can edit the system details directly:

1. Go to **Systems** and select the system you want to change.
2. Click on the ✎ icon in the upper right of the page to access the edit dialog for the system.
3. Change the field values as required and click **Update** to save the new values (see Adding and approving new systems in ERM for details).
4. A dialog appears if you have changed values that requires provisioning and you can go from the dialog to the provisioning view for the system.
5. In the provisioning view, your changes should now automatically appear under “**Dialing properties**”.
6. Click **Apply** to provision the settings to the system (or choose **Schedule for the night** if required).

ℹ The changed dialing properties are updated on the system only after they have been provisioned.

Direct provisioning

You can provision the changes directly:

1. Go to **Systems** and select the system you want to change.
2. Select the **Provisioning** tab located under the heading of the page.
3. In the provisioning view you can then make your changes under **Dialing properties**.
4. Click **Apply** to provision the settings to the system (or choose **Schedule for the night** if required).

Bulk provisioning

If you want to change **only** the SIP proxy and H.323 gatekeeper settings for multiple systems, you can do this directly via the system list:

1. Go to **Systems**.
2. Select the checkbox for the system (or multiple systems) you want to change.
3. A dialog appears in the lower right corner where you can select **Provisioning** to open a provisioning dialog. In this case everything that you choose to provision will be sent to all selected systems.
4. In the provisioning view you can then make your changes under **Dialing properties**.
5. Click **Apply** to provision the settings to the system (or choose **Schedule for the night** if required).

Provisioning configurations to an ERM system

You can provision configurations for one or more video conferencing systems simultaneously.

To update the configurations, go to **Systems** and select the system for which you want to provision new configurations, then click on the **Configuration** tab which is located just below the page title.

Overview

You can update the system configurations in two ways, either by selecting the configurations you want to update directly from the configuration list using the checkboxes, or by clicking the **Load template** (⟳) button to load an already saved template with selected configurations and values.

After you have a selected number of configurations, they will appear at the top of the page in the **Selected configurations** drop-down. You can clear all your selections by clicking **Clear** (✕).

When you are ready, click **Review** (👁) to get an overview of the choices you have made.

Apply configurations

After you have reviewed the selected configurations, you can provision them easily by clicking on **Apply** (✓) at the top right of the page. This opens up a results dialog where you can follow the provisioning of your configurations as well as see the status and more information for each individual event.

Apply to multiple systems

To apply the configurations to several systems at the same time, do the same steps as above, with the only difference being in the review view where you click on **Select system** which shows a list of all your managed video conferencing systems.

The system you are currently viewing is pre-selected and you can select other systems before clicking on **Apply** (✓) to provision your configurations to all the selected systems at the same time.

Save template

When reviewing your selected configurations, you have the choice to save these as a template by clicking **Save template** (💾) which lets you reuse them at a later time.

Load template

If you already have a template saved with configurations that you want to load, click on **Load template** (💾) at the top to load the configurations.

Provisioning commands to an ERM system

To provision commands to a system, start by selecting the system for which you want to send commands, then click on the **Commands** tab which is located under the heading of the page.

ℹ Commands are not displayed for passive systems unless there is an earlier version of commands cached for the specific system. See Commands for passive systems for more information.

Overview

To run a command directly, you simply click the **Run** button for a specific command. This opens a result dialog where you can follow the provisioning process and get more information.

You can also choose to queue commands to either save them as a new template, or run all commands in the queue directly. You do this by using the **Queue** button for the different commands that you want to add to the queue.

The commands you have chosen to queue are displayed at the top of the page in the **Queued commands** drop-down. Here you also have the option to clear the queue by clicking on **Clear** (✕).

When you are ready, click **Review** (👁) to get an overview of the choices you have made.

Apply commands

After you have reviewed your queued commands, you can provision them easily by clicking on **Apply** (✓) at the top right of the page. This opens up a results dialog where you can follow the provisioning of your commands as well as see the status and more information for each individual event.

Apply to multiple systems

To apply the command queue to several systems at the same time, do the same steps as above, with the only difference being in the review view where you click on **Select system** which shows a list of all your managed video conferencing systems.

The system you are currently viewing is pre-selected and you can select other systems before clicking on **Apply** (✓) to provision your command queue to all the selected systems at the same time.

Save template

When reviewing your selected commands, you have the choice to save these as a template by clicking **Save template** (💾) which lets you reuse them at a later time.

