Pexip Infinity v33.1

Release Notes

Software Version 33.1

Document Version 33.1.a

December 2023

Contents

Introduction

This document contains the release notes for Pexip Infinity version 33.1.

Complete information about how to install and operate Pexip Infinity is available from the Pexip technical documentation website at docs.pexip.com.

The website also contains comprehensive documentation on all aspects of deploying the Pexip Infinity platform. This includes how to administer and use the Connect app client suite; how to configure Pexip Infinity features such as One-Touch Join, VMR Scheduling for Exchange and Pexip Service; and how to integrate Pexip Infinity with other third-party systems and call control solutions including Google Meet, Microsoft Teams, Microsoft Skype for Business and Lync, Cisco Unified Communications Manager, Cisco VCS and Polycom DMA.

Management Node host server sizing information

- For typical deployments of **up to 30** Conferencing Nodes, you must ensure that the Management Node host server has at least 4 vCPUs and 4 GB of RAM.
- For deployments with **more than 30** Conferencing Nodes, you will need to increase the number of cores and the amount of RAM on the Management Node. Please contact your Pexip authorized support representative or your Pexip Solution Architect for guidance on Management Node sizing specific to your environment.

Upgrading to version 33.1

ℹ If you are running a software version between v27 and v31.3 inclusive, you must first upgrade to version **31.4** and then upgrade again to version 33.1; see Upgrading from versions 27-31.3 to version 33.1.

Upgrading from version 31.4 or later to version 33.1

When the upgrade process starts, the Management Node is upgraded first. Then up to 10 Conferencing Nodes are selected and are automatically placed into maintenance mode. When all calls have finished on a node that is in maintenance mode, that node is upgraded and then put back into active service. Another Conferencing Node is then selected, placed into maintenance mode and upgraded, and so on until all Conferencing Nodes have been upgraded.

If all of the calls on a Conferencing Node that is in maintenance mode have not cleared after 1 hour, the node is taken out of maintenance mode and put at the back of the queue of nodes to be upgraded. A further attempt to upgrade that node will be made after all other nodes have been upgraded (or had upgrade attempts made). Up to 10 Conferencing Nodes may simultaneously be in maintenance mode or in the process of being upgraded at any one time.

Alternatively, to avoid unpredictable system behavior due to Conferencing Nodes running conflicting software versions, you may want to manually put **all** of your Conferencing Nodes into maintenance mode before initiating the upgrade process. This will allow all existing calls to finish, but will not admit **any** new calls. You should then actively monitor your Conferencing Nodes' status and manually take each node out of maintenance mode after it has been upgraded to the new software version, so that the system can start taking new calls again on those upgraded nodes.

Remove MD5/SHA1 certificates before upgrading to v32 or later

ℹ If you are upgrading from versions prior to v32, you must remove any existing MD5/SHA1 certificates, except root certificates, before upgrading to v32 or later.

You can check all your existing certificates by the following methods:

- Go to **Certificates > TLS Certificates** and **Certificates > Intermediate CA Certificates**, and then view the **Certificate contents** for each certificate and check the **Signature Algorithm** for references to md5 or sha1.
- Go to **https://<manageraddress>/api/admin/configuration/v1/tls_certificate/** and **https://<manageraddress>/api/admin/configuration/v1/ca_certificate/** and search for references to md5 or sha1.

How to upgrade

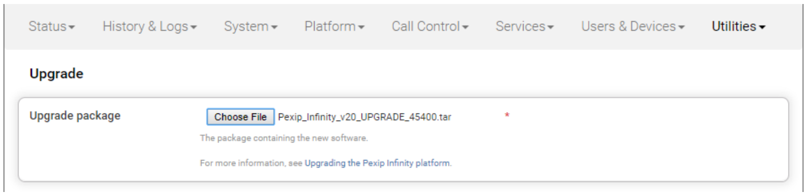
When upgrading, please note that:

- A Management Node upgrade may take a long time, potentially up to 1 hour. Do **not** reboot the Management Node under any circumstances. If you are concerned about the time the upgrade is taking, please contact your Pexip authorized support representative.
- There is normally no need to reboot a Conferencing Node. If a Conferencing Node appears to be stuck for over 1 hour then contact your Pexip authorized support representative — do **not** reboot the node.

