XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

What’s new

February 1, 2019

The Long Term Service Release (LTSR) program for XenApp and XenDesktop 7.6 provides stability and long-term support for the XenApp/XenDesktop 7.6 release.

The latest update to LTSR is Cumulative Update 7 (CU7). Citrix recommends that you update the LTSR components of your deployment to CU7.

If you are new to the LTSR program and did not deploy the original XenApp/XenDesktop 7.6 LTSR release, there is no need for you to install it now. Instead, Citrix recommends that you bypass the 7.6 LTSR release and begin right with CU7. Documentation of the entire 7.6 LTSR release is available here.

In addition, Citrix also recommends specific versions of Citrix Receiver and other components. While not required for LTSR compliance, upgrading to the current versions of those components ensures further ease of maintenance and the availability of the latest fixes in your deployment.

Downloads

7.6 LTSR CU7 (XenApp)
7.6 LTSR CU7 (XenDesktop)

Documentation

7.6 LTSR Cumulative Update 7
7.6 LTSR Cumulative Update 6
7.6 LTSR Cumulative Update 5
7.6 LTSR Cumulative Update 4
7.6 LTSR Cumulative Update 3
7.6 LTSR Cumulative Update 2
7.6 LTSR Cumulative Update 1
7.6 LTSR

Helpful links

- Citrix Supportability Pack
  The Supportability Pack is a collection of popular tools written by Citrix engineers to help diagnose
and troubleshoot XenDesktop/XenApp products. The tools are cataloged by features and components to make it easier to find and use. Early versions of the Pack serves as a launch pad for efforts …

- Citrix L T S R Assistant
  L T S R Assistant scans components of XenApp and XenDesktop 7.6 to determine if they are Long Term Service Release (L T S R) compliant. The components to be scanned can reside on virtual or …

- L T S R Frequently Asked Questions (FAQs)
  Citrix Windows App Delivery team has been releasing innovations and feature enhancements for the XenApp and XenDesktop product lines at a rapid pace, with the 2015 year bringing about new product releases on a quarterly basis. This rapid pace of innovation enhances the use cases for XenApp and …

- XenApp and XenDesktop servicing options
  Flexible service options enable predictable support. Citrix delivers new features and functionality for XenApp and XenDesktop frequently to keep your business competitive, streamline IT operations, enhance data security, and ensure your employees have access to their business resources from anywhere. …

- Product Lifecycle dates
  Refer to this table for product lifecycle dates. The Product Matrix table below provides information for Citrix products whose product lifecycle is governed by lifecycle phases. Product lifecycle milestones include Notice of Status Change (NSC), End of Sales (EOS), End of Maintenance (EOM) and End of Life (EOL). …

- L T S R Program for Receiver for Windows
  For each major version (e.g., v3.0) of a Citrix Receiver for Windows, Mac, Linux, HTML5, Java, or WinCE, customers will receive a minimum lifecycle of four years. The lifecycle consists of a Mainstream Maintenance Phase for at least the first three years followed by an Extended Maintenance Phase for …

**Cumulative Update 7 (CU 7)**

February 19, 2019

Release date: February 2019

Cumulative Update 7 (CU 7) is the latest Cumulative Update to the XenApp and XenDesktop 7.6 Long Term Service Release (L T S R). It provides updates to five baseline components of the original 7.6 L T S R.

**Issues fixed since XenApp and XenDesktop 7.6 L T S R CU 6**

**Known issues in this release**
Downloads

Download LTSR CU7 (XenApp)
Download LTSR CU7 (XenDesktop)

New deployments

How do I deploy CU7 from scratch?

You can set up a brand-new XenApp or XenDesktop environment based on CU7 - using the CU7 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the XenApp and XenDesktop 7.6 Long Term Service Release documentation and pay close attention to the Technical Overview, New Deployments, and Security sections before you start planning your deployment. Make sure your setup meets the system requirements for all components. Follow New Deployments for deployment instructions.

Note:
Provisioning Services and Session Recording are available as separate downloads and installers.

Existing deployments

What do I update?

CU7 provides updates to five baseline components of 7.6 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU7. For example: If Provisioning Services is part of your LTSR deployment, update the Provisioning Services components to CU7. If Provisioning Services is not part of your deployment, you do not need to install or update it.

Since the 7.6 LTSR release, we have added a metainstaller that lets you update the existing components of your LTSR environment from a unified interface. Following the Upgrade instructions, use the metainstaller to update the LTSR components of your deployment.

Note:
The following information is specific to the CU7 release. For the equivalent information for the LTSR base release, CU1, CU2, CU3, CU4, CU5, or CU6, see the respective documentation.
### LTSR Baseline Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDA for Desktop OS</td>
<td>7.6.7000</td>
<td>Special rules apply for Windows 10. See <a href="#">CU7 compatible components and platforms</a>.</td>
</tr>
<tr>
<td>VDA for Server OS</td>
<td>7.6.7000</td>
<td></td>
</tr>
<tr>
<td>Delivery Controller</td>
<td>7.6.7000</td>
<td></td>
</tr>
<tr>
<td>Citrix Studio</td>
<td>7.6.7000</td>
<td></td>
</tr>
<tr>
<td>Citrix Director</td>
<td>7.6.7000</td>
<td></td>
</tr>
<tr>
<td>Group Policy Management Experience</td>
<td>2.5.7000</td>
<td></td>
</tr>
<tr>
<td>Session Recording</td>
<td>7.6.7000</td>
<td>Platinum Edition only</td>
</tr>
<tr>
<td>StoreFront</td>
<td>3.0.7000.1</td>
<td></td>
</tr>
<tr>
<td>StoreFront Service</td>
<td>7.6.7000</td>
<td></td>
</tr>
<tr>
<td>Provisioning Services</td>
<td>7.6.8</td>
<td>Special rules apply for Windows 10. See <a href="#">CU7 compatible components and platforms</a>.</td>
</tr>
<tr>
<td>Universal Print Server</td>
<td>7.6.7000</td>
<td>Only Windows 2008 R2 SP1, Windows 2012, Windows 2012 R2 supported</td>
</tr>
</tbody>
</table>

**LTSR CU7 compatible components**

The following components - at the versions given below - are compatible with LTSR environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 7.6 LTSR environments.

**Note about Windows 10:**

Windows 10 does not get the full set of 7.6 LTSR benefits. For deployments that include Windows 10 machines, Citrix recommends that you use the latest 7.15 LTSR version of the VDA for Desktop OS and of Provisioning Services.

For more information, see [Adding Windows 10 Compatibility to XenApp and XenDesktop 7.6 LTSR](#) and the [XenApp and XenDesktop Servicing Options (LTSR) FAQ](#).
<table>
<thead>
<tr>
<th>LTSR CU7 Compatible Components and Platforms</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Management</td>
<td>7.15.3000</td>
</tr>
<tr>
<td>AppDNA</td>
<td>7.14</td>
</tr>
<tr>
<td>License Server</td>
<td>11.15.0.0 Build 26000</td>
</tr>
<tr>
<td>HDX RealTime Optimization Pack</td>
<td>2.4.2000</td>
</tr>
<tr>
<td>Windows 10</td>
<td>VDA and Provisioning Services: Latest 7.15 LTSR CU</td>
</tr>
</tbody>
</table>

LTSR supports the following versions of Citrix Workspace app and all later versions:

<table>
<thead>
<tr>
<th>LTSR compatible versions of Citrix Workspace app</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Workspace app for Android</td>
<td>1902</td>
</tr>
<tr>
<td>Citrix Workspace app for Chrome</td>
<td>1901</td>
</tr>
<tr>
<td>Citrix Workspace app for HTML5</td>
<td>1901</td>
</tr>
<tr>
<td>Citrix Workspace app for iOS</td>
<td>1901</td>
</tr>
<tr>
<td>Citrix Workspace app for Mac</td>
<td>1901</td>
</tr>
<tr>
<td>Citrix Workspace app for Linux</td>
<td>1810</td>
</tr>
<tr>
<td>Citrix Workspace app for Windows</td>
<td>1812</td>
</tr>
<tr>
<td>Citrix Workspace app for Windows (Store)</td>
<td>1812</td>
</tr>
</tbody>
</table>

LTSR also supports the following versions of Citrix Receiver and all later versions:

<table>
<thead>
<tr>
<th>LTSR compatible versions of Citrix Receiver</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Receiver for Chrome</td>
<td>2.6.9</td>
</tr>
<tr>
<td>Citrix Receiver for HTML5</td>
<td>2.6.9</td>
</tr>
<tr>
<td>Citrix Receiver for Mac</td>
<td>12.9.1</td>
</tr>
<tr>
<td>Citrix Receiver for Linux</td>
<td>13.10</td>
</tr>
<tr>
<td>Citrix Receiver for Windows</td>
<td>4.9.5000</td>
</tr>
</tbody>
</table>
**LTSR notable exclusions**

The following features, components, and platforms are not eligible for LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components will be available through regular current releases.