Load template

If you already have a template saved with commands that you want to load, click on **Load template** (⇄) at the top to load the template to your active command queue.

Commands for passive systems

For systems that do not have an active connection, the list of commands for the system cannot be loaded automatically. In these cases, an error message for missing active connection appears under the **Commands** tab.

To proceed, start by downloading XML files for both commands and valuespace for the system, which you can then upload to access the commands that apply to the system.

ⓘ This support is not available for all types of systems.

Enhanced Room Management: address books

ERM address books

ERM provides powerful management of address books, which can be provisioned to one or more of your available video conferencing systems.

Each address book can have its own manual entries along with external sources. When you go to **Address books** you see an overview of all your existing address books.

In the top right of the page you can:

- + Create a new address book.
- ↻ Refresh the current page.

The table shows all your previously added address books. You can use the search function and filtering button ▼ located above the table to quickly find the address book you are looking for. The table consists of the following columns:

- **Name**: address book name
- **Type** : manual or external address book
- **Actions:**
  - ✎ Edit the address book.
  - ⧉ Duplicate the address book.
  - 🗑 Remove the address book.

Create a new address book

You can click on + to open a dialog to create a new address book. In the dialog, you start by typing a name for the address book.

You can also choose to tag the address book as an external address book which allows you to enter the url for search address (TMS SOAP), and also the url for external editing. When you are ready, click on **Save** to create your new address book.

After the address book has been created, you are automatically redirected to continue working with the contents (see ERM address book details).

ERM address book details

You can edit an address book by going to **Address books** and clicking on your desired address book.

Note that the first view is only for reviewing the contents of the address book, while editing is done via other views. You can search the list by typing in the search field in the top left of the table.

In the top right of the page you can:

- ⤓ Exports address book entries to Excel.
- *i* Show search information for the address book.
- 🗑 Removes address book from ERM.
- ↻ Refresh page.

Address book content

The columns of the address book entries consist of the following:

- **Title**: title of the address book entry.
- **Group**: the entry group.
- **External**: whether the post comes from an external source.
- **SIP**: the SIP address.
- **H.323** the H.323 address.

Grouping

You can use the grouping button ▦ to open the grouping dialog. The available options for grouping is based on the groups defined for the address book.

When you have selected either a single or multiple groups then click **Apply** in the dialog to update the list. Note that on larger screen resolutions the room system list is updated directly when changing your selection in the grouping form.

Navigation

You navigate the address book via the tabs located directly below the address book title:

- **Content**: this takes you back to the reviewing the address book content.
- **Edit**: this provides an overview of all your manual entries in the address book, and you have the opportunity to create, delete and edit entries. See Manual address book entries for more information.
- **Groups**: you can always create new groups for entries when you edit the address book, but this option provides a clear overview of all your groups. See Managing address book groups for more information.
- **Synchronized sources**: address books support different types of external sources that you manage through this view. See Synchronized sources for more information.

Manual address book entries

In addition to external sources, ERM address books have support for adding your own manual entries that are provisioned to selected room systems together with all other address book entries.

To manage manual entries, go to **Address books**, select the desired address book and select the **Edit** tab.

In the top right of the page you can:

- + Add single entry.
- Add multiple entries.
- ⤓ Export entries to Excel.
- ↻ Refresh page.

Similar to the list of entries on the start page of the address book, the contents of the address book are displayed in this list, however the difference is that only entries that have been manually added are displayed as well as editing options.

The columns of the address book entries consist of the following:

- **Title**: title of the address book entry.
- **Group** : the entry group.
- **External** : whether the post comes from an external source.
- **SIP**: the SIP address
- **H.323**: the H.323 address
- **Actions:**
  - ✎ Edit entry
  - 🗑 Delete entry

Grouping

You can use the grouping button ⊞ to open the grouping dialog. The available options for grouping is based on the groups defined for the address book.

When you have selected either a single or multiple groups then click **Apply** in the dialog to update the list. Note that on larger screen resolutions the room system list is updated directly when changing your selection in the grouping form.

Add single entry

To add a new entry, click + to open a dialog:

- **Title**: title of the address book entry.
- **Description**: a description for the entry.
- **Group**: the entry group.
- **SIP** : the SIP address
- **H.323**: the H.323 address
- **H.323 E.164 alias**: alias for H.323 E.164
- **Phone number**: the entry phone number

When you are ready, click **Add** to add the new entry to your address book.