To upgrade Pexip Infinity software from v31.4 or later to v33.1:

1. Before upgrading an on-premises deployment, we recommend that you use your hypervisor's snapshot functionality to take a full VMware/Hyper-V snapshot of the Management Node. You may also want to take a snapshot of each Conferencing Node, although depending on the size and complexity of your deployment it may be easier to simply redeploy these from the Management Node (after it has been rolled back) in the unlikely event that this is required.

   Before upgrading a cloud-based deployment (Azure, AWS, GCP or Oracle), you should backup the Management Node via Pexip Infinity's inbuilt mechanism (**Utilities > Backup/Restore**).
2. Download the Pexip Infinity upgrade package for v33.1 from the Pexip download page.
3. Before upgrading, ensure that all "always-on" Conferencing Nodes are powered on and are reachable (i.e. no Connectivity Loss errors), and are all running the same version from which you are upgrading. You do not need to power on any cloud bursting nodes.
4. From the Pexip Infinity Administrator interface, go to **Utilities > Upgrade**.
5. Select **Choose File** and browse to the location of the upgrade package.



Upgrade

Upgrade package: Pexip_Infinity_v20_UPGRADE_45400.tar *

The package containing the new software.

For more information, see Upgrading the Pexip Infinity platform.

6. Select **Continue**. There will be a short delay while the upgrade package is uploaded.

   After the upgrade package has been uploaded, you are presented with a confirmation page showing details of the existing software version and the upgrade version.
7. To proceed, select **Start upgrade**.

   You are taken to the **Upgrade Status** page, showing the current upgrade status of the Management Node and all Conferencing Nodes. This page automatically refreshes every 5 seconds.
8. When the upgrade completes, all nodes will show a status of **No upgrade in progress** and have the new **Installed version**.

   If the upgrade process completes and there are some nodes that have failed to upgrade, you can restart the upgrade process by uploading the upgrade package to the Management Node again via **Utilities > Upgrade**. This will skip over any nodes that have already been upgraded.
9. If you have Pexip CVI for Microsoft Teams you must also upgrade your associated Teams Connector deployment in Azure to the same version as your Pexip Infinity deployment (including minor/"dot" releases).

   When upgrading your Teams Connector to version 33:

   New upgrade steps for version 33

   - There are some new variables in the variables script to support Microsoft Teams Rooms SIP/H.323 calling:
     - **$PexipConfiguredConnectorFqdn** and **$PexipOutboundFqdn**.

     These new variables are passed as new parameters to **create_vmss_deployment.ps1** in the installation and redeploy scripts.
   - There are some new variables in the variables script to support private routing:
     - **$PxExistingVNETResourceId** and **$PxUsePrivateRouting**.

     These new variables are passed as new parameters to **create_vmss_deployment.ps1** in the installation and redeploy scripts.
   - Changes related to the support of certificate-based authentication of the CVI app:
     - A password-based authentication future deprecation notice has been added to the installation script.
     - The **create_vmss_deployment.ps1** command in the installation and redeploy scripts now takes **AppId** and **AppPassword** parameters instead of **AppCredential** (they still support password-based authentication).
   - Other changes to the installation/redeployment scripts:
     - The commands to connect to MS Graph have been changed to use **PexTeamsMsGraph** in the **PexTeamsCviApplication** module.