<table>
<thead>
<tr>
<th>Excluded Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local App Access</td>
</tr>
<tr>
<td>Framehawk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Excluded Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux VDA</td>
</tr>
<tr>
<td>Personal vDisk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Excluded Windows Platforms *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2008 32-bit (for Universal Print Server)</td>
</tr>
</tbody>
</table>

*Citrix reserves the right to update platform support based on third party vendors’ lifecycle milestones.

**Install and upgrade analytics**

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers’ installation experiences. For more information, see [http://more.citrix.com/XD-INSTALLER](http://more.citrix.com/XD-INSTALLER).

**XenApp 6.5 migration**

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a Site running XenApp 7.6 (or a later supported release). This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp Site.

After you install the XenApp 7.6 core components and create a Site, the migration process follows this sequence:
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

- Run the XenApp 7.6 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Windows Server OS for use in the new Site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.
- Edit the XML files, if desired, to refine what you want to import to the new Site. By tailoring the files, you can import policy and application settings into your XenApp 7.6 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.6 Controller, which import settings from the XML files to the new XenApp Site.
- Reconfigure the new Site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

February 1, 2019

XenApp/XenDesktop 7.6 LTSR Cumulative Update 7 contains all fixes that were included in XenApp and XenDesktop 7.6 LTSR, Cumulative Update 1, Cumulative Update 2, Cumulative Update 3, Cumulative Update 4, Cumulative Update 5, Cumulative Update 6, plus the following, new fixes:

Controller 7.6.7000

- After you choose a month for the Trends view graph duration, only seven days of historical data is shown. [LC9908]

Provisioning Services 7.6.8

Console Issues

- The Provisioning Services XIP library for VMware ESXi does not support TLS v1.2. [LC9629]

Server Issues

- When an additional virtual hard disk (VHD) footer is assigned to a merged VHD, the file size of the merged base might increase. [LC9837]
**StoreFront 3.0.7000.1**

- When using the Safari 12 and later browsers, client detection might fail on Citrix Receiver for Web because the Netscape Plugin Application Programming Interface (NPAPI) support was removed. For more information, see the Knowledge Center article CTX238286. [LD0863]

**VDA for Desktop OS 7.6.7000**

**Keyboard**

- When you use the Chinese keyboard layout in a user session, the Input Method Editor (IME) automatically changes to the Wubi Chinese character input method. The issue occurs when the default IME is not set to Wubi. [LD0429]

**Session/Connection**

- When processing a credit card transactions through a user device, the application and the user device can become unresponsive, or only a subset of data might be received. [LD0152]

- Attempts to start an application from a random server might fail. This error message appears:

  **Unable to launch your application. Cannot connect to the Citrix XenApp Server. The Citrix SSL Server you selected is not accepting connections.**

  The issue occurs when the server stops accepting connections on an SSL-enabled VDA. [LD0239]

- When anonymous users access a member of a Citrix Delivery Group, an incorrect logon interface might appear with the message **Connection Restored** after the Common Gateway Protocol (CGP) times out. The correct message reads, **Could Not Reconnect**. [LD0363]

- This fix addresses a memory leak issue that occurs when the **Auto connect client drives** policy is disabled. [LD0370]

**System Exceptions**

- VDAs might experience a fatal exception on wdica.sys and display a blue screen with bug check code 0x3b (SYSTEM_SERVICE_EXCEPTION). [LD0089]

- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x22. [LD0119]
User Interface

- Attempts to copy and paste the HTML formatted content to or from a session might fail in a published instance of Internet Explorer. [LD0395]

VDA for Server OS 7.6.7000

Keyboard

- When you use the Chinese keyboard layout in a user session, the Input Method Editor (IME) automatically changes to the Wubi Chinese character input method. The issue occurs when the default IME is not set to Wubi. [LD0429]

Session/Connection

- When processing a credit card transaction through a user device, the application and the user device can become unresponsive, or only a subset of data might be received. [LD0152]
- Attempts to start an application from a random server might fail. This error message appears: Unable to launch your application. Cannot connect to the Citrix XenApp Server. The Citrix SSL Server you selected is not accepting connections.
  The issue occurs when the server stops accepting connections on an SSL-enabled VDA. [LD0239]
- When anonymous users access a member of a Citrix Delivery Group, an incorrect logon interface might appear with the message Connection Restored after the Common Gateway Protocol (CGP) times out. The correct message reads, Could Not Reconnect. [LD0363]
- This fix addresses a memory leak issue that occurs when the Auto connect client drives policy is disabled. [LD0370]

System Exceptions

- VDAs might experience a fatal exception on wdica.sys and display a blue screen with bug check code 0x3b (SYSTEM_SERVICE_EXCEPTION). [LD0089]
- VDAs might experience a fatal exception on picadm.sys and display a blue screen with bug check code 0x22. [LD0119]
User Interface

- Attempts to copy and paste the HTML formatted content to or from a session might fail in a published instance of Internet Explorer. [LD0395]

Cumulative Update 6 (CU 6)

February 13, 2019

Release date: August 2018

Cumulative Update 6 (CU6) is the latest Cumulative Update to the XenApp and XenDesktop 7.6 Long Term Service Release (LTSR). It provides updates to seven baseline components of the original 7.6 LTSR.

Issues fixed since XenApp and XenDesktop 7.6 LTSR CU5

Known issues in this release

Downloads

Download LTSR CU6 (XenApp)

Download LTSR CU6 (XenDesktop)

New deployments

How do I deploy CU6 from scratch?

You can set up a brand-new XenApp or XenDesktop environment based on CU6 - using the CU6 metainstaller. Before you do that, we recommend that you familiarize yourself with the product:

Peruse the XenApp and XenDesktop 7.6 Long Term Service Release documentation and pay close attention to the Technical Overview, New Deployments, and Security sections before you start planning your deployment. Make sure your setup meets the system requirements for all components. Follow New Deployments for deployment instructions.

Note:

Provisioning Services and Session Recording are available as separate downloads and installers.
Existing deployments

What do I update?

CU6 provides updates to seven baseline components of 7.6 LTSR. Remember: Citrix recommends that you update all LTSR components of your deployment to CU6. For example: If Provisioning Services is part of your LTSR deployment, update the Provisioning Services component to CU6. If Provisioning Services is not part of your deployment, you do not need to install or update it.

Since the 7.6 LTSR release, we have added a metainstaller that lets you update the existing components of your LTSR environment from a unified interface. Following the Upgrade instructions, use the metainstaller to update the LTSR components of your deployment.

Note

The following information is specific to the CU6 release. For the equivalent information for the LTSR base release, CU1, CU2, CU3, CU4, or CU5, see the respective documentation.

<table>
<thead>
<tr>
<th>LTSR Baseline Components</th>
<th>Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDA for Desktop OS</td>
<td>7.6.6000</td>
<td>Special rules apply for Windows 10. See CU6 compatible components and platforms</td>
</tr>
<tr>
<td>VDA for Server OS</td>
<td>7.6.6000</td>
<td></td>
</tr>
<tr>
<td>Delivery Controller</td>
<td>7.6.6000</td>
<td></td>
</tr>
<tr>
<td>Citrix Studio</td>
<td>7.6.6000</td>
<td></td>
</tr>
<tr>
<td>Citrix Director</td>
<td>7.6.6000</td>
<td></td>
</tr>
<tr>
<td>Group Policy Management Experience</td>
<td>2.5.6000</td>
<td></td>
</tr>
<tr>
<td>StoreFront</td>
<td>3.0.6000.1</td>
<td></td>
</tr>
<tr>
<td>Provisioning Services</td>
<td>7.6.7</td>
<td>Special rules apply for Windows 10. See CU6 compatible components and platforms</td>
</tr>
<tr>
<td>Universal Print Server</td>
<td>7.6.6000</td>
<td>Only Windows 2008 R2 SP1, Windows 2012, Windows 2012 R2 supported</td>
</tr>
<tr>
<td>Session Recording</td>
<td>7.6.6000</td>
<td>Platinum Edition only</td>
</tr>
</tbody>
</table>
LTSR CU6 compatible components

The following components - at the versions given below - are recommended for use in 7.6 LTSR CU6 environments. They are not eligible for the LTSR benefits (extended lifecycle and fix-only cumulative updates). Citrix might ask you to upgrade to a newer version of these components within your 7.6 LTSR environments.