Add multiple entries

To add multiple entries simultaneously, click on ◈ to open a dialog with the same fields as when adding a single entry. The difference is that the form is now table-based where it is easy to enter one entry per line.

Via the dialog you may also add multiple systems from an Excel file (.csv, .xls, .xlsx) and choose the appropriate columns as you import entries. Start by clicking **From Excel** located at the top followed by selecting the file that you want to import.

Managing address book groups

Address books can become difficult to navigate as the content grows larger, so ERM lets you divide your entries into groups for better structure.

To manage groups, go to **Address books** and select your desired address book and select the **Groups** tab.

In the top right of the page you can:

- + Add a new group.
- ↻ Refresh page.

The page provides a tree overview of all available groups that are grouped with parents and child groups. Use the search field at the top left to quickly find what you are looking for. There are also actions on the far right for each individual group:

- + Add child group
- ✎ Edit group
- 🗑 Delete group

If a group has child groups, a ▾ icon appears to the left to be able to toggle these.

Add a new group

There are two ways to add new groups to the group tree. Either click on + at the top of the page, or click on + from any existing group in the tree view to create a child group.

This opens a dialog where you fill in the name, and select the parent group (if any) of the new group and then click on **Save** to continue.

Synchronized sources

ERM address books have powerful support for adding synchronized sources to make your work easier.

To manage external sources, go to **Address books** and click on your desired address book and select the **Synchronized sources** tab.

In the top right of the page you can:

- + Add a new source.
- ↻ Refresh page.

The page lists all the existing sources that you have already added to the address book, which can deleted by clicking on 🗑 at the far right of the row.

Add a new source

To add a new source, clicking on + top open a dialog to add a new source:

- **Description**: a description of the source you are adding. This is used primarily to identify the source in the overview of all sources.
- **Add to sub group**: groups/folder structure and records are synchronized to this folder. Leave blank to sync to master level.

You must then select the type of synchronized source to add.

Managed video conferencing systems

Start by choosing whether it should only apply to systems under a specific organizational unit, and then make the choices below:

- **Merge subfolders**: select this to merge subfolders into one folder for the systems.
- **Also include hidden systems**: select this option to include all systems, even the systems that are tagged as hidden.

TMS

To add addresses from an existing TMS, enter the **URL for PhonebookSearch** and enter the **MAC address for identification** to proceed.

Copy of address book

To enable merging of different address books, there is support for adding content from an existing address book. Select an existing address book and the entries from the selected address book will be synchronized.

ERM firmware

To simplify working with firmware, ERM has a register where you can easily manage different firmware versions for all your video conferencing systems.

To manage firmware, start by going to **Firmware** which takes you to the overview of your previously added firmware.

ℹ You need to take the disk space of firmware files into consideration. Each firmware version may require 1-2 GB of additional storage space.

In the top right of the page you can:

- + Add new firmware.
- ↻ Refresh page.

The table shows previously added firmwares with the following columns:

- **Version**: the version you specified for the firmware.
- **File name**: the firmware file name.
- **Product**: the product the firmware applies to.
- **Uploaded**: date and time when the firmware was added.
- **Actions:**:
  - ⧉ Duplicate the firmware.
  - ⤓ Download the firmware.
  - 🗑 Delete the firmware.

You can use the filter button ▼ at the top right of the firmware list to display the filtering dialog where you can filter firmware by product type.

Add new firmware

Click on + to open a dialog where you specify the version of the firmware, which product that applies and the firmware file. When you are ready, click the **Upload** button to add your new firmware to ERM.

ℹ The product list is populated from the systems that you add to ERM. This means you need to add at least one system to ERM before you can upload any firmware files.

After your new firmware has been uploaded, you can then provision this to any number of video conferencing systems. See ERM provisioning overview for more information.

Panels, macros, room controls and collections

A powerful way to add value to your meeting room experience is by using room controls in ERM, which adds new features to the room's touch panel of Cisco/Webex room systems.

You can add all your room controls to ERM and then provision them to any selection of systems. You can also save a selection of room controls as a collection, which simplifies the workflow when, for example, a new room system is added.

Room controls

To manage room controls, go to **Panels and macros** to get an overview of all available room controls.

In the top right of the page you can:

- + Add a new room control.
- ↻ Refresh page.