   Standard upgrade steps

   - When upgrading from a previous major release (e.g. from v27.n to v33.1), you must use the latest version of the redeploy script as contained within the v33 documentation. You can use your existing redeploy script if you are upgrading to a new minor/ "dot" release for the same major version (e.g. from 33.0 to 33.1).
   - You must be using Az module version 9.0.1 minimum.
     - To check your installed version you can run:
       ```
       Get-InstalledModule -Name Az -AllVersions
       ```
     - To install the latest appropriate Az version you can run:
       ```
       Install-Module -Name Az -MinimumVersion 9.0.1 -MaximumVersion 9.7.1 -AllowClobber -Scope AllUsers
       ```
   - If you (the person performing the upgrade) did not perform the initial installation, you should ensure that you have all the relevant PowerShell modules and versions installed. If you are connecting to Azure Resource Manager / Microsoft Graph from your Windows PC for the first time, you must run the following PowerShell commands (as Administrator):
     ```
     Install-Module -Name Az -MinimumVersion 9.0.1 -MaximumVersion 9.7.1 -AllowClobber -Scope AllUsers
     Install-Module Microsoft.Graph -MinimumVersion 1.28.0 -MaximumVersion 2.2.0 -AllowClobber -Scope AllUsers
     ```
     Note that:
     - The installation of Microsoft Graph PowerShell SDK can take 5-10 minutes. Wait until you the get PS prompt back (several minutes after the install reports as completed) before continuing.

        - The Az PowerShell module collects telemetry data (usage data) by default, however you can opt out from this data collection using `Disable-AzDataCollection` (see this article for more information).
        - The Az PowerShell module remembers login information by default (i.e. you're not automatically logged out when closing your PowerShell window), but you can disable this with `Disable-AzContextAutosave` if required (see this article for more information).
    - If you have deployed multiple Teams Connectors, you must follow the same redeploy process (with the appropriate variable initialization script) for each Teams Connector.
    - As with all upgrades, you can continue to use the Pexip CVI app from your existing deployment.
    - Your Pexip Infinity and Teams Connector installations must both be running the same software version (including minor/"dot" releases).

  Full instructions are available at https://docs.pexip.com/admin/teams_managing.htm#upgrading.

If you are using VMware snapshots for backup purposes, we recommend that you delete those snapshots after approximately two weeks, providing your upgraded system is operating as expected. This is because Virtual Machines, in general, should not run with snapshots over time.

For full details on upgrading Pexip Infinity, see Upgrading the Pexip Infinity platform.

Upgrading from versions 27-31.3 to version 33.1

If you are running a software version between v27 and v31.3 inclusive, you must first upgrade to version **31.4** and then upgrade again to version 33.1. To do this:

1. Before upgrading, ensure that all "always-on" Conferencing Nodes are powered on and are reachable (i.e. no Connectivity Loss errors), and are all running the same version from which you are upgrading. You do not need to power on any cloud bursting nodes.
2. Download the Pexip Infinity **v31.4** upgrade file.
3. Follow the steps outlined in Upgrading from version 31.4 or later to version 33.1, but when asked to **Choose File** browse to the location of the **v31.4** upgrade file.
4. Verify that the upgrade has completed successfully.
5. Download the Pexip Infinity **v33.1** upgrade file.
6. Follow the steps outlined in Upgrading from version 31.4 or later to version 33.1, and when asked to **Choose File** browse to the location of the **v33.1** upgrade file.

Upgrading from versions 22-26 to version 33.1

If you are running a software version between v22 and v26 inclusive, you must first upgrade to version **27.4**, and then upgrade again to version **31.4**, and then upgrade again to 33.1. To do this:

