Pexip Infinity Secure Mode Deployment Guide

Introduction

This guide contains instructions for deploying and using Pexip Infinity in a secure mode of operation.

For further information about the deployment instructions and configuration settings described in this guide, please see the Pexip Infinity technical documentation website.

Securing the host environment

The VMware host environment must be hardened before deploying Pexip Infinity. It is expected that the host server contains at least two physical network interfaces and that management access to the ESXi host is restricted to a specific physical network and that virtual machines (VMs) are connected to a separate physical network.

Instructions for performing VMware-specific hardening are described in the *VMware vSphere ESXi 6.0 Security Technical Implementation Guide* which can be found at http://iasecontent.disa.mil/stigs/zip/U_VMware_vSphere_6-0_ESXi_V1R4_STIG.zip.

Management of the ESXi host can run out-of-band of the video conferencing network.

Reserving virtual machine resources

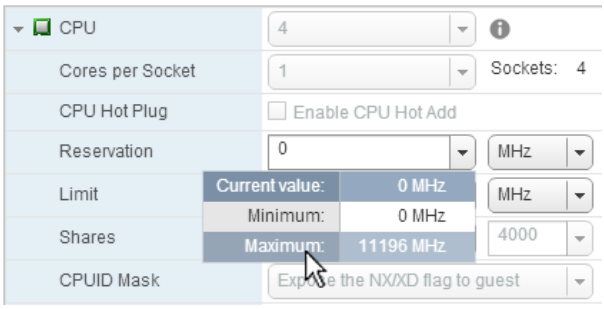
The resources allocated to each virtual machine must be reserved after it has been deployed. This ensures that each VM has guaranteed access to the resources that it expects and is thus isolated from any other VMs on the host.

To do this, find the VM in the vSphere client and edit its settings. There are separate settings for CPU, Memory, and Disk hardware.

CPU resource limits

There are three CPU resource settings: **Reservation**, **Limit**, and **Shares**. These specify the guaranteed CPU resource for the VM, the maximum CPU resource for the VM, and the weighting applied to the VM when sharing resources with its siblings.

These should be configured as follows:

Reservation	Select the menu entry labeled ***Maximum***.  (The value associated with ***Maximum*** will then appear in the **Reservation** field.)
Limit	Select the menu entry labeled ***Minimum***.
Shares	Select ***Normal***.

These settings ensure that the VM is guaranteed access to all of its allocated CPU resource, with no ability to burst above this resource allocation. Note that the MHz/GHz values for **Reservation** and **Limit** should thus be identical. As the resources are guaranteed, no sharing is necessary, so a setting of ***Normal*** is appropriate.

Memory resource limits

There are three memory resource settings: **Reservation**, **Limit**, and **Shares**. These specify the guaranteed memory resource for the VM, the maximum memory resource for the VM, and the weighting applied to the VM when sharing resources with its siblings. These should be configured as follows:

Reservation	Select the **Reserve all guest memory (All locked)** check box.
Limit	Select the menu entry labeled ***Minimum***.
Shares	Select ***Normal***.

These settings ensure that the VM is guaranteed access to all its allocated memory resource, with no ability to burst above this resource allocation. Note that the MB values for **Reservation** and **Limit** should thus be identical. As the resources are guaranteed, no sharing is necessary, so a setting of ***Normal*** is appropriate.

Disk resource limits

There are two disk resource settings: **Shares**, and **Limit - IOPs**. These specify the weighing applied to the VM when sharing resources with other VMs on the host, and the maximum number of IOPs the VM is permitted to consume. These should be configured as follows:

Shares	Select ***Normal***.
Limit - IOPs	Enter the appropriate number of IOPs for the Virtual Machine. The sum of all IOP limits for all VMs on the same host must not exceed the capacity of the datastore.

These settings ensure that the VM is limited to its fair share of IOPs. As the sum of all IOP limits on the same host do not exceed the host capabilities, sharing is not necessary, so a setting of ***Normal*** is appropriate.