The room control widget shows the title, description and how many files it consists of. It is also marked with **Panel** if the room control contains xml files and **Macro** if there are js files. The checkbox in the widget is used to perform bulk actions for most room controls at the same time. Each widget also has these actions located at the bottom:

- ✎ Edit the room control.
- ⤓ Download the room control.

Adding a new room control

To add a new entry, click + to open a dialog with a create form containing the following fields:

- **Title**: room control title.
- **Description**: description for the room control.
- **Files**: select multiple xml and js files for your room control, or select the **Zip** tab to import a zip file for the room control.

Editing room controls

When you click on ✎ for a specific room control widget, the editing dialog appears, which you navigate with the tabs located at the top of the dialog:

- **Content**: title and description of the room control.
- **Files**: shows the different files that the room control consists of.
- **Upload**: uploads new files for the room control.
- **System**: shows a list of video conferencing systems that currently have the collection installed, with an option to reinstall the collection, and to **Add** (install) it onto systems.
- **Remove**: removes the control.

Bulk actions

In the overview of room controls, each room control widget has a checkbox in the left corner, this enables you to select several room controls at the same time, which produces a dialog at the bottom left with bulk actions, such as to create a collection.

Download

The download option opens a dialog from where you can export the selected room controls.

Collections

You can group together a set of room controls as a collection, and view these in the **Collections** tab.

The collection widget shows the title, description and how many files and room controls the collection consists of. Each widget also has these actions located at the bottom:

- ✏ Edit the collection.
- ⤓ Download the collection.

Editing a collection

When you click on ✏ for a specific collection widget, the editing dialog appears, which you navigate with the tabs located at the top of the dialog:

- **Content**: title and description of the collection.
- **Controls**: shows the room controls that the collection consists of, and lets you add or remove room controls.
- **Systems**: shows a list of video conferencing systems that currently have the collection installed, with an option to reinstall the collection, and to **Add** (install) it onto systems.
- **Remove**: removes the collection.

Call statistics

ERM lets you generate reports for your video conferencing system's call statistics and usage.

To produce reports, go to **Call statistics** and then select a time period and filtering options to generate your statistics report.

Filtering

The first filtering option is to select a **From** and **To** date for the reporting period. More advanced filtering is available by using the filter button ▼ located at the top right, which opens the filtering dialog where the following options are available:

- **Select system**: only show statistics for a selection of systems.
- **Organization unit**: only show statistics for a certain organization unit.
- **Debug info**: include debug information in the report. Note that option for generating debug data is only available to users with staff permission, or if it is enabled for regular users from **Security and privacy** settings under **Admin > Settings**.

When you are ready, click **Apply** to generate a new report.

Statistics report

When you have selected your filtering options, a report with statistics for the selected time period appears. At the top of the report there are navigation tabs:

- **Overview**: this is an overview with a diagram of how many hours per day the systems have been in call. You can also export the report to Excel from this view.
- **Participants**: displays a list of all participants in the calls, as well as the number of hours and the number of calls for each individual participant.
- **Group**: a list of all calls grouped on which organizational unit they belong to, by number of hours and total number of calls for each individual group.
- **Debug – Calls**: shows all individual calls, which group, start time, stop time, how many participants and the length of each call.
- **Debug – Participants**: displays a list of all participants who participated in meetings, and which call, group, start time and end time each individual participant has had.

Export

You can export the report via the **Overview** tab where the export button is at the top right (X). If you have chosen to include debug information in the report, there is also a separate button for exporting the debug data.

People count

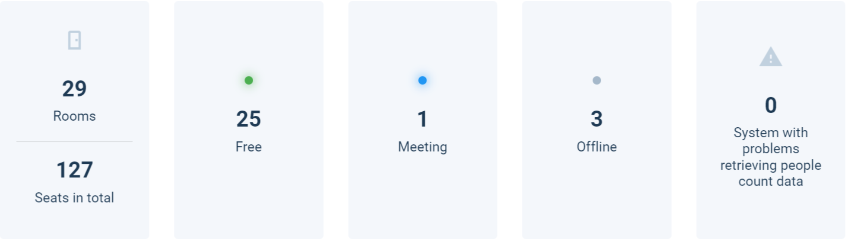
By using people count and call statistics from room systems, ERM lets you create powerful reporting from both online and offline meetings in conference rooms.

People count enables real time and historic monitoring of meeting room usage and scheduling efficiency as well as facility management for decision making. You access people count by going to **People count**.