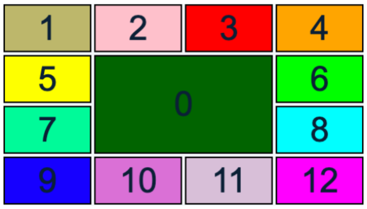
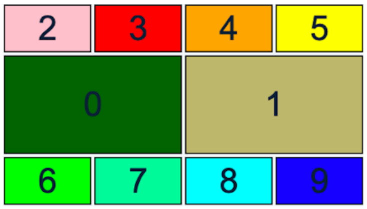
1. Before upgrading, ensure that all "always-on" Conferencing Nodes are powered on and are reachable (i.e. no Connectivity Loss errors), and are all running the same version from which you are upgrading. You do not need to power on any cloud bursting nodes.
2. Download the Pexip Infinity **v27.4** upgrade file.
3. Follow the steps outlined in Upgrading from version 31.4 or later to version 33.1, but when asked to **Choose File** browse to the location of the **v27.4** upgrade file.
4. Verify that the upgrade has completed successfully.
5. Download the Pexip Infinity **v31.4** upgrade file.
6. Follow the steps outlined in Upgrading from version 31.4 or later to version 33.1, but when asked to **Choose File** browse to the location of the **v31.4** upgrade file.
7. Verify that the upgrade has completed successfully.
8. Download the Pexip Infinity **v33.1** upgrade file.
9. Follow the steps outlined in Upgrading from version 31.4 or later to version 33.1, and when asked to **Choose File** browse to the location of the **v33.1** upgrade file.

New features and improvements in this release

You can go to https://docs.pexip.com/admin/whats_new.htm and follow the relevant links for more information about all of these features.

This topic covers the Pexip Infinity platform; for new features in the latest release of the Connect web app see the web app release notes.

Pexip Infinity platform

Feature	Description
Participant policy and custom Identity Provider attributes	You can now use local and external policy to override a participant's role, alias and display name before they join a conference. This allows you, for example, to anonymize a participant's name or modify their role based on other properties of the call or their associated Identity Provider. This new **Participant policy** option is configured in the same way as the existing local and external policy types and is executed after any service configuration policy and before any media location policy. To support participant policy, you can now also define custom attributes for your selected Identity Providers (**Users & Devices > Identity Providers > Advanced Options**). The attributes you assign are made available to any local or external participant policy, where a Connect app or other WebRTC participant uses that provider for authentication. These attributes can then be used in the participant policy decision-making process (for example whether to accept or reject a call, or assign a specific role).
Custom layouts*	You can design your own layouts and use them in the same way as the standard adaptive composition and classic layouts that are included by default. Custom layouts are specified through JSON configuration files that are uploaded via themes. The theme can then be assigned as the default theme or applied to specific VMRs and gateway rules as required, to control where your custom layouts may be used. A new **customlayouts** license is required to upload your own custom layout files. In addition, two new example custom layouts have been added to the base theme, as files **custom_layout_one_main_twelve_around.json** and **custom_layout_two_mains_eight_around.json**. These custom layouts are available for use in all service types in the same way as the existing standard layouts: • **1+12** (Large main speaker and up to 12 other participants)  • **2+8** (Two main speakers and up to 8 other participants)  (The numbers in the images indicate the order in which participants are displayed.)