BIOS configuration

The BIOS of each Virtual Machine must be configured and secured after deployment. This ensures that the system boots from the correct devices and that this configuration cannot be modified by unauthorized personnel.

To do this:

1. Use the vSphere client to edit the configuration of the VM to force it to boot into the BIOS as soon as it is powered on. This is usually found under **VM Options > Boot Options** as a configuration item named **Force BIOS setup**. This option should be selected to force entry to the BIOS on the next boot.
2. Power on the Virtual Machine and open its console, which should contain the BIOS setup utility.
3. Configure the boot order:
   a. Go to the **Boot** configuration page, and ensure that ***Hard Drive*** is the first entry.
   b. Expand the ***Hard Drive*** device tree and ensure that ***VMware Virtual SCSI Hard Drive (0:0)*** is the first entry.
4. Configure the BIOS security:
   a. Go to the **Security** configuration page.
   b. Configure a **Supervisor password** to prevent unauthorized modification of the BIOS configuration.
5. Save and exit.
   a. Go to the **Exit** configuration page.
   b. Select the **Exit Saving Changes** option.

Pexip Infinity Management Node deployment and bootstrap configuration

This section describes the steps needed to deploy the Pexip Infinity Management Node into the secure environment described above.

1. Use the vSphere client to deploy the Management Node OVA onto the selected ESXi host system.
   See *Installing the Management Node* for full instructions on how to do this.
   The VLAN ID used for the Management Node must not conflict with existing reserved VLAN IDs and must not use VLAN ID 4095 (which is reserved for virtual guest tagging), as the system will be locked down according to the *VMware ESXi Server Security Technical Implementation Guide*.
2. Log in to the Management Node console as the **admin** user. A password for this user must be set.
3. Enter the **admin** user password to permit the installation wizard to start.
4. Complete the installation wizard, ensuring that:
   - **Enable incident reporting** is set to ***no***.
   - **Send deployment and usage statistics to Pexip** is set to ***no***.

   On completion, the installation wizard will reboot the system.
5. Use a web browser to connect to the Pexip Infinity Administrator interface and ensure that you can log in using the credentials configured in the installation wizard.
6. Log in to the Management Node console as the admin user. Issue the following command:
   ```
   $ securitywizard
   ```
7. Enter the admin user password to permit the security wizard to start.
8. Complete the security wizard, providing answers as described below:

Setting	Value to enter
Enable FIPS 140-2 compliance mode (default = NO)	YES

Setting	Value to enter
Disable system administrator account (NO) (this applies to SSH and console access)	YES
Accept ICMPv6 redirects (NO)	NO
Drop incoming packets to closed ports rather than reject (YES)	YES
Accept multicast ICMPv6 echo requests (YES)	NO
Enable IPv6 Duplicate Address Detection (YES)	NO
SIP UDP listen port (5060) *	5060
SIP TCP listen port (5060) *	5060
SIP TLS listen port (5061) *	5061
Active management web sessions (0) *	100
Active per-user management web sessions (0) *	10
Enable management web validation of host headers (NO)	YES
Enable TLS 1.0 (YES)	NO
Enable Anonymous DH for outbound SIP/TLS (YES)	NO
Permit TLS <1.2 for inbound HTTPS (NO)	NO
Enable HTTP Content-Security-Policy for Conferencing Nodes (NO)	YES

* The SIP listen ports and web session limits may be customized for the target environment, as appropriate.

On completion, the security wizard will reboot the system. After the system has rebooted, no OS-level user access will be available on the system and it cannot be re-enabled. Note that only the Management Node is rebooted automatically. If the security wizard is run after any Conferencing Nodes have been deployed, those Conferencing Nodes must be manually rebooted.