Note about Windows 10:

Windows 10 does not get the full set of 7.6 LTSR benefits. For deployments that include Windows 10 machines, Citrix recommends that you use the latest 7.15 LTSR version of the VDA for Desktop OS and of Provisioning Services.

For more information, see Adding Windows 10 Compatibility to XenApp and XenDesktop 7.6 LTSR and the XenApp and XenDesktop Servicing Options (LTSR) FAQ.

<table>
<thead>
<tr>
<th>Profile Management</th>
<th>7.15.2001</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppDNA</td>
<td>7.14</td>
</tr>
<tr>
<td>License Server</td>
<td>11.15.0.0 Build 24100</td>
</tr>
<tr>
<td>HDX RealTime Optimization Pack</td>
<td>2.4.1000</td>
</tr>
<tr>
<td>Windows 10</td>
<td>VDA and Provisioning Services: Latest 7.15 LTSR CU</td>
</tr>
</tbody>
</table>

LTSR supports the following versions of Citrix Workspace app and all later versions:

<table>
<thead>
<tr>
<th>LTSR compatible versions of Citrix Workspace app</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Workspace app for Android</td>
<td>1808</td>
</tr>
<tr>
<td>Citrix Workspace app for Chrome</td>
<td>1808</td>
</tr>
<tr>
<td>Citrix Workspace app for HTML5</td>
<td>1808</td>
</tr>
<tr>
<td>Citrix Workspace app for iOS</td>
<td>1808</td>
</tr>
<tr>
<td>Citrix Workspace app for Mac</td>
<td>1808</td>
</tr>
<tr>
<td>Citrix Workspace app for Linux</td>
<td>1808</td>
</tr>
<tr>
<td>Citrix Workspace app for Windows</td>
<td>1808</td>
</tr>
</tbody>
</table>
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

LTSR also supports the following versions of Citrix Receiver and all later versions:

<table>
<thead>
<tr>
<th>LTSR compatible versions of Citrix Receiver</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Receiver for Android</td>
<td>3.13.2</td>
</tr>
<tr>
<td>Citrix Receiver for Chrome</td>
<td>2.6.9</td>
</tr>
<tr>
<td>Citrix Receiver for HTML5</td>
<td>2.6.9</td>
</tr>
<tr>
<td>Citrix Receiver for iOS</td>
<td>7.5.6</td>
</tr>
<tr>
<td>Citrix Receiver for Mac</td>
<td>12.9.1</td>
</tr>
<tr>
<td>Citrix Receiver for Linux</td>
<td>13.10</td>
</tr>
<tr>
<td>Citrix Receiver for Universal Windows Platform</td>
<td>1.0.5</td>
</tr>
<tr>
<td>Citrix Receiver for Windows</td>
<td>4.9.3000</td>
</tr>
</tbody>
</table>

**LTSR notable exclusions**

The following features, components, and platforms are not eligible for LTSR lifecycle milestones and benefits. Specifically, cumulative updates and extended lifecycle benefits are excluded. Updates to excluded features and components will be available through regular current releases.

- **Excluded Features**
  - Local App Access
  - Framehawk

- **Excluded Components**
  - Linux VDA
  - Personal vDisk

- **Excluded Windows Platforms**
  - Windows 2008 32-bit (for Universal Print Server)

*Citrix reserves the right to update platform support based on third party vendors’ lifecycle milestones.*
Install and upgrade analytics

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences. For more information, see http://more.citrix.com/XD-INSTALLER.

XenApp 6.5 migration

The XenApp 6.5 migration process helps you more efficiently and quickly transition from a XenApp 6.5 farm to a Site running XenApp 7.6 (or a later supported release). This is helpful in deployments that contain large numbers of applications and Citrix group policies, lowering the risk of inadvertently introducing errors when manually moving applications and Citrix group policies to the new XenApp Site.

After you install the XenApp 7.6 core components and create a Site, the migration process follows this sequence:

- Run the XenApp 7.6 installer on each XenApp 6.5 worker, which automatically upgrades it to a new Virtual Delivery Agent for Windows Server OS for use in the new Site.
- Run PowerShell export cmdlets on a XenApp 6.5 controller, which exports application and Citrix policy settings to XML files.
- Edit the XML files, if desired, to refine what you want to import to the new Site. By tailoring the files, you can import policy and application settings into your XenApp 7.6 Site in stages: some now and others later.
- Run PowerShell import cmdlets on the new XenApp 7.6 Controller, which import settings from the XML files to the new XenApp Site.
- Reconfigure the new Site as needed, and then test it.

For more information, see Migrate XenApp 6.x.

Fixed issues

February 15, 2019

Warning:

Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

XenApp/XenDesktop 7.6 LTSR Cumulative Update 2 contains all fixes that were included in XenApp and XenDesktop 7.6 LTSR and Cumulative Update 1, plus the following, new fixes:

**Citrix Director**

- When a user session is viewed in the HDX panel of Citrix Director, a priority warning might incorrectly appear for the audio virtual channel.
  
  [#LC5564]

**Citrix Policy**

- The w3wp.exe process can consume 100% of the CPU.
  
  [#LC4355]

- Citrix Studio might allow policy filter editing for read-only administrators.
  
  [#LC4801]

- Citrix group policies stored in Active Directory are removed from the machine on the next GPO refresh or when you run GPUpdate /Force. This issue occurs on VDA versions 7.6.300 and later.
  
  [#LC5204]

- The following error message appears when opening the Citrix Studio and selecting the policy node:

  “Changes made to policies outside of this console, such as in PowerShell or management tools from previous versions, resulted in a discrepancy between policies. The assigned objects of policy <policy name> must match. Object Delivery Group has assignments <assignment name> in the “user” component and <assignment name> in the “computer” component.”

  [#LC5510]

**Citrix Studio**

- Citrix Studio does not receive logging entries while in the logging node when trying to retrieve large amounts of data.
  
  [#LC5292]

- Citrix Studio might show an incorrect message or prompt for a Site upgrade when a FlexCast Management Architecture service has been stopped or is unavailable.
  
  [#LC5319]
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

Controller

- When a large number of sessions are launched in a short time, Director might take a long time to show session information.
  [#LC1617]
- When using VMware ESXi 5.x or 6.0 to create MCS machines, occasionally the machine deployments are consolidated and cloned as a thick provisioned disk.
  [#LC4655]
- When the VDA is in maintenance mode, the Get-BrokerSession cmdlet might return the maintenance mode state of the Delivery Group instead of the individual machine.
  [#LC4840]
- Citrix Studio occasionally launches with the following error message: “Could not connect to broker service.”
  [#LC4854]
- This fix addresses an issue that prevents Machine Creation Services provisioning from working in Amazon Web Services when the Controller is isolated from Amazon’s public API endpoints by way of a web proxy.
  [#LC5109]
- Citrix Studio might show an incorrect message or prompt for a Site upgrade when a FlexCast Management Architecture service has been stopped or is unavailable.
  [#LC5319]

HDX MediaStream Flash Redirection

- With HDX MediaStream Flash Redirection enabled, Microsoft Internet Explorer might close unexpectedly when it runs pseudoserverinproc2.dll.

To enable the fix, create the following registry key:

- On Windows 32-bit systems:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  Name: AllowCOMObjectTrack
  Type: DWORD
  Value: 0
On Windows 64-bit systems:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer

Name: AllowCOMObjectTrack
Type: DWORD
Value: 0

[#LC1885]

• With HDX MediaStream Windows Media Redirection enabled, certain third party players might exit unexpectedly while rendering files on a VDA that is running on Windows 10.

[#LC5110]

Licensing

• Site Setup in Citrix Studio might fail to proceed when choosing “Use an existing license.” As a workaround, restart the Citrix Web Services for Licensing service on the license server to complete its configuration.

[#630814]

Provisioning Services

Console

• When expanding Sites, the PVS console occasionally times out.