Feature	Description
Portrait mode support for WebRTC devices in Adaptive Composition layouts *	Any WebRTC device with a portrait aspect ratio (such as 9:16) can now receive a layout specifically designed for a portrait display when in a conference that is using an Adaptive Composition layout. This is a technology preview feature and can be enabled via **Platform > Global Settings > Tech Preview Features > Enable AC Portrait**.
Teams Connector enhancements: support for calling Microsoft Teams Room devices, blue-green deployments, private routing*, and certificate-based authentication for the CVI application	Pexip's Cloud Video Interop (CVI) integration with Microsoft Teams has been enhanced: • Users who have Microsoft Teams Room devices with Pro licensing can now make and receive 1:1 (also referred to as point-to-point) SIP/H.323 video calls with VTCs, and call into Pexip Infinity VMRs. • You can now enable private routing between your Pexip Infinity platform and your Teams Connector deployment. This enables traffic to go over a private/internal network instead of the public internet. • Changes to the installation process and upgrade scripts are: ○ There are some new variables in the variables script, and new parameters to **create_vmss_deployment.ps1** in the installation and redeploy scripts to support Microsoft Teams Rooms SIP/H.323 calling, private routing and certificate-based authentication for the CVI app ID. ○ From version 33 you can use certificate-based authentication (CBA) to authenticate the Teams Connector CVI application towards MS Graph. In version 33, CBA is optional and the previous password-based authentication method is still the default mechanism. ℹ The CBA method will be the default and recommended mechanism in version 34. Password-based authentication will still be supported in version 34 but we plan to deprecate it in a future release, thus we recommend migrating to CBA as soon as practicable. Note that when upgrading to version 33 you can continue to use your existing Teams Connector API app that you have previously deployed. • VTCs now see a splash screen if a Teams client starts PowerPoint Live sharing, or uses any other non-supported content share sources. • Other administrative changes are: ○ Call capacity has been restored to 15 calls per Teams Connector. ○ Firewall changes to support calls between Microsoft Teams Rooms and VTC endpoints: ■ You need to open port 4277/TCP on your Conferencing Nodes to receive signaling from your Teams Connector instances. ■ Signaling is now sent from Microsoft Teams to port 10101/TCP on the Teams Connector's Azure load balancer. ○ The app password is now stored in the Azure Key Vault (instead of the Automation account). ○ Improvements in the Administrator interface (**Status > Live View**): ■ The private IP address of a Teams Connector instance is now shown when viewing its status in **Live View**. ■ Any overly long meeting names are now truncated when displayed in **Live View**. ○ The Teams-like layout and Microsoft's Large Gallery view are now fully supported features. ○ The Teams Tenant ID is now provided in the call information (as **teams_tenant_id**) that is available to local and external policy. Note that version 33 of the Teams Connector contains updates that necessitate an upgrade to your Pexip platform to ensure compatibility with the latest updates to the Microsoft Teams APIs and to the Teams Connector's latest features. We strongly recommend that you upgrade your Pexip deployment — both the Pexip Infinity platform and the Pexip Teams Connector — to version 33 as soon as practicable.
ESXi 8.0 support	The Pexip Infinity platform now supports VMware vSphere ESXi 6.5, 6.7, 7.0 and 8.0.

Feature	Description
Breakout rooms *	Breakout rooms are now supported on VMRs. This lets you configure individual VMRs so that its participants can be moved into segregated breakout rooms. This is a technology preview feature and can be enabled via **Platform > Global Settings > Tech Preview Features > Enable Breakout Rooms**.
Improved One-Touch Join endpoint compatibility for Microsoft Teams SIP Guest Join	The ***Microsoft Teams SIP Guest Join*** meeting type option for One-Touch Join has been updated to provide increased endpoint compatibility with Poly devices and for Cisco Unified Communications Manager (CUCM) integrations.
New custom jinja filters	This release includes two new custom jinja filters: • **pex_url_decode**: this can be used to decode previously URL-encoded links. For example, it can be used with OTJ custom rules to simplify the regular expressions required. • **pex_urldefense_decode**: this can be used to decode strings that have been encoded by Proofpoint's URL Defense. ⓘ Note also the change in functionality whereby One-Touch Join now automatically decodes these strings.
Denoising*	Denoising is a server-side feature that removes the background noise from somebody who is speaking. (In comparison, Softmute softens the gain from a noisy, but non-speaking participant.) This is a technology preview feature and can be enabled via **Platform > Global Settings > Tech Preview Features > Enable Denoise** and can then be individually enabled or disabled at the VMR level.
OTJ meeting type icons	One-Touch Join endpoints now include an icon representing the meeting type (for Microsoft Teams, Google Meet, Webex and Zoom meetings) when displaying meeting information. This is automatically available on Cisco endpoints capable of supporting this feature.
New theme content to support the latest features	A new **no_powerpoint_live.jpg** file has been added to version 2 themes to support the new PowerPoint Live related splash screen used in the Microsoft Teams interop calls. Note that this is a static jpg image i.e. you can only customize it by supplying your own replacement jpg image.
Per-location syslog servers	You can now select, per system location, the syslog servers to be used by the Conferencing Nodes in that location. On upgrade to v33, all existing syslog servers will be assigned to all existing locations. Any subsequently created locations must have their associated syslog servers assigned manually.
Administrative improvements	This release contains the following administrative improvements: • A "Google Meet Gateway Token expiring" alarm is raised when the Google Meet gateway token is due to expire within the next 30 days. • When configuring event sinks there is a new advanced tuning setting — **Time between metrics updates** — that specifies the time between event sink metrics updates. • There is a new **User Group** configuration page in the Administrator interface at **https://<manageraddress>/admin/platform/usergroup/** which is used in conjunction with version 3 of the VMR portal to map users to Pexip Infinity resources.
* Technology preview only	