Pexip Infinity Conferencing Node deployment

When deploying Conferencing Nodes, note that:

- Before deploying any Conferencing Nodes, you must complete the Management Node deployment and bootstrap configuration.
- As the host system will be locked down according to the *VMware ESXi Server Security Technical Implementation Guide:*
  - All Conferencing Nodes should be deployed manually (see *Manually deploying a Conferencing Node on an ESXi host*).
  - The VLAN ID used for the Conferencing Node must not conflict with existing reserved VLAN IDs and must not use VLAN ID 4095 (which is reserved for virtual guest tagging).

Pexip Infinity application configuration

This section describes the application-specific configuration required for Pexip Infinity to operate in a secure environment.

This configuration is performed using a web browser to access the Pexip Infinity Administrator interface. Log in to the Administrator interface using the credentials configured earlier in the installation wizard.

More information about all of these settings can be found on the Pexip Infinity technical documentation website.

TLS certificates

This section describes the process for bootstrapping the PKI environment.

Management Node and Conferencing Node server certificates

The Pexip Infinity platform ships with default self-signed server certificates for the Management Node and each Conferencing Node. Because these certificates are self-signed, they will not be trusted by clients. Therefore you must replace these certificates with your own certificates that have been signed by a trusted certificate authority. You should also configure a SIP TLS FQDN on each Conferencing Node that matches one of the entries in the TLS certificate.

Creating a certificate signing request (CSR)

You can use Pexip Infinity's inbuilt Certificate Signing Request (CSR) generator to assist in acquiring a server certificate from a Certificate Authority.

The resulting CSR file contents should be submitted to the CA for signing. After the CA has signed the CSR, the certificate will be ready for uploading.

In deployments that do not use DNS resolution, the Common Name should contain the IP address of the Conferencing Node instead of an FQDN — to achieve this you need to use third-party tools such as the OpenSSL toolkit (http://www.openssl.org), available for Windows, Mac and Linux.

Uploading a certificate to a Pexip node

To upload a new TLS server certificate for the Management Node or a Conferencing Node:

1. From the Pexip Infinity Administrator interface, go to **Platform Configuration > TLS Certificates**.
2. Select **Add TLS certificate**.
3. Complete the following fields:

TLS certificate	Paste the PEM-formatted certificate into the text area or alternatively select the file containing the new TLS certificate. You must upload the certificate file that you have obtained from the Certificate Authority (typically with a .CRT or .PEM extension). Do not upload your certificate signing request (.CSR file). The certificate must be valid for the hostname or FQDN of the Management Node or Conferencing Node to which it will be assigned. You can paste multiple certificates into the text area, but one of those certificates must pair with the associated private key.
Private key	Paste the PEM-formatted private key into the text area or alternatively select the file containing the private key that is associated with the new TLS certificate. Private key files typically have a .KEY or .PEM extension. Pexip Infinity supports RSA and ECDSA keys.
Private key passphrase	If the private key is encrypted, you must also supply the associated passphrase.
TLS parameters	Optionally, paste any additional PEM-formatted parameters into the text area or alternatively select the file containing the parameters that are to be associated with the new TLS certificate. Custom DH parameters and an EC curve name for ephemeral keys can be added. Such parameters can be generated through the OpenSSL toolkit using the commands `openssl dhparam` and `openssl ecparam`. For example, the command `openssl dhparam -2 -outform PEM 2048` generates 2048 bit DH parameters. Note that these parameters can alternatively be added 'as is' to the end of the TLS certificate.
Nodes	Select one or more nodes to which the new TLS certificate is to be applied. If required, you can upload a certificate and then apply it to a node later.

4. Select **Save**.

Trusted CA certificates

You must also upload the trusted Certificate Authority (CA) certificates for the secure environment. This must include any required chain of intermediate certificates for the CA that signed the server certificates. Note that the default set of trusted CA certificates

that ship with Pexip Infinity are not used when FIPS 140-2 compliance mode is enabled.

