



Pexip Infinity

VMware Installation Guide

Software Version 33

Document Version 33.a

October 2023

]pexip[


Contents

Introduction	4
Configuring VMware for Pexip Infinity	5
Supported ESXi versions	5
Supported VMware editions	5
Prerequisites	5
Synchronizing time	5
Using a static MAC address for the Management Node	6
Reducing MTU with ESXi 6.7u2 and above	6
Advanced VMware ESXi administration	7
Host server requirements	7
General recommendations	7
Impact on virtual environment	7
CPU	7
Memory	7
Storage	7
Network	8
Traffic shaping	8
NIC teaming	8
Upgrading VM hardware versions	8
vMotion	8
Enhanced vMotion Compatibility (EVC)	9
Installing the Management Node	10
Deploying the Management Node template	10
Enabling automatic startup	12
Running the installation wizard	12
Opening a console window	12
Running the installation wizard	12
Initial platform configuration	14
Accessing the Pexip Infinity Administrator interface	14
Configuring the Pexip Infinity platform	14
Deploying a Conferencing Node on an ESXi host	16
Generating, downloading and deploying the ova file	16
Enabling automatic startup	18
Disabling EVC	18
Testing and next steps after initial installation	19
Making a test call	19

Further configuration	19
Integrating with a call control system	20
Configuring the Pexip Infinity Distributed Gateway	20
Registering devices directly to the Pexip Infinity platform	20
Customizing the user experience	20
Informing users about the new video conferencing service	20
Pexip Infinity installation checklist	21
Prior to installation	21
Hypervisor / host servers	21
Pexip Infinity Administrator interface	21
Hypervisor maintenance	21
Pexip Infinity configuration datasheet	22

Introduction

This installation guide describes the minimum steps required to deploy and test a simple Pexip Infinity platform in a VMware environment.

-  Full information on configuring and using Pexip Infinity is available:
 - on the [Pexip Infinity technical documentation website](#) (from where all documentation can also be downloaded in PDF format)
 - as online help, by clicking the **Help** link in the top right corner of the Pexip Infinity Administrator interface (available after the Management Node has been deployed).

-  You must ensure you have completed all necessary platform-based [Planning and prerequisites](#) prior to installation.

Please visit the [Pexip Academy](#) for access to a range of training resources and videos, including VMware installations.

Configuring VMware for Pexip Infinity

This section describes the basic VMware configuration required before you [install the Management Node](#) or [install a Conferencing Node](#). For more advanced deployments, see also [Advanced VMware ESXi administration](#).

Supported ESXi versions

Version 33 of the Pexip Infinity platform supports VMware vSphere ESXi 6.5, 6.7, 7.0 and 8.0.

Standalone ESXi hosts are not supported.

Supported VMware editions

The Pexip Infinity platform will run on the **free edition** of vSphere Hypervisor. However, this edition has a number of limitations (limited support from VMware, no access to vCenter or vMotion). For this reason we do not recommend its use except in smaller deployments, or test or demo environments.


The minimum edition of VMware that we recommend is the vSphere **Standard edition**. This does not have the limitations of the free edition. If you do not already use VMware in your enterprise, the vSphere **Essentials Kit** is a simple way to get started and will provide you with Standard edition licenses for 3 servers (with 2 CPUs each) plus a vCenter license.

The **Enterprise Plus edition** includes further additional features relevant to the Pexip Infinity platform that could be of benefit to larger deployments. These include Storage DRS and Distributed Switch.

For a comparison of the VMware editions, see <http://www.vmware.com/products/vsphere.html#compare>.



Prerequisites

You must have a suitable VMware environment already installed.

-  If an ESXi host is being managed by vCenter Server, all administration must be performed via vCenter Server. Do not log in directly to the ESXi host; configuration changes made in this way may be lost. To ensure that ESXi hosts being managed by vCenter Server are accessible via vCenter Server only and are not directly accessible, you should put them in Lockdown mode. Lockdown mode forces all operations to be performed through vCenter Server.

Synchronizing time

Pexip Infinity uses NTP servers to obtain accurate system time. This is necessary to ensure correct operation, including configuration replication and log timestamps.

-  All host servers **must** be synchronized with accurate time before you install the Management Node or Conferencing Nodes on them.
-  NTP **must** be enabled on the Management Node VM before you deploy any Conferencing Nodes (this is done during installation of the Management Node).

We strongly recommend that you configure at least three distinct NTP servers or NTP server pools on all your host servers and the Management Node itself. This ensures that log entries from all nodes are properly synchronized.

The VMs hosting the Management Node and Conferencing Nodes use the UTC timezone, and all logs are in UTC. Do not attempt to change the timezone on these systems. Note however that the administrator web interface uses your local time.

To synchronize time on the host server using the vSphere web client (HTML 5):

1. Log in to the VM manager (vCenter Server).
2. From the vSphere client's navigation panel, select the host server on which the software image is to be installed.
3. From the main panel, select the **Configure** tab.
4. From the left-hand panel, select **System > Time Configuration**.
5. From the top right of the page, select **Edit**. The **Edit Time Configuration** dialog box appears.
6. Select **Use Network Time Protocol (Enable NTP client)**.
7. In the **NTP Servers** field, we strongly recommend that you enter at least 3 distinct NTP servers or NTP server pools to ensure that log entries from all nodes are properly synchronized.
8. From the **NTP Service Startup Policy** drop-down menu, select **Start and stop with host**.
9. Select **OK**.