Changes in functionality

This topic covers the Pexip Infinity platform; for changes in the latest release of the Connect web app see the web app release notes.

Changes in this release

Feature	Description
Pexip Smart Scale	Pexip Smart Scale has been removed from Pexip Infinity.
Management API schema	The Management API schema has moved from **/api/admin/schema/** to **/admin/platform/schema/**.
Management API rate limiting	The rate limit of requests to the management API has been reduced from 10,000 requests every 60 seconds to 1000 requests every 60 seconds.
Removed support for Xen	Support for Xen hypervisors has been removed.
OTJ: Automatic URL Defense decoding	One-Touch Join now automatically decodes any URLs within a meeting invitation that have been encoded by Proofpoint's URL Defense, thus improving the ability of the default meeting processing rules to extract the correct meeting alias. ℹ See also New custom jinja filters.
Resource usage for voice activity features	Voice Focus and Softmute now use the equivalent of an extra 6 audio connections per participant (previously an extra 4).

Planned changes in future releases

Feature	Description	More information
Remove support for ESXi 6.5	Support for ESXi 6.5 will be removed in a future release. When this occurs, Pexip will support VMware installation on ESXi 6.7, 7.0 and 8.0.	
Deprecation of password-based authentication for the Teams Connector CVI application	From version 33 you can use certificate-based authentication (CBA) to authenticate the Teams Connector CVI application towards MS Graph. In version 33, CBA is optional and the previous password-based authentication method is still the default mechanism. ℹ The CBA method will be the default and recommended mechanism in version 34. Password-based authentication will still be supported in version 34 but we plan to deprecate it in a future release, thus we recommend migrating to CBA as soon as practicable.	

Issues fixed in version 33

Version 33.1

Pexip Infinity

Ref #	Resolution
35658	Resolved an issue where a streaming participant's overlay text was lost after a custom layout was applied using the `transform_layout` API command.
35274	Resolved an issue where a conference may be abruptly terminated when an RTMP stream fails to connect.
32902	Attempting to upload a new TLS certificate for which there is more than one trusted chain no longer results in an "Internal server error" message.
34035	Resolved an issue where the transmit resolution from Pexip Infinity may drop at the start of a call.
32539	Resolved an issue that caused calls on the Conferencing Node to disconnect when an RTMP Guest participant was muted.

Connect web apps

Webapp3

Ref #	Resolution
4425	Changing a camera during a call no longer results in a lower video resolution being sent.
35323 GL4339	When the browser language on Safari (on iOS) or Chrome (on Mac and Android) is set to Traditional Chinese, the web app is now correctly displayed in that language (instead of Simplified Chinese).
35226 GL4325	Resolved an issue where the `disconnectDestination` link only took effect when the disconnect was user-initiated.
34842 GL4276	Resolved an issue with Webapp3 on iOS if a `disconnectDestination` had been set, whereby the participant would continue to send frozen video after disconnecting.

Webapp2

There were no significant user-facing fixes in this release.