To best utilize the people count feature, each system needs to have the **Number of seats in room** parameter configured (see Adding and approving new systems in ERM).

Live people count

At the top of the page, you get a quick compilation of all video conferencing systems that support people count and its current usage.



29
Rooms

127
Seats in total

25
Free

1
Meeting

3
Offline

0
System with problems retrieving people count data

The table further down includes status indicators and current people count for all systems:

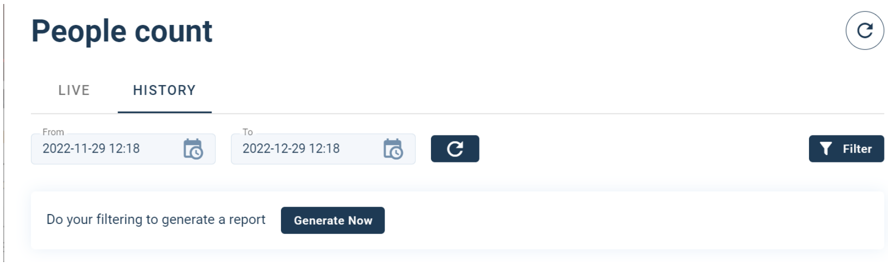
- **Name:** the name and model of the system.
- **People count**: the current people count and total seats for the system.
- **Status**:
  - ● **Free**: the system is online and is free.
  - ○ **Offline**: the system is offline.
  - 👥 **Meeting**: the system has a scheduled meeting with people present.

Filtering and grouping

Filtering and grouping work in the same way as for the list when video conferencing systems are managed via **Systems** (see Searching, filtering and grouping for more information).

People count history

You can create historic people count reports to see the utilization of your rooms.



From 2022-11-29 12:18

To 2022-12-29 12:18

Do your filtering to generate a report

You can set from and to dates and also add filters:

- **Select system**: select either all, subset or single system to generate a historic view of people count usage.
- **Organization unit**: select a specific organization unit.

- **Include times**: enter daily hours (24 hours per day) in comma-separated list, for example: **8,10,19**. It also supports ranges, for example: **8-17**.
- **Include days of the week**: enter day numbers (1=Monday, 7=Sunday) in a comma-separated list, for example: **1,4,5**. It also supports intervals, for example: **1-4**.
- **View as a percentage of room capacity**, **Skip empty rooms** and **Fill in missing data with 0 values:** select these options as appropriate.

Select **Apply** to apply the filters.

The report consists of graphs showing the number of people in the rooms:

- In the last hour
- By date
- Per hour
- Per day of the week

Enhanced Room Management: administration

Enhanced Room Management has admin settings and features for a number of different areas.

ERM administration settings

As an ERM administrator, you can configure various default settings for your system via **Admin > Settings**.

Setting	Description
Base settings	
Default address book	The default address book when e.g. a new system is added.
Default branding profile	The default branding profile when e.g. a new system is added.
HTTP feedback slot	Determines which HTTP feedback slot to use by default when subscribing to live updates is provisioned to the system.
First and last hour of night time	When provisioning is scheduled to run at night, it takes place within this time interval.
Security and privacy	
Default password	Add a list of passwords that ERM should try to use if a new system is added. Note, when a new password is provisioned to a system and the default password option is activated, the first password from this setting is used.
Enable debug reports for users without administrator rights	By default, only users with administrator permissions can generate debug data for statistics reports. This setting allows other users to use this as well.
Passive provision address key	Defines which address key to use for passive provisioning.
Public CA certificates	Support for adding one or more consecutive PEM formats.
Dial settings	
Dial-in protocol	Specifies the protocol to use for dial-in.
Default SIP proxy	Determines whether a default SIP proxy should be used when dialing properties are provisioned to systems.
Default SIP proxy user name	The SIP proxy user name.
Default SIP proxy password	The SIP proxy password.
Standard H323 gatekeeper	Determines if a H323 gatekeeper address should be pre-filled when dialing properties are provisioned to systems.
New systems	

Setting	Description
Automatically register new systems from these IP series	Enter the IP series for systems that you want to be automatically registered to ERM.
Automatically approve and try to create active connection	This option is only available if there is a default password specified in the **Security and privacy** settings. When a new system is registered, it automatically tries to create an active connection to the system. Note that the default password will be forwarded to the system.