To verify that NTP has been enabled correctly:

1. Select the **Configure** tab and then **System > Time Configuration**.
2. From the **Time Configuration** page, ensure that value in the **Date & Time** field is correct.

Using a static MAC address for the Management Node

We recommend using a static MAC address for the virtual machine hosting your Management Node. This will ensure that the licenses on your Management Node do not become invalid if, for example, the node reboots and comes up on a different physical blade.

Reducing MTU with ESXi 6.7u2 and above

If you are using ESXi 6.7u2 and above, and are operating Pexip nodes at an MTU below that of the local network, you need to disable ESXi's receive MTU check. To do this, run the following `esxcli` command:

```
esxcli system settings advanced set -o "/Net/Vmxnet3NonTsoPacketGtMtuAllowed" -i 1
```

For more information, please see: <https://kb.vmware.com/s/article/75213>.

Advanced VMware ESXi administration

Simple deployments of the Pexip Infinity platform should not require any special VMware knowledge or configuration beyond that described in [Configuring VMware for Pexip Infinity](#).

This section describes some important requirements for advanced VMware ESXi administration when used with Pexip Infinity. It assumes that you are already familiar with VMware. For more information on VMware ESXi in general, see <http://www.vmware.com/products/esxi-and-esx.html>.

- i** If an ESXi host is being managed by vCenter Server, all administration must be performed via vCenter Server. Do not log in directly to the ESXi host; configuration changes made in this way may be lost. To ensure that ESXi hosts being managed by vCenter Server are accessible via vCenter Server only and are not directly accessible, you should put them in Lockdown mode. Lockdown mode forces all operations to be performed through vCenter Server.

Host server requirements

The recommended hardware requirements for the Management Node and Conferencing Node host servers are described in [Server design recommendations](#). In addition to this:

- **GPU:** host servers do not require any specific hardware cards or GPUs.
- **Disk:** either direct attached storage or shared storage can be used. The primary disk activity will be logging.
- **Multitenancy:** this version of Pexip Infinity requires a dedicated VMware host for supported deployments. Multitenancy with other applications may be supported in the future, and is possible in a test environment as long as other applications on the same host server are not consuming significant CPU and Pexip Infinity can be given reserved memory.

General recommendations

Pexip Infinity can take advantage of advanced CPU features, so for optimal performance we recommend that you run Conferencing Nodes on your newer host servers.

CPUs with a large cache (15–30 MB+) are recommended over CPUs with a smaller cache (4–10 MB), especially when running 10 or more participants per conference.

To protect the overall quality of the conference, we highly recommend that any hardware resources allocated to a Conferencing Node are reserved specifically for its own use.

Impact on virtual environment

CPU

The CPU is the most critical component in a successful deployment of the Pexip Infinity platform.

Newer Intel (or AMD) CPUs typically provide more features which Pexip Infinity will utilize to give better performance. We therefore recommend that you deploy Pexip Infinity on newer hardware, and move applications that are not so time-critical (for example, mail servers, web servers, file servers) to your older hardware.

Memory

The memory specified for the Pexip Infinity deployment should not be shared with other processes, because Pexip Infinity accesses memory at a high speed when active. However, the amount of memory needed is quite small compared to the workload, and increasing the memory beyond the recommended scope will not significantly increase performance.

Storage

Apart from storing the Pexip Infinity application, the disk activity during operation will mainly be used for logging. There is therefore no need to deploy your fastest or newest SSD drives for this application, as most of the real-time activity happens in memory. Standard

disk access as required for most servers should be used to get good logging performance. Although Pexip Infinity will work with SAS drives, we strongly recommend SSDs for both the Management Node and Conferencing Nodes. General VM processes (such as snapshots and backups) and platform upgrades will be faster with SSDs.

Network

Gigabit Ethernet connectivity from the host server is strongly recommended, because Conferencing Nodes are sending and receiving real-time audio and video data, and any network bottlenecks should be avoided. The amount of traffic to be expected can be calculated based on the capacity of the servers, but typically 100 Mbps network links can easily be saturated if there is a large number of calls going through a given Conferencing Node. In general, you can expect 1–3 Mbps per call connection, depending on call control setup.

Traffic shaping

Any shaping of the Conferencing Node traffic that can potentially limit its flow should not be used without considerable planning. If bandwidth usage to or from a Conferencing Node is too high, this should be addressed in the call control, as shaping it on the Conferencing Node level will most likely reduce the experience for the participants.

NIC teaming

VMware NIC teaming is a way to group several network interface cards (NICs) to behave as one logical NIC. When using NIC teaming in ESXi, we recommend you load balance based on **originating virtual port ID** due to its low complexity (it does not steal CPU cycles from the host). You can also load balance based on **source MAC hash**; however we do not recommend **IP hash** because of the high CPU overhead when a large number of media packets are involved.

Upgrading VM hardware versions

The virtual hardware version is fixed at the time a Management Node or Conferencing Node VM is first deployed. If you subsequently upgrade your Pexip Infinity deployment, you may need to manually upgrade the VM hardware version to ensure you can make use of support for the most recent CPU instruction sets.