[#LC4737]

• The XenDesktop Setup wizard does not use the template boot properties when creating targets. To enable the fix, create the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ProvisioningServices

Name: UseTemplateBootOrder
Type: REG_DWORD
Data: 1

[#LC5237]
Server

• The number of target devices on the Provisioning Services Console might show less than the actual value after the database connection is lost and recovered.

[#LC4275]

• Boot Device Manager target devices fail to acquire an IP address whereas PXE target devices acquire them successfully. This happens because the DHCP Discover request sent by the Boot Device Manager set the “Seconds Elapsed” value to 0. The request is then dropped by IP Helper. The “Seconds Elapsed” value is now set to 4 to avoid this problem.

[#LC4369]

• If you change the MTU size to less than 1,500 byte, the bootstrap file fails to download and target devices fail to start using the Boot Device Manager (BDM). This enhancement allows you to lower the MTU size to less than 1,500 byte by setting the following registry key. The enhancement is disabled by default:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\PVSTSB\Parameters
Name: AllowMTUAdjust
Type: DWORD
Value: 1

[#LC4531]

• When expanding Sites, the PVS console occasionally times out.

[#LC4737]

• When attempting to import a new vDisk version of a VHDX file, the import fails and an error message appears that says the Manifest file is invalid.

[#LC4985]

• The Provisioning Server logs might show incorrect IP addresses for target devices.

[#LC5323]

• The following database access error might appear in the event viewer of the Provisioning Server:

“DBAccess error: <Couldn’t add record – same fields as an existing record>”

The issue occurs when multiple Provisioning Servers call a specific stored procedure simultaneously, causing conflicts between the calls to the stored procedure. As a result, an attempt to insert a record with the same key value twice might occur.

[#LC5364]
• Attempts to restart provisioned targets might fail intermittently because of a database timeout error. The following error message might appear:

“Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding.”

[#LC5511]

• The BNPXE Server that enables the target devices to start from the network binds to the IP address 127.0.0.1. This prevents target devices from booting. This issue can happen when BNPXE enumerates the network interfaces, but the operating system has not discovered all the interfaces yet and only returns 127.0.0.1.

[#LC5916]

• Attempts to start target devices might fail when using HP Moonshot systems.

[#LC6024]

Target Device

• When creating a personal vDisk, a “Personal vDisk cannot start” error dialog appears after the machine is booted and a formatted disk cannot be used due to an “unknown format” error.

[#LC5935]

StoreFront

• When using Windows Server 2008 R2, the Citrix StoreFront MMC might exit unexpectedly if you try to “Set Unified Experience as Default” in the Stores menu.

[#LC3614]

• This fix addresses issues with syncing changed subscription items from remote groups to local and back.

[#LC4690]

• Setting the “Session Timeout” of Citrix Receiver for Web to more than 24 days causes a Session Timeout warning to appear immediately after logon.

[#LC4787]

• The Desktop Appliance Site does not launch the assigned desktop if the store is using Resources Aggregation.

[#LC4838]
• With StoreFront 3.0.1, Workspace Control might not work when using Aggregation.
  [#LC5042]
• When using PowerShell script commands, the AllFailedBypassDuration setting is occasionally not applied.
  [#LC5500]
• If the “IncludedClientIPFilter” or “ExcludedClientIPFilter” options are enabled by the “Set-BrokerAccessPolicyRule” command, you might not be able to view resources such as shared resources, published desktops, or published applications on StoreFront.
  [#LC6058]

Universal Print Server

Client

• The NextGen application occasionally fails when trying to print to the Universal Print Server.
  [#LC4246]

Server

• The Citrix XTE Server service (XTE.exe) can exit unexpectedly.
  [#LC0759]

VDA for Desktop OS

Desktop Studio

• A logged off RDP session might appear as “Disconnected” in Citrix Studio and becomes unavailable for reconnection.
  [#LC5427]

HDX 3D Pro

• The context menu might not display correctly on the desktop when the window is maximized.
  [#LC5263]
HDX MediaStream Windows Media Redirection

• With HDX MediaStream Windows Media Redirection enabled, certain third party players might exit unexpectedly while rendering files on a VDA that is running on Windows 10.

[#LC5110]

Installing, Uninstalling, Upgrading

• Attempts to reconnect to a session from an endpoint with a different resolution can cause the VDA to exit unexpectedly and might result in a black or white window.

[#LC4606]

Keyboard

• When upgrading from Version 5.4.400 to Version 7.6.300, the ICA Service\System32 directory is missing, and keyboard/mouse inputs fail to register in Mac clients.

[#LC4681]

Printing

• When a default printer is not set, all mapped printers might fail in sessions.

[#LC4354]

• With legacy printer names enabled, autocreated printers might not be available for use in a published application when multiple sessions are established on a single server for the same user.

[#LC4517]

• The “Auto-create client printers” policy might fail to set default printers correctly in a published application and Microsoft XPS Document Writer is set as the default printer.

[#LC4696]

• Excel spreadsheets generated by SAP fail to print on printers redirected using the Universal Print Driver EMF driver.

[#LC4853]

• After a user logs off and logs back on, printers connected to the session might not be accessible.

[#LC5188]
• The Print Preview on Client option within Citrix Universal Print Driver displays to the local end point.
[#LC5404]

Session/Connection

• When resizing a reconnected session with a Citrix policy in place to prohibit session wallpaper and a Microsoft group policy in place that specified a wallpaper, the Citrix policy is not honored.
[#LC0115]

• Information remains visible on the screen after the VDA goes into screen saver or power save mode, until the user provides input (mouse or keyboard) which updates the session with a blank screen. This occurs when screen savers and the power-save option in sessions are enabled by the DWORD value HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\SetDisplayRequiredMode = 0.
[#LC1650]

• On systems with Hotfix ICAWS760WX86022 installed, attempts to reconnect to a user session might fail when you restart the Citrix ICA Service.
[#LC3714]

• With this enhancement, an entry is written to the Windows Event log when a USB device is redirected in a session.
[#LC3996]

• When you log on to a web interface that is configured for single sign-on using UPN credentials, the session window might appear for a while and then exit unexpectedly.
[#LC4035]

• Using published instances of Microsoft Internet Explorer, attempts to download a file from a website and saving it to a mapped client drive (“Save as…”) can fail.
[#LC4300]

• Audio files might fail to play in a VDA session when connected through Citrix Receiver for Mac or a Chromebook.
[#LC4596]

• After a network interruption between a VDA and Citrix Receiver, you cannot play back an .avi file on Windows Media Player.
[#LC4670]
• When switching sessions between windowed and full-screen mode with legacy graphics mode enabled, the application windows running on the VDA might not retain the maximized state.

[#LC4693]

• After upgrading a VDA from version 5.6.300, VDAs can become unresponsive.

[#LC4851]

• Time zone redirection might not work in user sessions running on iOS devices.

[#LC4869]

• After using the Remote Desktop Protocol, the ICA session might display a grey screen when re-connecting to the VM. This issue only occurs on VDAs installed with /NOCITRIXWDDM.

[#LC4970]

• A USB device might fail to work after it is redirected to Version 7.6.300 of the VDA. The issue occurs when the instance ID of the device is different from the serial number.

To enable this fix, add the Product ID or Vendor ID pairs to the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\icausbb\Parameters

Name: UsingSerialNumberDevices

Type: REG_MULTI_SZ

Value: <Note: Next to the comments string, add the vid=xxxx and pid=xxxx pairs. (The syntax for the value is an ordered list of case insensitive rules where “#” is a line comment and each rule is an ordered vid and pid pair. For example, vid=#-number and pid=#-number. The maximum hex value for a vid/pid is FFFF. If the length of a vid/pid hex value is less than 4, pair the number with zeroes (0). For example, if the vid is 12 and pid is 13; the vid/pid pair should be vid=0012, pid=0013. Each rule has a fixed length: 17, no spaces at the beginning or the end of the rule. Examples: #vid=FFFF, #pid=FFFF #vid=0012, #pid=0013.)>

[#LC5035]

• The svchost.exe process can consume 100% of the CPU.

[#LC5041]

• With Excelhook enabled and after applying hotfix ICATS760WX64028, the Excel window does not minimize when clicking the Excel icon in the taskbar.

[#LC5060]

• The svchost.exe process might fail intermittently on SCardHook64.dll when a user is logging on or off and Certificate Propagation is active.