Version 33

Pexip Infinity

Ref #	Resolution
35118	Resolves a minor issue whereby a gateway participant may be disconnected when using Teams-like layout.
34064	When a third participant attempts to join a VMR that is enabled for direct media and has a participant limit of 2, their call will now be rejected (previously one of the existing participants was disconnected).

One-Touch Join

Ref #	Resolution
23468	Resolved an issue where the default "Microsoft Teams Meeting Body for BlueJeans" rule failed to match some invitations.

Google Meet interoperability

Ref #	Resolution
34419	When Live Streaming has been enabled, the main video stream is no longer included in a picture-in-picture within the presentation stream sent to the Google Meet client.

Connect web apps

Webapp3

Ref #	Resolution
34979	Webapp3 clients are now able to send TURN messages to Transcoding Conferencing Nodes and Proxying Edge Nodes on port 443 when the media relay feature is enabled on Pexip Infinity (**Platform > Global Settings > Connectivity > Enable Media Relay On TCP Port 443**).
34707 GL4246	When a participant who is muted is presenting content that includes audio, the presentation audio is no longer also muted.
GL4202	When a layout change is applied to a Virtual Auditorium, the change is now applied to Guests as well as to Hosts.
34311 GL4192	Guest participants who join a meeting using a Guest PIN are no longer offered the PIN entry keypad while waiting for a Host to join.
GL4068	When a Host mutes or unmutes themselves via the participant panel, their mute state is now synchronized locally and on Pexip Infinity.
GL4015	Users who are denied access to a meeting due to SSO authentication issues are no longer shown an error. Instead, they are returned to the post-meeting page and shown a "SSO Authentication Failed" message.
GL3991	Resolved an issue whereby a camera or microphone's mute state could become unsynchronized following a change in device while in a meeting.
GL3987	Improvements to translations.
33189 GL3928	When an end-to-end encrypted call is between two Webapp3 clients, the secure check codes now match.
GL3908	When a chat message from a Skype for Business client is shown, the sender's display name is used rather than the name "User".
GL3847	Resolved an issue whereby when **muteCamera** or **muteMicrophone** were included in a preconfigured URL, the device joined muted even if the value was set to **=false**.
GL3806	Resolved an issue when shouldMaskConference was enabled, whereby meeting names were not encoded if they included the **@** symbol.
GL3698	When a user unplugs their camera or microphone during a meeting, their mute state is now synchronized with Pexip Infinity.
GL3655	Usability improvements to allow Guest participants who accidentally elect to join as a Host to easily revert to joining as a Guest.
GL3178	Improvements to the usability of the PIN entry screen when an incorrect PIN has previously been entered.

Webapp2

There were no significant user-facing fixes in this release.

Known limitations

Pexip Infinity

Ref #	Limitation
35248	The **available_layouts** REST API returns all custom layouts on the system, instead of just those in the theme for the given conference. Transforming to a custom layout not in the current theme causes the transform to fail and the 1:0 layout is displayed instead.
30756	Under certain circumstances, when a Conferencing Node is handling WebRTC calls that include presentation, the observed media load may exceed 100%.
27534	A Connect app that is paired to another video device (such as a SIP endpoint) cannot be used to connect to a Media Playback Service.
24424	Only 3 of the assigned DNS servers will be used by the Management Node or by a Conferencing Node (as configured in its associated system location).
19176	Changing the IP address of the Management Node and then manually rebooting before completing the installation wizard may result in failed connectivity to Conferencing Nodes. To work around this, you must ensure that you re-run and fully complete the installation wizard after changing the Management Node configuration.
16232	The Call-id is not logged on an administrative event when a Guest joins a conference and all Guests are muted.
16119	"License limit reached" alarms are not lowered as expected, even though an appropriate "Alarm lowered" message is logged.
15943	"Connectivity lost between nodes" alarms are not recorded in the alarm history (**History & Logs > Alarm History**).
13305	The G.719 codec is not currently supported for SIP.
12218	In some call scenarios that take a long time for the call setup to complete (for example calls that involve ICE, a Conferencing Node behind static NAT, and where the client is also behind a NAT) any audio prompts (such as requests to enter a PIN) may be played too early and the client may not hear all of the message.
7906	If a caller dials into a Virtual Reception and enters the number of the conference they want to join, but there are insufficient hardware resources available to join the caller to that conference, the caller is disconnected from the Virtual Reception.
6739	Any changes made to VMR configuration — such as updating the participant limit — while the conference is ongoing do not take immediate effect, and may result in conference separation (i.e. new participants will join a separate VMR from those that are currently connected). All participants must disconnect from the conference for the change to take effect.
5601	When changing the certificates in a chain, a reboot of the associated Conferencing Nodes may be required if the changes do not produce the desired effect.