Pexip Infinity supports hardware versions 11 and later. Note that:

- AVX2 instruction set requires ESXi 6.0+ and VM hardware version 11+
- AVX512 instruction set requires ESXi 6.7+ and VM hardware version 14+


Management Node: we recommend upgrading the hardware version of the Management Node VM to match the ESXi host version that the Management Node is running on.

Conferencing Nodes: we recommend upgrading the hardware version of the Conferencing Node VMs to at least match the ESXi host version that you are running in your environment.

See <https://kb.vmware.com/s/article/1010675> for ESXi version to virtual hardware version compatibility information, and instructions on upgrading a VM's hardware version (vmversion).

vMotion

Conferencing Nodes (and the Management Node) can be moved across host servers using vMotion.

-  You must put the Conferencing Node into maintenance mode and wait until all conferences on that node have finished before migrating it to another host server.

For more information on vMotion in general, see <http://www.vmware.com/products/vsphere/features/vmotion.html>.



Enhanced vMotion Compatibility (EVC)

When EVC (Enhanced vMotion Compatibility) is enabled across a cluster of host servers, all servers in that cluster will emulate the lowest common denominator CPU. This allows you to move VMs between any servers in the cluster without any problems, but it means that if any servers in that cluster have newer-generation CPUs, their advanced features cannot be used.

Because Conferencing Nodes use the advanced features of newer-generation CPUs, (for example AVX and later on newer Intel CPUs), we recommend that you disable EVC (Enhanced vMotion Compatibility) for any clusters hosting Conferencing Nodes where the cluster includes a mix of new and old CPUs.

If you enable EVC on mixed-CPU clusters, the Pexip Infinity platform will run more slowly because it will cause the Conferencing Nodes to assume they are running on older hardware.

If you enable EVC, you must select the Sandy Bridge-compatible EVC mode as a minimum. This is the lowest EVC mode that supports the AVX instruction set, which is the minimum required to run the Pexip Infinity platform.

-  When enabling EVC or lowering the EVC mode, you should first shut down any currently running VMs with a higher EVC mode than the one you intend to enable.
-  When disabling EVC or raising the EVC mode, any currently running VMs will not have access to the new level until they have been shut down and restarted.

For instructions on disabling EVC, see [Disabling EVC](#).

For more information on EVC in general, see <https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.vcenterhost.doc/GUID-9F444D9B-44A0-4967-8C07-693C6B40278A.html>.

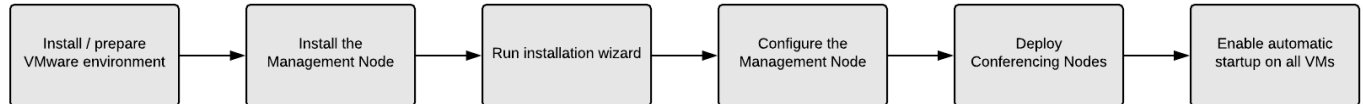
Installing the Management Node

Before installing the Management Node we recommend that you review the [VMware configuration prerequisites](#) and the [Installation checklist](#).

Installation of the Management Node is a two-step process:

1. **Deploying the VM template:** this creates a new unconfigured instance of a generic Management Node VM.
The process for deploying the template in a VMware hypervisor environment is described below.
2. **Running the installation wizard:** after deploying the Management Node template, the [installation wizard](#) allows you to enter the basic configuration details for your Management Node VM.

This flowchart provides an overview of the basic steps involved in deploying the Pexip Infinity platform on VMware:



Deploying the Management Node template

i If an ESXi host is being managed by vCenter Server, all administration must be performed via vCenter Server. Do not log in directly to the ESXi host; configuration changes made in this way may be lost. To ensure that ESXi hosts being managed by vCenter Server are accessible via vCenter Server only and are not directly accessible, you should put them in Lockdown mode. Lockdown mode forces all operations to be performed through vCenter Server.

To install a new instance of a Pexip Infinity Management Node using the vSphere web client:

1. Either:
 - a. Ensure the VM Manager can access the **Management Node OVA image** file hosted on the [Pexip download page](#), or
 - b. Download the **Management Node OVA image** file from the [Pexip download page](#) to your local machine.
2. Log in to the VM Manager (vCenter Server).
3. If you are using VMware 7.0u3 or later you must import an intermediate certificate bundle to enable VMware to trust the OVA image:
 - a. Go to <https://dl.pexip.com/resources/certificates/index.html>, and download the intermediate certificate PEM file **2022_10-bundle.pem**.
 - b. Import the PEM file into VMware as described in <https://kb.vmware.com/s/article/84240>.

Note that:

 - If you do not import the certificate bundle, you can still deploy the OVA image but you will have to ignore the untrusted certificate warnings.
 - Earlier versions of VMware do not require the certificate bundle as they do not perform the same level of validation.
4. Select **VMs and Templates**.
5. Click on the **Actions** menu and select **Deploy OVF Template....**
The **Deploy OVF Template** window will open.
6. At the **Select template** step, either enter the URL to download the **Management Node OVA image** file, or **Browse** to the location of the **Pexip Infinity OVA** file, and select **Next**:

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template
Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
☒ URL
☐ Local file

 No file chosen

7. If you are using VMware 7.0u3 or later, a **Source Verification** pop-up appears (even if you have imported the certificate bundle). Verify that the certificate thumbprint shown is **AF:1F:4D:92:2D:DF:5F:81:1C:C2:BC:D5:38:28:14:75:0A:D9:02:0E** and then select **Yes** to proceed.