[#LC5083]
This fix addresses an issue that breaks client-side fetching for DirectShow based applications, preventing videos from rendering.

[#LC5098]

The operating system experiences an error on picadd.sys and a blue screen appears with bugcheck code 0xd5.

[#LC5134]

An external USB DVD drive that is mapped into a session as a mapped client drive can cause slow session performance.

[#LC5231]

COM port mapping can intermittently fail.

[#LC5235]

The following counters in the performance monitor might display inconsistently.
- ICA Session\Input Session Bandwidth
- ICA Session\Output Session Bandwidth

The issue occurs only when the count value is high.

[#LC5262]

The operating system experiences an error on picadd.sys and a blue screen appears with bugcheck code 0x3b.

[#LC5299]

The VDA might become unresponsive at the “Welcome” screen due to a deadlock on picadm.sys.

[#LC5326]

Attempts to save a published Microsoft Excel spreadsheet to a Chromebook device might fail. The issue occurs because the file extension is not present.

[#LC6001]

**Smart Cards**

- The Sign-in option does not appear on Version 7.6.300 and later VDAs running on Windows 10 Build 10586 and later. As a result, smart card logons are not possible.

[#LC4778]

- When you allow your ICA session to be disconnected through an idle session timer and then log on to the Remote PC from the console, smart card logons no longer work. At times, the option to see the smart card tile is missing, or the card is not detected.
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

[#LC5187]

• XenDesktop smart card sessions might randomly disconnect.

[#LC5265]

• Attempts to log on by using certain smart cards might result in the following error message:
  “No valid certificates were found on this smart card.
  Please try another smart card or contact your administrator.”

[#LC5456]

System Exceptions

• With Adobe Shockwave plugin installed on a machine catalog that is attached to a PVD, Mi-
  crosoft Internet Explorer might exit unexpectedly in a user session.

[#LC4027]

• The operating system experiences an error on picadm.sys and a blue screen appears with
  bugcheck code 0x50.

[#LC4529]

• The operating system experiences an error on picadm.sys and a blue screen appears.

[#LC4567]

• A non-handled exception copying from USB devices might cause the operating system to expe-
  rience an error and a blue screen appears.

[#LC4782]

• A published application process might exit unexpectedly with an exception “c000041d” on Mo-
  bileDesktopHook64.dll.

[#LC4821]

• When you log on to a VDA running on Windows Server 2008 R2 through a remote desktop and
  launch certain third-party applications, the applications might exit unexpectedly.

[#LC5891]

User Experience

• When you switch from a touch-optimized published desktop to a regular published desktop, the
  Start button:
    – Does not highlight when you hover over it
Brings up the local desktop instead of the published desktop

• Certain .wmv files might not play at the correct aspect ratio.

• Customized functions for a 3Dconnexion SpaceMouse might not work in a VDA session. To enable this fix, set a REG_DWORD in the registry:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picakbf

  Name: Enable3DConnexionMouse
  Type: REG_DWORD
  Data: 1

• Connecting to audio recording/dictation software during an ICA session might cause the software to exit unexpectedly.

User Interface

• After publishing seamless applications, the generic Citrix Receiver icon may appear instead of the published app icon in the taskbar.

VDA for Server OS

HDX MediaStream Windows Media Redirection

• With HDX MediaStream Windows Media Redirection enabled, certain third party players might exit unexpectedly while rendering files on a VDA that is running on Windows 10.

Keyboard

• When upgrading from Version 5.4.400 to Version 7.6.300, the ICA Service\System32 directory is missing, and keyboard/mouse inputs fail to register in Mac clients.
• The Bloomberg keyboard is unable to be mapped within the VDA session even though it is al-
lowed in the policy.
   [#LC5360]

Printing

• When a default printer is not set, all mapped printers might fail in sessions.
   [#LC4354]
• With legacy printer names enabled, autocreated printers might not be available for use in a pub-
lished application when multiple sessions are established on a single server for the same user.
   [#LC4517]
• The “Auto-create client printers” policy might fail to set default printers correctly in a published
application and Microsoft XPS Document Writer is set as the default printer.
   [#LC4696]
• Excel spreadsheets generated by SAP fail to print on printers redirected using the Universal Print
Driver EMF driver.
   [#LC4853]
• After a user logs off and logs back on, printers connected to the session might not be accessible.
   [#LC5188]
• The Print Preview on Client option within Citrix Universal Print Driver displays to the local end
point.
   [#LC5404]

Server/Site Administration

• The changes made or values added to the registry key “HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Main” created by the WfShell.exe process might not be preserved during logoff.
   [#LC4648]

Session/Connection

• When resizing a reconnected session with a Citrix policy in place to prohibit session wallpaper
and a Microsoft group policy in place that specified a wallpaper, the Citrix policy is not honored.
   [#LC0115]
• When exiting a 64bit ThinAPP packaged application, the application can experience an unexpected exception on sfrhook64.dll.

To prevent this, create following server-side registry key to resolve the issue:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\SfrHook

Name: SkipUnloadonProcessExit
Type: DWORD
Data: Any Value

[LC3484]

• On systems with Hotfix ICAWS760WX86022 installed, attempts to reconnect to a user session might fail when you restart the Citrix ICA Service.

[LC3714]

• With this enhancement, an entry is written to the Windows Event log when a USB device is redirected in a session.

[LC3996]

• Using published instances of Microsoft Internet Explorer, attempts to download a file from a website and saving it to a mapped client drive (“Save as…”) can fail.

[LC4300]

• In sessions on systems with Fix #LC1155 installed, an image display area inside a custom application is not resized properly if you resize the window manually.

[LC4319]

• Audio files might fail to play in a VDA session when connected through Citrix Receiver for Mac or a Chromebook.

[LC4596]

• After a network interruption between a VDA and Citrix Receiver, you cannot play back an .avi file on Windows Media Player.

[LC4670]

• Time zone redirection might not work in user sessions running on iOS devices.

[LC4869]

• After using the Remote Desktop Protocol, the ICA session might display a grey screen when reconnecting to the VM. This issue only occurs on VDAs installed with /NOCITRIXWDDM.

[LC4970]
• A USB device might fail to work after it is redirected to Version 7.6.300 of the VDA. The issue occurs when the instance ID of the device is different from the serial number.

To enable this fix, add the Product ID or Vendor ID pairs to the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\icausbb\Parameters

Name: UsingSerialNumberDevices

Type: REG_MULTI_SZ

Value: <Note: Next to the comments string, add the vid=xxxx and pid=xxxx pairs. (The syntax for the value is an ordered list of case insensitive rules where “#” is a line comment and each rule is an ordered vid and pid pair. For example, vid=#-number and pid=#-number. The maximum hex value for a vid/pid is FFFF. If the length of a vid/pid hex value is less than 4, pair the number with zeroes (0). For example, if the vid is 12 and pid is 13; the vid/pid pairs should be vid=0012, pid=0013. Each rule has a fixed length: 17, no spaces at the beginning or the end of the rule. Examples: #vid=FFFF, #pid=FFFF #vid=0012, #pid=0013.)>

[LC5035]

• The svchost.exe process can consume 100% of the CPU.

[LC5041]

• With Excelhook enabled and after applying hotfix ICATS760WX64028, the Excel window does not minimize when clicking the Excel icon in the taskbar.

[LC5060]

• The svchost.exe process might fail intermittently on SCardHook64.dll when a user is logging on or off and Certificate Propagation is active.

[LC5083]

• This fix addresses an issue that breaks client-side fetching for DirectShow based applications, preventing videos from rendering.

[LC5098]

• Sessions might not disconnect, resulting in random VDA re-registrations.

[LC5122]

• The operating system experiences an error on picadd.sys and a blue screen appears with bugcheck code 0xd5.

[LC5134]

• An external USB DVD drive that is mapped into a session as a mapped client drive can cause slow session performance.