To manage the set of custom trusted CA certificates, go to **Platform Configuration > Trusted CA Certificates**. This shows a list and the current status of all the trusted CA certificates that have been uploaded. From here you can:

- **Upload a file of Trusted CA certificates**: select **Import files**, select **Choose Files** to pick one or more PEM files that you want to import, and then select **Import**.

  This adds the certificates in the selected files to the existing list of trusted CA certificates (or to the list of TLS certificates, depending on the certificate types contained in the file). If a certificate with the same subject name already exists (e.g. when replacing an expired certificate), the new certificate is uploaded alongside the original certificate (unless the issuer and serial number details are identical, in which case the existing certificate is updated with the new contents from the file).
- **View or modify an existing certificate**: select the **Subject name** of the certificate you want to view. The decoded certificate data is shown.

  If required, you can modify the PEM-formatted certificate data and select **Save**.
- **Download all certificates**: select **Export**. A **ca-certificates.pem** file containing all of the custom-added certificates in PEM format is created and automatically saved to your local file system.
- **Delete one or more certificates**: select the boxes next to the certificates to be deleted, and from the **Action** drop-down menu select ***Delete selected Trusted CA certificates*** and select **Go**.

IPv6 (optional)

If required, configure the **IPv6 address** and **IPv6 gateway addresses** of the Management Node and each Conferencing Node.

To configure these addresses:

- Go to **Platform Configuration > Management Node** and click on the name of the Management Node.
- Go to **Platform Configuration > Conferencing Nodes** and click on the name of the Conferencing Node.

Global settings

Go to **Platform Configuration > Global Settings** and review — and modify where required — the following settings:

Setting	Action
Enable SIP Enable H.323 Enable WebRTC Enable RTMP	Review the call protocols (SIP, H.323, WebRTC and RTMP) and disable those protocols you do not need to support.
Enable chat	Disable this option.
Enable outbound calls	Disable this option.
Enable support for Pexip Infinity Connect and Mobile App	Disable support for these applications.
DSCP value for management traffic	Set a DSCP value for management traffic sent from the Management Node and Conferencing Nodes. We recommend a value of 16.
Enable SSH	Disable this option.
Signaling port range start and end	Verify the range of ports (UDP and TCP) that all Conferencing Nodes are to use for signaling.
Media port range start and end	Verify the range of ports (UDP and TCP) that all Conferencing Nodes are to use for media.
OCSP state and OCSP responder URL	Set this to ***Override*** and specify the **OCSP responder URL** to which OCSP requests will be sent.

Setting	Action
SIP TLS certificate verification mode	Set this to ***On***.
Enable HTTP access for external systems	Ensure that this option is disabled.
Login banner text	Configure this field with some appropriate text for your deployment.
Management web interface session timeout	Set this to 10 minutes or other timeout value suitable for your deployment.

Configure administrator accounts and authentication settings

You must configure the Pexip Infinity platform to authenticate and authorize login accounts via a centrally-managed LDAP-accessible server.

Administrator roles

1. Go to **Users > Administrator Roles**.
2. Select the existing **Read-only** role and remove the following permissions:
   - ***May view logs***
   - ***May generate system snapshot***
3. Select the existing **Read-write** role and remove the following permissions:
   - ***May view logs***
   - ***May generate system snapshot***
4. Create an **Auditor** role:
   a. Select **Add role**.
   b. Specify a **Name** of "Auditor".
   c. Assign the following permissions to the role:
      - ***Is an administrator***
      - ***May use web interface***
      - ***May use API***
      - ***May view logs***
      - ***May generate system snapshot***
   d. Save the role.

LDAP server connection details

You must configure the details of the LDAP-accessible server and set the system to authenticate against the LDAP database and locally (for "last resort" contingency access):

1. Go to **Users > Administrator Authentication**.
2. Set the **Authentication source** to ***LDAP database and local database***.
3. In the **LDAP Configuration** section, specify the connection details for the LDAP-accessible server.
4. Save the settings.