8. At the **Select name and folder** step:

- a. Enter an appropriate **Name** for the Management Node. This name is used in the VMware interface to identify this Management Node virtual machine (VM).
- b. Select the location or datacenter within which the Management Node will be located.
- c. Select **Next**.

9. At the **Select a compute resource** step, select the host, cluster, resource pool or vApp in which to run the template, and select **Next**.

10. At the **Review details** step, you may see the following warning:

This warning message is shown whenever any advanced settings are part of an OVA deployment. Here, the advanced configuration options that are being referenced are those mandated for the US Department of Defense JITC (Joint Interoperability Test Command) certification.

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Ready to complete

The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	Pexip AS (Untrusted certificate)
Product	Pexip Infinity
Version	28.1.0
Vendor	Pexip AS
Download size	1.3 GB
Size on disk	Unknown (thin provisioned) 98.6 GB (thick provisioned)
Extra configuration	parallelIO.present = FALSE tools.setInfo.sizeLimit = 1048576 scsiO:0.mode = persistent RemoteDisplay.maxConnections = 1 isolation.tools.vixMessage.disable = TRUE isolation.tools.diskShrink.disable = TRUE isolation.tools.memSchedFakeSampleStats.disable = TRUE vmSafe.enable = FALSE isolation.monitor.control.disable = TRUE isolation.tools.copy.disable = TRUE isolation.gui.hostShellAction.disable = TRUE isolation.tools.getCreds.disable = TRUE isolation.device.connectable.disable = TRUE isolation.tools.unify.disable = TRUE log.keepOld = 10

Select **Next**.

11. At the **License agreements** step, read the license agreements, and if you agree to the terms select **Accept** and then **Next**.
12. At the **Select storage** page, select a **Thick** virtual disk format, a **VM Storage Policy** and **Datastore** to be used, and select **Next**.
13. At the **Select networks** step, select the VM Network and IP configuration, and select **Next**.
14. At the **Ready to complete** page, review the configuration and select **Finish**.

Progress is shown in the **Recent Tasks** tab at the bottom of the screen. When the template has been deployed successfully, a green tick will appear.

Enabling automatic startup

After deploying a new Management Node from VMware, you must enable automatic startup of that virtual machine (VM). In VMware, automatic startup is disabled by default for every new VM — which means that if the host server is powered down for any reason, when it restarts the VM will not restart and must be started manually.

You can only enable automatic startup after the Management Node has been deployed.

To enable automatic startup using the vSphere web client (HTML 5):

1. Log in to the VM manager (vCenter Server).
2. From the navigation panel, select the **Hosts And Clusters** tab and navigate to the host server on which the node's VM is installed.
3. From the main panel, select the **Configure** tab.
4. From the left-hand panel, select **Virtual Machines > VM Startup/Shutdown**.
5. At the top right of the page, select **Edit**.
6. In the **System influence** section, select **Automatically start and stop the virtual machines with the system**.
7. Select **OK**.

Running the installation wizard

To run the installation wizard, which configures the Management Node, you must open a console window on the Management Node VM.

Opening a console window

1. Using the vSphere client, log in to the Management Node's VM Manager (vCenter Server or, for stand-alone deployments, the ESXi host).
2. Power on the new Management Node VM (if it is not already powered on).
3. Right-click on the new Management Node VM and select **Open Remote Console > Web Console**.

Running the installation wizard

1. At the prompt, enter the username *admin*.

The display reads:

```
You are required to change your password immediately (root enforced)
Enter new UNIX password:
```

2. Create a password for the Management Node operating system by typing the password, pressing Enter, retyping the password, and pressing Enter again.
3. Ensure you record the password in a secure location. After you have finished running the installation wizard you will not need the password again unless you need to access the Management Node using SSH.

You are presented with another login prompt:

```
[sudo] password for admin:
```

4. Log in again with the password you just created.
The Pexip installation wizard starts.
5. Follow the prompts to set the following configuration for the Management Node.

If you press enter, the default value is applied:

Setting	Default value	Multiple entries allowed?	Can be changed via Pexip Infinity Administrator interface?
IP address	As assigned by DHCP, otherwise 192.168.0.100 *	No	No ‡
Network mask	As assigned by DHCP, otherwise 255.255.255.0 *	No	No ‡

Setting	Default value	Multiple entries allowed?	Can be changed via Pexip Infinity Administrator interface?
Gateway	As assigned by DHCP, otherwise 192.168.0.1 *	No	No ‡
Hostname	As assigned by DHCP, otherwise <no default>	No	No ‡
Domain suffix	As assigned by DHCP, otherwise <no default>	No	No ‡
DNS servers	As assigned by DHCP, otherwise 8.8.8.8	Yes, if separated by a space or comma	Yes
NTP servers †	As assigned by DHCP, otherwise two of the following: <ul style="list-style-type: none"> 0.pexip.pool.ntp.org 1.pexip.pool.ntp.org 2.pexip.pool.ntp.org 3.pexip.pool.ntp.org 	Yes, if separated by a space or comma	Yes
Web administration username	admin	No	No ‡
Web administration password	<no default>	No	Yes
Enable incident reporting (yes/no)	<no default>		Yes
Contact email address **	<no default>	No	Yes
Send deployment and usage statistics to Pexip (yes/no)	<no default>		Yes

* The addresses entered here are assigned as static IP addresses.