Pexip Teams Connector

Ref #	Limitation
35285	Participants connected via Azure Communication Services (ACS) will not see video from participants joining via CVI as "trusted". We are working with Microsoft to address the issue that these participants are filtered out. A temporary workaround is to configure your system so that CVI participants connect as normal/untrusted guests, and ensure that someone admits them from the lobby. Please contact your Pexip authorized support representative for assistance and refer to issue #35285.
27854	In a large Teams meeting you may see a discrepancy in the participant count on Pexip versus that which is reported on the Teams side. We are working with Microsoft to resolve this.

Cisco

Ref #	Limitation
4142	If the presentation channel already active from an MXP is taken by another connected participant, the MXP may not properly receive presentation content.

Poly/Polycom

Ref #	Limitation
13541	When a Polycom Trio is registered to Skype for Business, and has dialed in to Pexip Infinity, it will receive presentation as main video from Pexip Infinity. However, when the same endpoint is dialed out to from Pexip Infinity, it will receive presentation as RDP.

Microsoft

Microsoft Skype for Business and Lync

Ref #	Limitation
17210	RDP presentation content from a Skype for Business meeting may sometimes take several seconds to render on VTC devices that are gatewayed into that meeting. One workaround is to use Video-based Screen Sharing (VbSS) instead of RDP for content sharing. If you must use RDP then you can configure your system to adjust the bandwidth used for RDP presentation which will reduce the delay in rendering the RDP content for the VTC device — contact your Pexip authorized support representative for configuration details.
13201	When a Skype for Business client is presenting PowerPoint slides in a Skype for Business meeting, sometimes only the first slide is sent to standards-based endpoints that are gatewayed into that meeting.
5100	If a Conferencing Node being used as a gateway into a SfB/Lync meeting is near processor capacity and another endpoint in the SfB/Lync meeting starts sending content, a participant may be inadvertently disconnected from the conference. To resolve this, the endpoint can dial back into the conference.
4926	Participants calling into Skype for Business / Lync through the Infinity Gateway may experience inconsistent call rejection messages if a Conferencing Node is placed into maintenance mode.
4812	In some instances, one of two messages sent to a VMR from two SfB/Lync clients not previously connected may not be properly retained by the VMR. To resolve, re-send the message.
4195	Participants connected via the Infinity Gateway into a SfB/Lync meeting may not receive presentation content from SfB/Lync participants. This occurs if the SfB/Lync user has a screen resolution where the width is an odd number of pixels, such as a resolution of 1437x758. If this occurs, one workaround is for the user to share an application rather than their full desktop.

VMR Scheduling for Exchange

Ref #	Limitation
19530	When using Microsoft's OWA with Office 365 account, join instructions that use the **<style>** element will not be added, even though the "Success" message is displayed to the user.
16602	In some circumstances, users are not able to obtain a VMR for a meeting if an existing meeting invitation is being edited and has previously had a VMR assigned. This may happen if a user has previously activated the add-in when editing an invitation but then discarded their changes, or if the user has removed the information added to the invitation when the add-in was previously activated. By default, users will see a message "VMR already assigned".