LDAP group to role mapping

LDAP role mappings are used to map the LDAP groups associated with LDAP user records to the Pexip Infinity administrator roles. You must configure a separate LDAP role mapping for each LDAP group for which you want to map one or more Pexip Infinity administrator roles.

1. Go to **Users > LDAP Role Mappings**.
2. Select **Add LDAP role mapping**.
3. Configure the role mapping:

Option	Description
Name	Enter a descriptive name for the role mapping.
LDAP group DN	Select the LDAP group against which you want to map one or more administrator roles. The list of LDAP groups is only populated when there is an active connection to an LDAP server (**Users > Administrator Authentication**).
Roles	Select from the list of **Available roles** the administrator roles to associate with the LDAP group and then use the right arrow to move the selected roles into the **Chosen Roles** list.

4. Save the role.
5. Configure as many LDAP role mappings as required, ensuring that every administrator role is mapped to at least one LDAP group.

Enable certificate-based authentication

This configuration requires administrators to log in to the Pexip Infinity Administrator interface by presenting (via their browser) a client certificate containing their user identification details.

1. Install suitable client certificates into the certificate stores of the browsers to be used by the Pexip Infinity administrators. The identities contained in the certificates must exist in the LDAP database.
2. Go to **Users > Administrator Authentication**.
3. Set **Require client certificate** to one of the ***Required*** options as appropriate for your installation:
   Required (user identity in subject CN): administrators identify themselves via the identity contained in the subject CN (common name) of the client certificate presented by their browser.
   Required (user identity in subjectAltName userPrincipalName): administrators identify themselves via the identity contained in the **subjectAltName userPrincipalName** attribute of the client certificate presented by their browser.
4. Save the settings.
   When a client certificate is required, the standard login page is no longer presented. Administrators will not be able to access the Pexip Infinity Administrator interface or the management API if their browser does not present a valid certificate that contains a user identity which exists in the selected **Authentication source**.

Configure "last resort" contingency local account access

In case of prolonged lack of access to the LDAP-accessible server, a method of "last resort" access is required. This allows administrative access to the local Pexip Infinity administrator account via a securely-held certificate. To set this up:

1. Create a self-signed certificate for the local administrator account:
   a. Create a certificate generator script:

```
cat >mkcert <<ENDSCRIPT
#!/usr/bin/env bash

set -e

# Generate user certificate
USER=\$1

cat >cba.cnf <<EOF
[ usr_cert ]

basicConstraints=CA:TRUE
```

```
keyUsage=digitalSignature,keyEncipherment,keyCertSign
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer
subjectAltName=otherName:1.3.6.1.4.1.311.20.2.3;UTF8:\${USER}
EOF

openssl genrsa -out \${USER}.key 4096
openssl req -new -key \${USER}.key -subj "/O=Users/CN=\${USER}" -days 3650 -out
\${USER}.csr
openssl x509 -req -days 3650 -in \${USER}.csr -signkey \${USER}.key -extfile
cba.cnf -extensions usr_cert -set_serial 01 -out \${USER}.pem

# Convert user certificate to PKCS12 format for import into browser
openssl pkcs12 -export -out \${USER}.p12 -inkey \${USER}.key -in \${USER}.pem

rm cba.cnf
rm \${USER}.csr
rm \${USER}.key
ENDSCRIPT
```

b. Set its permissions:
   `chmod 755 mkcert`

c. Invoke it:
   `./mkcert <username>`

   Where **<username>** is the **Web administration username** that you set up in the Pexip Infinity installation wizard.

A pair of Export Password prompts will appear — blank entries are permitted (if no export password is desired). Site-specific policy should be followed, however.

The result will be two files in the current directory:

- **<username>.pem**: the user's public certificate.
- **<username>.p12**: the PKCS#12 bundle containing the user's certificate and private key.

The script generated above will issue a certificate valid for 10 years. It is a site-specific responsibility to ensure the continued validity of **<username>.p12** and to rerun this process before it expires.