** Shown and required if incident reporting is enabled.

† The NTP server must be accessible by the Management Node at the time the startup wizard is run. Installation will fail if the Management Node is unable to synchronize its time with an NTP server.

‡ After they have been configured, do not attempt to change these settings by any other means. To change these settings on server-based deployments, you must re-run the installation wizard.

The installation begins and the Management Node restarts using the values you have configured.

Initial platform configuration

After you have run the installation wizard, you must perform some preliminary configuration of the Pexip Infinity platform before you can deploy a Conferencing Node.

This section lists the configuration required, and provides a summary of each step with a link to further information.

All configuration should be done using the Pexip Infinity Administrator interface.

i **No changes** should be made to any Pexip VM via the terminal interface (other than as described when running the initial Pexip 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, configuration of Ethernet interfaces, or the installation of any third-party code/applications.

Accessing the Pexip Infinity Administrator interface

The Pexip Infinity Administrator interface is hosted on the Management Node. To access this:

1. Open a web browser and type in the IP address or DNS name that you assigned to the Management Node using the installation wizard (you may need to wait a minute or so after installation is complete before you can access the Administrator interface).
2. Until you have uploaded appropriate TLS certificates to the Management Node, your browser may present you with a warning that the website's security certificate is not trusted. You should proceed, but upload appropriate TLS certificates to the Management Node (and Conferencing Nodes, when they have been created) as soon as possible.

The **Pexip Infinity Conferencing Platform** login page will appear.

3. Log in using the web administration username and password you set using the installation wizard.

You are now ready to begin configuring the Pexip Infinity platform and deploying Conferencing Nodes.

As a first step, we strongly recommend that you configure at least 2 additional NTP servers or NTP server pools to ensure that log entries from all nodes are properly synchronized.

It may take some time for any configuration changes to take effect across the Conferencing Nodes. In typical deployments, configuration replication is performed approximately once per minute. However, in very large deployments (more than 60 Conferencing Nodes), configuration replication intervals are extended, and it may take longer for configuration changes to be applied to all Conferencing Nodes (the administrator log shows when each node has been updated).

Brief details of how to perform the initial configuration are given below. For complete information on how to configure your Pexip Infinity solution, see the Pexip Infinity technical documentation website at docs.pexip.com.

Configuring the Pexip Infinity platform

This table lists the Pexip Infinity platform configuration steps that are required before you can deploy Conferencing Nodes and make calls.

Configuration step	Purpose
1. Enable DNS (System > DNS Servers)	<p>Pexip Infinity uses DNS to resolve the hostnames of external system components including NTP servers, syslog servers, SNMP servers and web proxies. It is also used for call routing purposes — SIP proxies, gatekeepers, external call control and conferencing systems and so on. The address of at least one DNS server must be added to your system.</p> <p>You will already have configured at least one DNS server when running the install wizard, but you can now change it or add more DNS servers.</p>

Configuration step	Purpose
2. Enable NTP (System > NTP Servers)	<p>Pexip Infinity uses NTP servers to obtain accurate system time. This is necessary to ensure correct operation, including configuration replication and log timestamps.</p> <p>We strongly recommend that you configure at least three distinct NTP servers or NTP server pools on all your host servers and the Management Node itself. This ensures that log entries from all nodes are properly synchronized.</p> <p>You will already have configured at least one NTP server when running the install wizard, but you can now change it or add more NTP servers.</p>
3. Add licenses (Platform > Licenses)	<p>You must install a system license with sufficient concurrent call capacity for your environment before you can place calls to Pexip Infinity services.</p>
4. Add a system location (Platform > Locations)	<p>These are labels that allow you to group together Conferencing Nodes that are in the same datacenter. You must have at least one location configured before you can deploy a Conferencing Node.</p>
5. Upload TLS certificates (Certificates > TLS Certificates)	<p>You must install TLS certificates on the Management Node and — when you deploy them — each Conferencing Node. TLS certificates are used by these systems to verify their identity to clients connecting to them.</p> <p>All nodes are deployed with self-signed certificates, but we strongly recommend they are replaced with ones signed by either an external CA or a trusted internal CA.</p>
6. Add Virtual Meeting Rooms (Services > Virtual Meeting Rooms)	<p>Conferences take place in Virtual Meeting Rooms and Virtual Auditoriums. VMR configuration includes any PINs required to access the conference. You must deploy at least one Conferencing Node before you can call into a conference.</p>
7. Add an alias for the Virtual Meeting Room (done while adding the Virtual Meeting Room)	<p>A Virtual Meeting Room or Virtual Auditorium can have more than one alias. Conference participants can access a Virtual Meeting Room or Virtual Auditorium by dialing any one of its aliases.</p>

Deploying a Conferencing Node on an ESXi host

This process generates an **.ova** file that then must be deployed from within VMware on to an ESXi host.