[LC5231]
• COM port mapping can intermittently fail.
  [#LC5235]
• The following counters in the performance monitor might display inconsistently.
  - ICA Session\Input Session Bandwidth
  - ICA Session\Output Session Bandwidth
  The issue occurs only when the count value is high.
  [#LC5262]
• The operating system experiences an error on picadd.sys and a blue screen appears with
  bugcheck code 0x3b.
  [#LC5299]
• The VDA might become unresponsive at the “Welcome” screen due to a deadlock on picadm.sys.
  [#LC5326]
• With Special Folder Redirection enabled, published applications might fail to launch and the
  following error message appears:
  “The Citrix server is unable to process your request to start this published application.”
  [#LC5593]
• After upgrading a VDA from Version 7.6.300 to Version 7.6 LTSR Cumulative Update 1, launching
  of applications might be slow or can fail.
  [#LC5661]
• Attempts to save a published Microsoft Excel spreadsheet to a Chromebook device might fail.
  The issue occurs because the file extension is not present.
  [#LC6001]

Smart Cards

• The Sign-in option does not appear on Version 7.6.300 and laterVDAs running on Windows 10
  Build 10586 and later. As a result, smart card logons are not possible.
  [#LC4778]
• XenDesktop smart card sessions might randomly disconnect.
  [#LC5265]
• Attempts to log on by using certain smart cards might result in the following error message:
  “No valid certificates were found on this smart card.
  Please try another smart card or contact your administrator.”
  [#LC5456]

**System Exceptions**

• The operating system experiences an error on picadm.sys and a blue screen appears with
  bugcheck code 0x50.
  [#LC4529]

• The operating system experiences an error on picadm.sys and a blue screen appears.
  [#LC4567]

• A non-handled exception copying from USB devices might cause the operating system to expe-
  rience an error and a blue screen appears.
  [#LC4782]

• A published application process might exit unexpectedly with an exception “c000041d” on Mo-
  bileDesktopHook64.dll.
  [#LC4821]

• When you log on to a VDA running on Windows Server 2008 R2 through a remote desktop and
  launch certain third-party applications, the applications might exit unexpectedly.
  [#LC5891]

**User Experience**

• When you switch from a touch-optimized published desktop to a regular published desktop, the
  Start button:
  – Does not highlight when you hover over it
  – Brings up the local desktop instead of the published desktop
  [#LC3466]

• Certain .wmv files might not play at the correct aspect ratio.
  [#LC4695]

• Connecting to audio recording/dictation software during an ICA session might cause the soft-
  ware to exit unexpectedly.
  [#LC5407]
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

User Interface

• After publishing seamless applications, the generic Citrix Receiver icon may appear instead of
  the published app icon in the taskbar.

  [#LC4757]

Known issues

February 5, 2019

Known issues in Cumulative Update 7

No new issues have been found in CU7 to date.

Known issues in Cumulative Update 6

• Attempts to upgrade from Versions 2.5, 2.6, or 3.0.1 of StoreFront to any version of StoreFront
  included with any Cumulative Update for XenApp and XenDesktop 7.6 LTSR using the metainstan-
  celer can fail. The issue occurs when the StoreFront Management Console is open or a Power-
  Shell session is running during the upgrade and without warning. [LCM-4801]

• After you upgrade to XenApp and XenDesktop 7.6 LTSR CU6, a site upgrade failure might occur
  when the site’s License Server is not updated to the version that is released as a part of CU6.
  There are no notifications by the product installer during the upgrade. [LCM-5466]

Known issues in Cumulative Update 5

Attempts to upgrade from Versions 2.5 or 2.6 of StoreFront to any version of StoreFront included with
any Cumulative Update for XenApp and XenDesktop 7.6 LTSR can fail. The issue occurs when the Store-
Front Management Console is open or a PowerShell session is running during the upgrade and with-
out warning. The issue is limited to systems running Windows 2012 R2 Server with .NET 4.6 or .NET
4.7 updates installed. [3283]

Known issues in Cumulative Update 4

No new issues have been found in CU4 to date.
Known issues in Cumulative Update 3

No new issues have been found in CU3 to date.

Known issues in Cumulative Update 2

- Attempts to manually update XenDesktop 5.6, 7.1, 7.5, or XenApp 7.5 deployments using the PowerShell SDK can fail to upgrade one or more DBSchemas. As a workaround, upgrade the Site DBschema using the Automatic or Manual Site upgrade methods from Citrix Studio rather than using the PowerShell SDK. [LCM-903]

- When using Citrix Receiver for Linux, HDX Flash redirection can fall back to server-side rendering and the websites are added to the dynamic blacklist. As a workaround, use Emulation Mode. [LCM-944]

- Citrix Studio can exit unexpectedly upon launch. The issue occurs if you have Studio and Storefront installed on a single Windows 2008 R2 SP1 system that was previously updated with Microsoft articles KB3163251 and KB3135996v2. The following error message appears in the Event Viewer:

  ".NET Runtime version 2.0.50727.5485 - Fatal Execution Engine Error."

  As a workaround, run the following prompt from the command line:

  "C:\windows\microsoft.net\framework64\v2.0.50727\ngen update /force" [LCM-969]

- Attempts to install VDA for Server OS can fail with a generic error code 1603. For more information, including a workaround, see Knowledge Center article CTX213807. [LCM-1013]

- **Note:** This issue is fixed as LC6934 in CU4.

  Certain websites, including Qumu, are automatically blacklisted and fall back to server-side content rendering. As a workaround to keep affected sites from being blacklisted, set the following registry key on the VDA:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\Name: SupportedUrlHeads

    Type: REG_MULTI_SZ

    Data: each value on a separate line, null separated:

    http://
    https://
    file:// [LCM-1605]

- **Note:** This issue is fixed as LC6471 in CU3.
After installing StoreFront 3.0.1000 or 3.0.2000, the management console fails to start and the following error message appears: “The Management console is unavailable because of a root certificate missing, go to verisign and download the certificate - Verisign class primary CA - G5.” For more information, see Knowledge Center article CTX218815. [LC6471]

- **Note:** This issue is fixed as LC6816 in CU3.

Upgrading StoreFront to version 3.0.2000 from version 2.5 fails with Error 1603. For more information, see Knowledge Center article CTX220411. [LC6816]

### Known issues in Cumulative Update 1

- If you install a component of this release using its standalone msi (not recommended) rather than through the Metainstaller, a prompt appears for the License Server compatibility check in Desktop Studio that makes sure that your License server is the required version. If you are using the License server released with XenApp/Desktop 7.6 or from a more recent version, you do not need to upgrade the License server. Click Continue to proceed with the DBschema upgrade. [575064]

- When you upgrade an instance of Version 11.12.1 of the license server (included in the XenApp/XenDesktop 7.6 RTM release) that was deployed using Active Directory, both the Citrix Licensing and the Citrix Licensing Support Services are disabled.

  To prevent this issue, install Version 11.13.1 of the license server using citrixlicensing.exe from the CU1 media before installing the rest of CU1. [630116]

- **Note:** This issue is fixed as #630814 in CU2.

  Site Setup in Citrix Studio might fail to proceed when choosing “Use an existing license.” As a workaround, restart the “Citrix Web Services for Licensing” service on the license server to complete its configuration. [630814]

- If you install a component of this release using its standalone msi (not recommended) rather than through the Metainstaller, Citrix Scout displays dual entries for that component. [636862]

- **Note:** This issue is fixed as LC6471 in CU3.

  After installing StoreFront 3.0.1000 or 3.0.2000, the management console fails to start and the following error message appears: “The Management console is unavailable because of a root certificate missing, go to verisign and download the certificate - Verisign class primary CA - G5.” For more information, see Knowledge Center article CTX218815. [LC6471]

- **Note:** This issue is fixed as #LC6816 in CU3.

  Upgrading StoreFront to version 3.0.2000 from version 2.5 fails with Error 1603. For more information, see Knowledge Center article CTX220411. [LC6816]
Known issues in LTSR

- Attempts to update a XenApp 6.5 server to become a VDA for Server OS can fail. The issue occurs on XenApp 6.5 servers that were installed in Controller and Session-Host mode because the Citrix XML Service shares a common port with IIS Server.

As a workaround, uninstall XenApp 6.5 server, restart the server, and then install LTSR or its current Cumulative Update. For more information, see Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS. [LCM-893]

- **Note**: This issue is fixed as LC5098 in the LTSR CU2 VDAs.