2. It is a site-specific responsibility to ensure that **<username>.p12** (and any associated Export Password) is secured in a safe.
3. Configure Pexip Infinity to trust this certificate:
   a. Go to **Platform Configuration > Trusted CA Certificates**.
   b. Select **Import** and choose **<username>.pem** in the file browser.
   c. Select **Import** to upload the certificate.

Using the "last resort" local account access

If needed, due to prolonged lack of access to the LDAP-accessible server, you can access the Administrator interface via the local administrator account:

1. Remove **<username>.p12** from the safe, and add it to the appropriate browser's certificate store. For example:
   - In Firefox, browse to **about:preferences#advanced**, select **View Certificates**, select **Import**, and choose **<username>.p12**.
   - In Chrome, browse to **chrome://settings/certificates**, select **Import**, and choose **<username>.p12**.
   - In Internet Explorer, select **Tools > Internet Options**, select the **Content** tab, select **Certificates**, then select **Import** and follow the Certificate Import Wizard, choosing **<username>.p12** when asked.

   (Note that these browser-usage guidelines are subject to change, and depend on the current browser software version.)
2. You can now log in to the Administrator interface via the local administrator account.

Note that the "SSH password" is never used, as SSH access is disabled.

Securing network services

DNS servers

Configure at least two DNS servers (**System Configuration > DNS Servers**).

NTP servers

Configure at least two NTP servers (**System Configuration > NTP Servers**).

The configuration for each NTP server must include key authentication credentials.

Remote syslog servers

Configure at least one remote syslog server (**System Configuration > Syslog Servers**).

SNMP

Configure the Management Node and each Conferencing Node to use secure SNMPv3:

1. Go to **Platform Configuration > Management Node** and click on the name of the Management Node.
2. Set **SNMP mode** to ***SNMPv3 read-only***.
3. Configure the SNMPv3 credentials (**SNMPv3 username**, **privacy password** and **authentication password**) for this SNMP agent to match those used in requests from the SNMP management station.
4. Change the **SNMP community** to something other than "public".
5. Save the SNMP settings for the Management Node.
6. Apply the same configuration settings to each Conferencing Node (go to **Platform Configuration > Conferencing Nodes** and click on the name of each Conferencing Node in turn).

Secure ***SNMPv3 read-only*** mode uses SHA1 authentication and AES 128-bit encryption.

Location DSCP tags and MTU

Configure DSCP tags for signaling and media, and set the MTU size for each location:

1. Go to **Platform Configuration > Locations**.
2. Select the first location.
3. Configure the DSCP tags. We recommend:
   - **DSCP value for media** is set to 51.
   - **DSCP value for signaling** is set to 40.
4. Configure the **MTU**. We recommend a value of 1400 bytes to account for the overhead associated with the encryption headers.
5. Save the settings.
6. Repeat for every other location.

Contingency deployment

We recommend that you maintain a secondary deployment that you can switch to in the event that your primary deployment fails or is compromised.

- This fallback system should mimic the primary installation.
- It should be deployed without licensing.
- After the fallback system has been configured, all VMs should be completely powered off and remain off until required.

If the primary deployment is compromised and must be torn down, you should contact your Pexip authorized support representative to return the original license key and then re-activate the same license on the fallback system after it has been brought up.

Backing up configuration

We recommend that you take regular backups of your Pexip Infinity configuration so that up-to-date configuration can be restored to your contingency deployment or to a new deployment if needed.

There are two ways to maintain copies of your Management Node configuration data:

- Take a VMware snapshot of the Management Node VM.
- Use the backup and restore mechanism built into the Pexip Infinity Administrator interface.

In both cases you should follow site-specific guidelines for the backup policy and storage of backup files.

Certificate signing requests (CSRs)

To acquire a server certificate from a Certificate Authority (CA), a certificate signing request (CSR) has to be created and submitted to the CA. You can generate a CSR from within Pexip Infinity, and then upload the returned certificate associated with that request.