Note that:

- This file is specific to the Conferencing Node being deployed. It cannot be used to deploy multiple Conferencing Nodes.
- The file is single-use. It cannot be used to re-deploy the same Conferencing Node at a later date. To re-deploy the Conferencing Node, you must first delete it from the Pexip Infinity Management Node and from VMware, and then deploy a new Conferencing Node with the same configuration as the deleted node.
- Before you start, ensure that you are currently using the same machine that you will subsequently use to upload the generated file on to your host server.

Generating, downloading and deploying the ova file

1. From the Pexip Infinity Administrator interface, go to **Platform > Conferencing Nodes** and select **Add Conferencing Node**.
2. You are now asked to provide the network configuration to be applied to the Conferencing Node, by completing the following fields:

Option	Description
Name	Enter the name to use when referring to this Conferencing Node in the Pexip Infinity Administrator interface.
Description	An optional field where you can provide more information about the Conferencing Node.
Role	<p>This determines the Conferencing Node's role:</p> <ul style="list-style-type: none">◦ Proxying Edge Node: a Proxying Edge Node handles all media and signaling connections with an endpoint or external device, but does not host any conferences — instead it forwards the media on to a Transcoding Conferencing Node for processing.◦ Transcoding Conferencing Node: a Transcoding Conferencing Node handles all the media processing, protocol interworking, mixing and so on that is required in hosting Pexip Infinity calls and conferences. When combined with Proxying Edge Nodes, a transcoding node typically only processes the media forwarded on to it by those proxying nodes and has no direct connection with endpoints or external devices. However, a transcoding node can still receive and process the signaling and media directly from an endpoint or external device if required.
Hostname Domain	<p>Enter the hostname and domain to assign to this Conferencing Node. Each Conferencing Node and Management Node must have a unique hostname.</p> <p>The Hostname and Domain together make up the Conferencing Node's DNS name or FQDN. We recommend that you assign valid DNS names to all your Conferencing Nodes.</p>
IPv4 address	Enter the IP address to assign to this Conferencing Node when it is created.
Network mask	<p>Enter the IP network mask to assign to this Conferencing Node.</p> <p>Note that IPv4 address and Network mask apply to the eth0 interface.</p>
Gateway IPv4 address	<p>Enter the IP address of the default gateway to assign to this Conferencing Node.</p> <p>Note that the Gateway IPv4 address is not directly associated with a network interface, except that the address entered here lies in the subnet in which either eth0 or eth1 is configured to use. Thus, if the gateway address lies in the subnet in which eth0 lives, then the gateway will be assigned to eth0, and likewise for eth1.</p>
Secondary interface IPv4 address	The optional secondary interface IPv4 address for this Conferencing Node. If configured, this interface is used for signaling and media communications to clients, and the primary interface is used for communication with the Management Node and other Conferencing Nodes.

Option	Description
Secondary interface network mask	The optional secondary interface network mask for this Conferencing Node. Note that Secondary interface IPv4 address and Secondary interface network mask apply to the eth1 interface.
System location	Select the physical location of this Conferencing Node. A system location should not contain a mixture of proxying nodes and transcoding nodes. If the system location does not already exist, you can create a new one here by clicking ➕ to the right of the field. This will open up a new window showing the Add System Location page.
SIP TLS FQDN	A unique identity for this Conferencing Node, used in signaling SIP TLS Contact addresses.
TLS certificate	The TLS certificate to use on this node. This must be a certificate that contains the above SIP TLS FQDN . Each certificate is shown in the format <subject name> (<issuer>).
IPv6 address	The IPv6 address for this Conferencing Node. Each Conferencing Node must have a unique IPv6 address.
Gateway IPv6 address	The IPv6 address of the default gateway. If this is left blank, the Conferencing Node listens for IPv6 Router Advertisements to obtain a gateway address.
IPv4 static NAT address	The public IPv4 address used by this Conferencing Node when it is located behind a NAT device. Note that if you are using NAT, you must also configure your NAT device to route the Conferencing Node's IPv4 static NAT address to its IPv4 address .
Static routes	From the list of Available Static routes , select the routes to assign to the node, and then use the right arrow to move the selected routes into the Chosen Static routes list.
Enable distributed database	This should usually be enabled (checked) for all Conferencing Nodes that are expected to be "always on", and disabled (unchecked) for nodes that are expected to only be powered on some of the time (e.g. nodes that are likely to only be operational during peak times).
Enable SSH	Determines whether this node can be accessed over SSH. Use Global SSH setting: SSH access to this node is determined by the global Enable SSH setting (Platform > Global Settings > Connectivity > Enable SSH). Off: this node cannot be accessed over SSH, regardless of the global Enable SSH setting. On: this node can be accessed over SSH, regardless of the global Enable SSH setting. Default: Use Global SSH setting .