After updating your VDAs to 7.6 LTSR (7.6.300), client-side content redirection for DirectShow based applications (for example, - QUMU, QVOP) does not work, and videos fail to render. [LC5098-x]

- The VDA metainstaller no longer includes or updates the following Citrix clients:
  - Citrix Receiver for Windows, Enterprise Edition
  - Offline plug-in

Both clients have reached End of Life. The latest version of Citrix Receiver is available for download at [https://www.citrix.com/downloads/citrix-receiver.html](https://www.citrix.com/downloads/citrix-receiver.html). [XA-1532]

- Universal Print Server printers selected on the virtual desktop do not appear in the **Devices and Printers** window in Windows Control Panel. However, when users are working in applications, they can print using those printers. This issue occurs only on the Windows Server 2012, Windows 10 and Windows 8 platforms. For more information, see Knowledge Center article CTX213540. [335153]

System requirements

February 19, 2019

In this article:

Session Recording
Delivery Controller
Database
Studio
Director
Virtual Delivery Agent (VDA) for Windows Desktop OS
Virtual Delivery Agent (VDA) for Windows Server OS
Hosts / Virtualization resources
Active Directory functional level support
HDX - Desktop Composition Redirection
HDX - Windows Media Delivery
HDX - Flash Redirection
HDX 3D Pro
HDX - Video conferencing requirements for webcam video compression
HDX - Other
Universal Print Server requirements
Other requirements

The system requirements in this document were valid when this product version released. System requirements components not covered here (such as StoreFront, host systems, receivers and plugins, and Provisioning Services) are described in their respective documentation.

Important: Review Prepare to install before beginning an installation.

Unless otherwise noted, the component installer deploys software prerequisites automatically (such as .NET and C++ packages) if they are not detected on the machine. The Citrix installation media also contains some of this prerequisite software.

The installation media contains several third-party components. Before using the Citrix software, check for security updates from the third party, and install them.

The disk space values are estimates only, and are in addition to space needed for the product image, operating system, and other software.

If you install all the core components (Controller with SQL Server Express, Studio, Director, StoreFront, and Licensing) on a single server, you need a minimum of 3 GB of RAM to evaluate the product; more is recommended when running an environment for users. Performance will vary depending on your exact configuration, including the number of users, applications, desktops, and other factors.

Important: After you install XenApp on a Windows Server 2012 R2 system, use the Kerberos Enable Tool (XASsonKerb.exe) to ensure the correct operation of Citrix Kerberos authentication. The tool is located Support > Tools > XASsonKerb folder on the installation media; you must have local administrator privileges to use the tool. To ensure correct Kerberos operation, run xassonkerb.exe -install from a command prompt on the server. If you later apply an update that changes the registry location HKLM\System\CurrentControlSet\Control\LSA\OSConfig, run the command again. To see all available tool options, run the command with the -help parameter.
Session Recording

Session Recording Administration components

You can install the Session Recording Administration components (Session Recording Database, Session Recording Server, and Session Recording Policy Console) on a single server or on separate servers.

Session Recording Database

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:

- .NET Framework Version 3.5 Service Pack 1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.2 or 4.6.

Session Recording Server

Supported operating systems:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:

Before starting the Session Recording installation, you must install some prerequisites. Open the Server Manager and add the IIS role. Select the following options:

- Application Development:
  - ASP.NET 4.5 on Server 2012 and Server 2012 R2, ASP.NET on Server 2008 R2 (other components are automatically selected. Click Add to accept required roles)
- Security - Windows Authentication
- Management Tools - IIS 6 Management Compatibility
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility
  - IIS 6 Scripting Tools
  - IIS 6 Management Console
- .NET Framework Version 3.5 Service Pack 1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.2 or 4.6.
If the Session Recording Server uses HTTPS as its communications protocol, add a valid certificate. Session Recording uses HTTPS by default, which Citrix recommends.
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled.

**Session Recording Policy Console**

Supported operating systems:
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:
- .NET Framework Version 3.5 Service Pack 1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.2 or 4.6.

**Session Recording Agent**

Install the Session Recording Agent on every XenApp and XenDesktop server on which you want to record sessions.

Supported operating systems:
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 with Service Pack 1

Requirements:
- Microsoft Message Queuing (MSMQ), with Active Directory integration disabled, and MSMQ HTTP support enabled
- .NET Framework Version 3.5 Service Pack 1 (Windows Server 2008 R2 only) or .NET Framework Version 4.5.2 or 4.6.

**Session Recording Player**

Supported operating systems:
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 with Service Pack 1

For optimal results, install Session Recording Player on a workstation with:
- Screen resolution of 1024 x 768
- Color depth of at least 32-bit
- Memory: 1GB RAM (minimum). Additional RAM and CPU/GPU resources can improve performance when playing graphics intensive recordings; especially when there are a lot of animations in the recordings.

The seek response time depends on the size of the recording and your machine’s hardware specification.

Requirements:
- .NET Framework Version 3.5 Service Pack 1 or .NET Framework Version 4.5.2 or 4.6.

**Delivery Controller**

Supported operating systems:
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

Requirements:
- Disk space: 100 MB. Connection leasing (which is enabled by default) adds to this requirement; sizing depends on the number of users, applications, and mode (RDS or VDI). For example, 100,000 RDS users with 100 recently-used applications require approximately 3 GB of space for connection leases; deployments with more applications may require more space. For dedicated VDI desktops, 40,000 desktops require at least 400-500 MB. In any instance, providing several GBs of additional space is suggested.
- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 only).
- Microsoft .NET Framework 4.5.2, 4.6, 4.6.1
- Windows PowerShell 2.0 (included with Windows Server 2008 R2) or 3.0 (included with Windows Server 2012 R2 and Windows Server 2012).

**Database**

Supported Microsoft SQL Server versions for the Site Configuration Database (which initially includes the Configuration Logging Database and the Monitoring Database):
- SQL Server 2017, Express, Standard, and Enterprise Editions.
- SQL Server 2016, Express, Standard, and Enterprise Editions.
- SQL Server 2014 through SP2, Express, Standard, and Enterprise Editions.
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

- SQL Server 2012 through SP3, Express, Standard, and Enterprise Editions. By default, prior to CU4, SQL Server 2012 SP1 Express is installed when you install the Controller unless an existing, supported SQL Server installation is detected. As of CU4, SQL Server 2012 SP3 Express is installed when you install the Controller unless an existing, supported SQL Server installation is detected.
- SQL Server 2008 R2 SP2 and SP3, Express, Standard, Enterprise, and Datacenter Editions.

The following database features are supported (except for SQL Server Express, which supports only standalone mode):

- SQL Server Clustered Instances
- SQL Server Mirroring
- SQL Server AlwaysOn Availability Groups (including Basic Availability Groups)

Windows authentication is required for connections between the Controller and the SQL Server database.

For information about the latest supported database versions, see CTX114501.

**Studio**

**Supported operating systems:**

- Windows 8.1, Professional and Enterprise Editions
- Windows 8, Professional and Enterprise Editions
- Windows 7 Professional, Enterprise, and Ultimate Editions
- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

**Requirements:**

- Disk space: 75 MB
- Microsoft .NET Framework 4.6.1
- Microsoft .NET Framework 4.5.2, 4.6
- Microsoft Management Console 3.0 (included with all supported operating systems)
- Windows PowerShell 2.0

**Director**

**Supported operating systems:**

- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

Requirements:

- Disk space: 50 MB.
- Microsoft .NET Framework 4.5.2, 4.6
- Microsoft .NET Framework 3.5 SP1 (Windows Server 2008 R2 only)
- Microsoft Internet Information Services (IIS) 7.0 and ASP.NET 2.0. Ensure that the IIS server role has the Static Content role service installed. If these are not already installed, you are prompted for the Windows Server installation media, then they are installed for you.
- Supported browsers for viewing Director:
  - Internet Explorer 11 and 10. Compatibility mode is not supported for Internet Explorer. You must use the recommended browser settings to access Director. When you install Internet Explorer, accept the default to use the recommended security and compatibility settings. If you already installed the browser and chose not to use the recommended settings, go to Tools > Internet Options > Advanced > Reset and follow the instructions.
  - Firefox ESR (Extended Support Release).
  - Chrome.

Virtual Delivery Agent (VDA) for Windows Desktop OS

Supported operating systems:

For information about Windows 10 compatibility, see our blog.

- Windows 8.1, Professional and Enterprise Editions
- Windows 8, Professional and Enterprise Editions
- Windows 7 SP1, Professional, Enterprise, and Ultimate Editions

To use the Server VDI feature, you can use the command line interface to install a VDA for Windows Desktop OS on a supported server operating system; see Server VDI for guidance.

- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

Requirements:

- Microsoft .NET Framework 4.5.2, 4.6, 4.6.1
- Microsoft .NET Framework 3.5.1 (Windows 7 only)
Remote PC Access uses this VDA, which you install on physical office PCs.