You can create a new CSR for any given subject name / node, or if you have an existing certificate already installed on a Pexip Infinity node that you need to replace (for example if it is due to expire) you can create a CSR based on the existing certificate data.

CSRs generated via Pexip Infinity always request client certificate and server certificate capabilities.

This topic covers:

Requesting a certificate signing request (CSR) for an existing certificate / subject name

You can generate a certificate signing request (CSR) for an existing certificate / subject name, for example if your current certificate is soon due to expire and you want to replace it. Before generating the CSR you can change the certificate data to be included in the new request, such as adding extra subject alternative names (SANs) to those already present in the existing certificate.

To generate a CSR for an existing certificate / subject name:

1. Go to **Platform Configuration > TLS Certificates**.
2. Select the subject name of the certificate for which you want to generate a CSR.
   The certificate data is shown.
3. Go to the bottom of the page and select **Create certificate signing request**.

You are taken to the Add Certificate signing request page, and the CSR data is defaulted to the contents of the certificate you selected.

4. If required you can change the certificate data, such as the subject alternative names (SANs) and subject fields.
   Note that you cannot change the private key — the CSR uses the same private key as the original certificate.
5. Select **Save**.
   The CSR is generated and you are taken to the **Change Certificate signing request** page.
6. Select **Download**.
   This downloads the CSR to your local file system, with a filename in the format **<subject-name>.csr**.
   Note that the private key is not downloaded, or included within the CSR.
7. You can now submit this CSR file to your chosen CA for signing.
   The CA will then send you a signed certificate which you can upload into Pexip Infinity (see Uploading the signed certificate associated with a certificate signing request).

Note that you cannot generate a CSR for an existing temporary / self-signed certificate.

If the CSR generation fails with a "It was not possible to automatically create a certificate signing request from this certificate" message, then there was a problem with validating the original certificate data, most likely an invalid subject name or an invalid country code. In this case you will have to create the CSR manually.

Creating a new certificate signing request

To generate a CSR within Pexip Infinity:

1. Go to **Utilities > Certificate Signing Requests**.
2. Select **Add Certificate signing request**.
3. Complete the following fields:

TLS Certificate	***Create non-renewal CSR*** is selected by default. This lets you create a new CSR. To create a renewal CSR based on an existing certificate, choose a different subject name / issuer from the list (in which case the subject name and private key fields below are not displayed).
Subject name	Select the name to be specified as the Common Name field of the requested certificate's subject. This is typically set to the FQDN of the node on which the certificate is to be installed. The available options are prepopulated with the FQDNs (hostname plus domain) of the Management Node and each currently deployed Conferencing Node. The list also includes any **SIP TLS FQDN** names of your Conferencing Nodes, if such names have been configured and are different from the node's FQDN. If you want to specify a custom Common Name instead, select ***User-provided custom Common Name***.
Custom subject name	Enter the name that you want to use as the Common Name field of the requested certificate's subject, if you have selected ***User-provided custom Common Name*** above.
Private key type	Select the type of private key to generate, or select ***Upload user-provided private key*** if you want to provide your own private key. Default: RSA (2048bit)
Private key	Only applies if you have selected ***Upload user-provided private key*** above. Enter the PEM formatted RSA or ECC private key to use when generating your CSR. You can either paste the key into the input field or upload the private key file from your local file system.
Private key passphrase	Only applies if you have selected ***Upload user-provided private key*** above. If the private key is encrypted, you must also supply the associated passphrase.