3. Select **Save**.

4. You are now asked to complete the following fields:

Option	Description
Deployment type	Select Manual (ESXi 8.0 and above) , Manual (ESXi 7.0) , Manual (ESXi 6.7) or Manual (ESXi 6.5) as appropriate.
Number of virtual CPUs to assign	Enter the number of virtual CPUs to assign to the Conferencing Node. We recommend no more than one virtual CPU per physical core, unless you are making use of CPUs that support Hyper-Threading.
System memory (in megabytes) to assign	Enter the amount of RAM (in megabytes) to assign to the Conferencing Node. The number entered must be a multiple of 4. We recommend 1024 MB (1 GB) RAM for each virtual CPU. The field automatically defaults to the recommended amount, based on the number of virtual CPUs you have entered.

Option	Description
SSH password	<p>Enter the password to use when logging in to this Conferencing Node's Linux operating system over SSH. The username is always <i>admin</i>.</p> <p>Logging in to the operating system is required when changing passwords or for diagnostic purposes only, and should generally be done under the guidance of your Pexip authorized support representative. In particular, do not change any configuration using SSH — all changes should be made using the Pexip Infinity Administrator interface.</p>

5. Select **Download**.

A message appears at the top of the page: "The Conferencing Node image will download shortly or click on the following link".

After a short while, a file with the name **pexip-<hostname>.<domain>.ova** is generated and downloaded.

Note that the generated file is only available for your current session so you should download it immediately.

6. When you want to deploy the Conferencing Node VM, use a vSphere client to log in to vCenter Server. Select the **VMs and Templates** tab, click on the **Actions** menu and select **Deploy OVF Template....**

7. Follow the on-screen prompts to deploy the **.ova** file; this is similar to the steps you used when deploying the Management Node. You should always deploy the nodes with Thick Provisioned disks.

After deploying a new Conferencing Node, it takes approximately 5 minutes before the node is available for conference hosting and for its status to be updated on the Management Node. Until it becomes available, the Management Node reports the status of the Conferencing Node as having a last contacted and last updated date of "Never". "Connectivity lost between nodes" alarms relating to that node may also appear temporarily.

Enabling automatic startup

After deploying a new Conferencing Node from VMware, you must enable automatic startup of that virtual machine (VM). In VMware, automatic startup is disabled by default for every new VM — which means that if the host server is powered down for any reason, when it restarts the VM will not restart and must be started manually.

You can only enable automatic startup after the Conferencing Node has been deployed.

To enable automatic startup using the vSphere web client (HTML 5):

1. Log in to the VM manager (vCenter Server).
2. From the navigation panel, select the **Hosts And Clusters** tab and navigate to the host server on which the node's VM is installed.
3. From the main panel, select the **Configure** tab.
4. From the left-hand panel, select **Virtual Machines > VM Startup/Shutdown**.
5. At the top right of the page, select **Edit**.
6. In the **System influence** section, select **Automatically start and stop the virtual machines with the system**.
7. Select **OK**.

Disabling EVC

We strongly recommend that you disable EVC (Enhanced vMotion Compatibility) for any ESXi clusters hosting Conferencing Nodes that include a mix of old and new CPUs. If EVC is enabled on such clusters, the Pexip Infinity platform will run more slowly because the Conferencing Nodes assume they are running on older hardware.

To disable EVC:

1. From the vSphere client's navigation panel, select the cluster.
2. From the main panel, select the **Configure** tab.
3. From the left-hand panel, select **Configuration > VMware EVC**.
The current EVC settings are shown.
4. At the top right of the page, select **Edit**.
5. Select **Disable EVC**.




Testing and next steps after initial installation

After you have completed your installation and initial configuration of Pexip Infinity, you can make a test call to check that your system is working. You can also extend your deployment by integrating it with other call control or third-party systems, or by customizing the user experience. You should also consider how to let your users know about their new video conferencing service.

Making a test call

When you have deployed a Conferencing Node and configured a Virtual Meeting Room and an alias, you can make a test call to check that your system is working.

An easy way to do this is by using the Connect web app to dial the alias of one of the Virtual Meeting Rooms you've already created. Full details of how to use the Connect web app are given in [Using Connect web apps](#), but in summary:

1. Open a browser (we recommend Chrome or Edge) and type in the IP address (or FQDN, if you've set it up already) of one of the Conferencing Nodes.
 -  If your browser displays a security warning, this means that it does not trust the Conferencing Node's certificate. This could be because you have not replaced the node's default self-signed certificate, or you have used your own private certificates that have not been signed by an external Certificate Authority.
2. When prompted, enter your name.
3. In the **Meeting ID** field, enter the alias of the Virtual Meeting Room you are using for testing.
4. Ensure that you have selected the camera and microphone you wish to use, and they are working correctly:
 - You should see your own image in the video window.
 - The microphone icon shows a green bar  to indicate the level of audio being detected. To join without your audio, select the microphone icon; this will change to  to indicate that your microphone is off.
5. Select **Join**.
6. From another device, join the conference in the same way.

The two participants should be able to see and hear each other, and share content.

See [About the Connect web app](#) for more information.

Further configuration

You are now ready to continue [configuring the Pexip Infinity platform](#) and [services](#) and deploying more [Conferencing Nodes](#).

Specifically, you should now do the following:

- [Assigning hostnames and FQDNs](#)
- [Enabling SNMP on Conferencing Nodes](#)

At some point you may also want to:

- [integrate the Pexip Infinity platform with your call control system](#)
- [configure the Pexip Infinity Distributed Gateway](#)
- [register devices directly to the Pexip Infinity platform](#)
- [customize the user experience](#)

Integrating with a call control system

To integrate Pexip Infinity with your call control system, you must configure a trunk or neighbor zone towards each of the Conferencing Nodes.