Backend admin

Backend admin settings are only available to users with superuser permissions and they should only be changed on guidance from Pexip support.

ERM organization tree

A powerful way to get better structure over your video conferencing systems is to use ERM organization units.

By adding systems to organization units, you can better filter the systems and also get statistics based on the different units.

You can add new organization units when you edit a system or you can manage everything via **Admin > Organization tree**. In the top right of the page you can:

- + Add a new organization.
- ↻ Refresh page.

On the organization tree view page you get a clear overview of all available organization units that are grouped with parents and child groups. Use the search field at the top left to quickly find what you are looking for. There are also actions on the far right for each individual group:

- + Add child group
- ✎ Edit group
- 🗑 Delete group

If a group has child organization units an arrow ▾ icon appears to the left where you can toggle the child units.

Add a new organization

There are two ways to add new organizations to the group tree. Either click on the + icon at the top of the page, or click on + from any existing group to create a child organization.

This opens a dialog where you simply fill in the name, select the parent organization (if any) and click on **Save** to add your new organization unit.

ERM branding profiles

ERM has its own store of branding profiles where you can add, edit and delete different versions. You can then use provisioning to send the branding profiles to your desired number of systems.

You manage the different branding profiles via **Admin > Branding profiles**.

In the top right of the page you can:

- + Add branding profile.
- ↻ Refresh page.

On the page you get an overview of all previously added branding profiles with the following columns:

- **Name**: name of the branding profile.
- **Background active screen**: the brand image to display as a background on both the main screen and on the touch panel when the video system is in the awake state. The recommended image size is 3840×2160 pixels. Note, this will disable OBTP and meeting info.
- **Logo**: this dark brand logo is displayed on a light background in the bottom right corner on both the main screen and the touch panel. For best results, the logo should be a dark-colored version without padding, in png format with a transparent background. The recommended size is 272×272 pixels.
- **Background, non-active screen**: the brand image is displayed as a background on both the main screen and on the touch panel when the video system is in the halfwake state. The recommended image size is 3840×2160 pixels, in png or jpeg format.
- **Logo, non-active screen**: this light brand logo is displayed on a dark background in the bottom right corner on both the main screen and the touch panel. For best results, the logo should be an all white version without padding, in png format with a transparent background. The recommended size is 272×272 pixels.
- **Virtual background camera**: this image is displayed for the camera's virtual background. The recommended size is 1920×1080 pixels.
- **Actions:**
  - ✎ Edit the profile.
  - 🗑 Delete the profile.

Add branding profile

Clicking on + to open a dialog to add a new branding profile. In the dialog, start by typing a name followed by choosing which images to upload for the different modes available.

When you are ready, click **Add** to add the new profile. You can then provision the new branding profile to any desired number of systems (see ERM provisioning overview).

ERM proxy clients

The **Proxy clients** page (**Admin > Proxy clients**) lets you manage the ERM Proxys that are connected to your ERM server. It shows existing connected ERM Proxys and any new ERM Proxys that have successfully authenticated with the ERM server and are awaiting approval.

See ERM Proxy virtual machine for more details about the installation and operation of an ERM Proxy.

Viewing proxy clients

The main page provides an overview of accepted and new proxy clients:

- **Name**: the name of the proxy client. You can click here to edit the proxy.
  - 🆕 A new proxy client that needs to be approved before connecting to ERM.
  - 🔵 The proxy client is online.
  - 🔴 The proxy client is offline.
- **IP**: The IP number for the proxy client.
- **Last connection**: the time when ERM last had contact with the proxy.
- **Last checked**: the time when ERM last checked the proxy connection.
- **Actions**:
  - ✓ Approve the system to connect to ERM. Note that for multi tenants, the proxy client is added for the customer you are currently managing.
  - 🗑 Remove the proxy client from the current customer.

Editing a proxy client

Clicking on the proxy client’s name displays a dialog with the following options:

- **Name**: the proxy client name.
- **IP series**: automatically populate proxy settings for passive systems connecting from these IP series. To also enable active connections, you need to enable the relevant settings in the **Admin > Settings** page

Status changes

The sidebar shows the latest status change for all proxy clients. Each entry shows the time, name, IP number and which status was applied:

- 🟢 **Online**: the proxy went online.
- 🟡 **Connect**: the proxy connected.
- 🟠 **Connect**: the proxy connected but is not online.
- 🔴 **Offline**: the proxy went offline.