Subject alternative names	Select the subject alternative names (SANs) to be included in the CSR. This allows the certificate to be used to secure a server with multiple names (such as a different DNS name), or to secure multiple servers using the same certificate. You can choose from the same list of names presented in the **Subject name** field. Note that the name you choose as the Common Name is automatically included in the generated CSR's list of SANs (even if you remove it from the **Subject alternative names** list shown here). In some deployments it may be more practical to generate single CSR in which all of your Conferencing Node FQDNs are included in the list of SANs. This means that the same single server certificate returned by the CA can then be assigned to every Conferencing Node. When integrating with Microsoft Skype for Business / Lync, SAN entries must be included for every individual Conferencing Node in the public DMZ (public DMZ deployments) or in the trusted application pool (on-prem deployments).
Additional subject alternative names	Optionally, enter a comma-separated list of additional subject alternative names to include in the CSR. For example, when integrating with on-prem Skype for Business / Lync deployments you would typically need to add the trusted application pool FQDN.
Additional subject fields (if required you can enter the following additional CSR attributes; these are all blank by default)	
Organization name	The name of your organization.
Department	The department within your organization.
City	The city where your organization is located.
State or Province	The state or province where your organization is located.
Country	The 2 letter code of the country where your organization is located.
Advanced (in most scenarios you should leave the advanced options to their default settings)	
Include Microsoft certificate template extension	Select this option to specify a (Microsoft-specific) certificate template in the CSR. This is needed when using the Certification Authority MMC snap-in to request a certificate from an enterprise CA. Selecting this option causes the 'WebServer' certificate template to be specified. Default: disabled.
Include Common Name in Subject Alternative Names	Specifies whether to include the requested subject Common Name in the Subject Alternative Name field of the CSR. Default: enabled.

4. Select **Save**.
   You are taken to the **Change Certificate signing request** page.
5. Select **Download**.
   This downloads the CSR to your local file system, with a filename in the format **<subject-name>.csr**.
   Note that the private key is not downloaded, or included within the CSR.
6. You can now submit this CSR file to your chosen CA for signing.
   The CA will then send you a signed certificate which you can upload into Pexip Infinity (see below).

Uploading the signed certificate associated with a certificate signing request

When the Certificate Authority sends you a signed certificate in response to your CSR, you can upload that certificate into Pexip Infinity and assign it to one or more of your nodes. Make sure that you upload it via the **Certificate Signing Requests** page as this ensures that it is linked with the private key associated with your original CSR.

To upload the signed certificate:

1. Go to **Utilities > Certificate Signing Requests**.
2. Select the original CSR that is associated with the signed certificate.
   You are taken to the **Change Certificate signing request** page.
3. In the **Certificate** field either paste the PEM-formatted certificate into the input field or upload the certificate file from your local file system.
   The certificate file that you have obtained from the Certificate Authority typically has a .CRT or .PEM extension. Do not upload your certificate signing request (.CSR file).
4. Select **Complete**.
   Providing it is a valid certificate and is based on the original CSR:
   - the certificate is uploaded and automatically linked with the private key associated with your original CSR.
   - if you are uploading a replacement certificate (same subject name and private key) it will replace the existing certificate and maintain any existing node assignments.
   - the original CSR is deleted.
   - you are taken to the **Change TLS Certificate** page.
5. You can now assign that certificate to the Management Node or one of more Conferencing Nodes as required:
   a. From within the **Change TLS Certificate** page go to the **Nodes** field and from the **Available Nodes** list, select the nodes to which you want to assign the certificate and move them into the **Chosen Nodes** list.
   b. Go to the bottom of the page and select **Save**.

Troubleshooting

This section describes some of the error messages you may see when attempting to upload a signed certificate.

Error message	Possible cause	Resolution
Certificate and private key do not appear to be part of the same key pair	This most likely means that you have tried to upload the certificate against the wrong CSR.	Select the correct CSR and try again.

Modifying a CSR

After a CSR has been created it cannot be modified — the only available actions are to download it (for sending to a CA), or to apply the returned, signed certificate that is associated with that request.

If you need to change the content of a CSR, you should delete the original CSR and create a new CSR with the correct content.

Note that a CSR is automatically deleted when the resulting signed certificate is uploaded.