For further information about how to configure your specific call management system to work with Pexip Infinity, see the following documentation:

- [Pexip Infinity and Microsoft Skype for Business / Lync Deployment Guide](#)
- [Pexip Infinity and Cisco VCS Deployment Guide](#)
- [Pexip Infinity and Cisco Unified Communications Manager Deployment Guide](#)
- [Pexip Infinity and Polycom DMA Deployment Guide](#)

Configuring the Pexip Infinity Distributed Gateway

The Pexip Infinity Distributed Gateway ("Infinity Gateway") enables endpoints to make calls to other endpoint devices or systems. This includes calls between devices that use different protocols and media formats, such as SIP and H.323 systems, Skype for Business clients (MS-SIP), and Connect app clients (WebRTC). It also enables you to route calls from VTCs and standards-based endpoints into an externally-hosted conference, such as a Microsoft Teams or Skype for Business meeting, or Google Meet.

Registering devices directly to the Pexip Infinity platform

SIP and H.323 endpoints, and some Connect app clients can register directly to Pexip Infinity Conferencing Nodes. This allows Pexip Infinity to route outbound calls to those registered devices without having to go via a SIP proxy or H.323 gatekeeper, or rely on DNS.

Customizing the user experience

You can easily apply your own corporate branding to the Pexip Infinity platform, and produce a personalized user experience for all of your Pexip Infinity services.

Informing users about the new video conferencing service

Finally, you'll need to let your end users know about the new video conferencing services available to them, and how they can use it. The following end user guides are available:

- [Using your Virtual Meeting Room](#)
- [Using the Connect web apps](#)
- [Using the Connect desktop app](#)
- [Using the Connect mobile app](#)

We also have provided some [Example emails for sending to new users](#), which you can use as a basis for the information you provide to your users.

Pexip Infinity installation checklist

Use this checklist to identify the key tasks involved in preparing for and deploying the Pexip Infinity platform. Also, there is a configuration [datasheet](#) below to help you gather the key network and configuration information required.

Prior to installation

1. Download the appropriate Pexip Infinity Management Node installation file from the [Pexip download page](#).
2. Ensure that you have appropriate host servers (see [Server design guidelines](#)).
3. Assign network IP addresses and host names for the Management Node and Conferencing Nodes.
4. Create DNS records for your Management Node administration.
5. Create DNS records to allow endpoints/clients to discover your Pexip Infinity Conferencing Nodes (see [DNS record examples](#)).
6. Generate or request certificates (Base64-encoded X.509 PEM format) for the Management Node and Conferencing Nodes (see guidelines at [Certificate creation and requirements](#)).

Hypervisor / host servers

1. Note the CPU model number and the number of cores per socket on the host server to be used with the Conferencing Nodes, as this determines the maximum number of vCPUs to assign for the Conferencing Nodes.
2. Prior to deploying the Management Node or a Conferencing Node, ensure that all host servers are synchronized to NTP servers.
3. Upload the OVA file (or ZIP for Hyper-V) of the Management Node and run the setup wizard from the hypervisor console.

Pexip Infinity Administrator interface

1. Configure basic Management Node settings after installation (licenses, any additional DNS or NTP servers).
2. Add a system location.
3. Deploy Conferencing Nodes to the location (in conjunction with your hypervisor management tools).
4. Configure the SIP TLS FQDN on the Conferencing Nodes.
5. Verify your node's DNS records. (You can use the tool at <http://dns.pexip.com> to lookup and check SRV records for a domain.)
6. Replace the self-signed server certificates on the Management Node and Conferencing Nodes with your own certificates that have been signed by either an external CA or a trusted internal CA (see [Managing TLS certificates](#)).
7. Upload any required chain of intermediate CA certificates to the Management Node.
You can use a tool such as <https://www.sslshopper.com/ssl-checker.html> to verify certificates and the chain of trust (specify port 5061 i.e. use the format <domain>:5061 for the server hostname to ensure that SIP TLS connections are checked).
8. Configure your VMRs and aliases.
9. Configure the Infinity Gateway (via Call Routing Rules), if required.

Hypervisor maintenance

1. Enable automatic startup on every VM.
2. Backup your Management Node VM, and optionally, your Conferencing Node VMs.

Pexip Infinity configuration datasheet

Use this datasheet to help you gather the key network and configuration information required for your deployment.

Management Node (installation wizard)

Management Node IP address:

Network mask:

Gateway IP address:

Management Node hostname:

Management Node domain:

DNS server 1:

DNS server 2:

NTP server 1:

NTP server 2:

Management Node (configuration)

VM name:

System location 1 name:

License entitlement key:

Conferencing Nodes

CPU cores per socket on host server:
(to determine the size of each node)

Conferencing Node 1 name / VM name:

Conferencing Node 1 IP address:

Conferencing Node 1 hostname and domain:

Conferencing Node 2 name / VM name:

Conferencing Node 2 IP address:

Conferencing Node 2 hostname and domain:

For complete information on how to configure your Pexip Infinity solution, see the Pexip Infinity technical documentation website at docs.pexip.com.