Several multimedia acceleration features (such as HDX MediaStream Windows Media Redirection) require that Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features will not be installed and will not work. Do not remove Media Foundation from the machine after installing the Citrix software; otherwise, users will not be able to log on to the machine. On most Windows 8.1, Windows 8, and Windows 7 editions, Media Foundation support is already installed and cannot be removed. However, N editions do not include certain media-related technologies; you can obtain that software from Microsoft or a third party.

During VDA installation, you can choose to install the HDX 3D Pro version of the VDA for Windows Desktop OS. That version is particularly suited for use with DirectX and OpenGL-driven applications and with rich media such as video.

**Virtual Delivery Agent (VDA) for Windows Server OS**

Supported operating systems:

- Windows Server 2012 R2, Standard and Datacenter Editions
- Windows Server 2012, Standard and Datacenter Editions
- Windows Server 2008 R2 SP1, Standard, Enterprise, and Datacenter Editions

The installer automatically deploys the following requirements, which are also available on the Citrix installation media in the Support folders:

- Microsoft .NET Framework 4.5.2, 4.6, 4.6.1
- Microsoft .NET Framework 3.5.1 (Windows Server 2008 R2 only)

The installer automatically installs and enables Remote Desktop Services role services, if they are not already installed and enabled.

Several multimedia acceleration features (such as HDX MediaStream Windows Media Redirection) require that the Microsoft Media Foundation be installed on the machine on which you install the VDA. If the machine does not have Media Foundation installed, the multimedia acceleration features will not be installed and will not work. Do not remove Media Foundation from the machine after installing the Citrix software; otherwise, users will not be able to log on to the machine. On most Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 editions, the Media Foundation feature is installed through the Server Manager (for Windows Server 2012 R2 and Windows Server 2012: ServerMediaFoundation; for Windows Server 2008 R2: DesktopExperience). However, N editions do
not include certain media-related technologies; you can obtain that software from Microsoft or a third party.

**Hosts / Virtualization resources**

**Supported platforms**

**IMPORTANT:** The following major.minor versions are supported, including updates to those versions. CTX131239 contains the most current hypervisor version information, plus links to known issues.

XenServer.

- XenServer 7.2
- XenServer 7.1
- XenServer 7.0
- XenServer 6.5 SP1
- XenServer 6.5
- XenServer 6.2 SP1 plus hotfixes (you must apply SP1 to enable application of future hotfixes)
- XenServer 6.1

VMware vSphere (vCenter + ESXi). No support is provided for vSphere vCenter Linked Mode operation.

- VMware vSphere 6.5
- VMware vSphere 6.0
- VMware vSphere 5.5
- VMware vSphere 5.1
- VMware vSphere 5.0
- VMware vCenter 5.5 / 6 appliance

System Center Virtual Machine Manager - Includes any version of Hyper-V that can register with the supported System Center Virtual Machine Manager versions.

- System Center Virtual Machine Manager 2012 R2
- System Center Virtual Machine Manager 2012 SP1
- System Center Virtual Machine Manager 2012

Nutanix Acropolis 4.5 - Several XenApp and XenDesktop features are not available when using this platform; see CTX202032 for details. For more information on the use of the product with Acropolis, see [https://portal.nutanix.com/#/page/docs](https://portal.nutanix.com/#/page/docs).

Amazon Web Services (AWS)

- You can provision applications and desktops on supported Windows server operating systems.
- The Amazon Relational Database Service (RDS) is not supported.
- See [Citrix XenDesktop on AWS](https://portal.nutanix.com/#/page/docs) for additional information.
Citrix CloudPlatform

- The minimum supported version is 4.2.1 with hotfixes 4.2.1-4.
- Deployments were tested using XenServer 6.2 (with Service Pack 1 and hotfix XS62ESP1003) and vSphere 5.1 hypervisors.
- CloudPlatform does not support Hyper-V hypervisors.
- CloudPlatform 4.3.0.1 supports VMware vSphere 5.5.
- See the CloudPlatform documentation (including the Release Notes for your CloudPlatform version) and XenApp and XenDesktop concepts and deployment on CloudPlatform for additional support and Linux-based system requirements information.

The following virtualization resource and storage technology combinations are supported for Machine Creation Services and runtime Active Directory account injection into VMs. Combinations marked with an asterisk (*) are recommended.

<table>
<thead>
<tr>
<th>Virtualization resource</th>
<th>Local Disks</th>
<th>NFS</th>
<th>Block Storage</th>
<th>Storage Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>XenServer</td>
<td>Yes</td>
<td>Yes *</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>VMware</td>
<td>Yes (no vMotion or dynamic placement)</td>
<td>Yes *</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Hyper-V</td>
<td>Yes</td>
<td>No</td>
<td>Yes * (requires Cluster Shared Volumes)</td>
<td>No</td>
</tr>
</tbody>
</table>

The Remote PC Access Wake on LAN feature requires Microsoft System Center Configuration Manager. See Configuration Manager and Remote PC Access Wake on LAN for details.

**Active Directory functional level support**

The following functional levels for the Active Directory forest and domain are supported:

- Windows 2000 native (not supported for domain controllers)
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
HDX - Desktop Composition Redirection

The Windows user device or thin client must support or contain:

- DirectX 9
- Pixel Shader 2.0 (supported in hardware)
- 32 bits per pixel
- 1.5 GHz 32-bit or 64-bit processor
- 1 GB RAM
- 128 MB video memory on the graphic card or an integrated graphics processor

HDX queries the Windows device to verify that it has the required GPU capabilities and automatically reverts to server-side desktop composition if it does not. List the devices with the required GPU capabilities that do not meet the processor speed or RAM specifications in the GPO group for devices excluded from Desktop Composition Redirection.

The minimum available bandwidth is 1.5 Mbps; recommended bandwidth is 5 Mbps. Those values incorporate end-to-end latency.

HDX - Windows Media Delivery

The following clients are supported for Windows Media client-side content fetching, Windows Media redirection, and real-time Windows Media multimedia transcoding: Receiver for Windows, Receiver for iOS, and Receiver for Linux.

To use Windows Media client-side content fetching on Windows 8 devices, set the Citrix Multimedia Redirector as a default program: in Control Panel > Programs > Default Programs > Set your default programs, select Citrix Multimedia Redirector and click either Set this program as default or Choose defaults for this program.

GPU transcoding requires an NVIDIA CUDA-enabled GPU with Compute Capability 1.1 or higher; see http://developer.nvidia.com/cuda/cuda-gpus.

HDX - Flash Redirection

The following clients and Adobe Flash Players are supported:

- Receiver for Windows (for second generation Flash Redirection features) - Second generation Flash Redirection features require Adobe Flash Player for Other Browsers, sometimes referred to as an NPAPI (Netscape Plugin Application Programming Interface) Flash Player
• Receiver for Linux (for second generation Flash Redirection features) - Second generation Flash Redirection features require Adobe Flash Player for other Linux or Adobe Flash Player for Ubuntu.

• Citrix Online plug-in 12.1 (for legacy Flash Redirection features) - Legacy Flash Redirection features require Adobe Flash Player for Windows Internet Explorer (sometimes referred to as an ActiveX player).

The major version number of the Flash Player on the endpoint must be greater than or equal to the major version number of the Flash Player on the VDA. If an earlier version of the Flash Player is installed on the endpoint, or if the Flash Player cannot be installed on the endpoint, Flash content is rendered on the VDA.

The machines running VDAs require:

• Adobe Flash Player for Windows Internet Explorer (the ActiveX player)
• Internet Explorer 11 (in non-Modern UI mode). - Flash Redirection works by remoting the ActiveX protocol from the VDA to the Flash Player on the endpoint. Because Internet Explorer is the only browser that supports the ActiveX protocol, the feature does not work unless Internet Explorer is installed on the VDA. Otherwise, Flash content is rendered on the VDA.
• Protected mode disabled in Internet Explorer (Tools > Internet Options > Security tab > Enable Protected Mode check box cleared). Restart Internet Explorer to effect the change.

**HDX 3D Pro**

When installing a VDA for Windows Desktop OS, you can choose to install the HDX 3D Pro version.

The physical or virtual machine hosting the application can use GPU Passthrough or Virtual GPU (vGPU):

• GPU Passthrough is available with Citrix XenServer. GPU Passthrough is also available with VMware vSphere and VMware ESX, where it is referred to as virtual Direct Graphics Acceleration (vDGA).
• vGPU is available with Citrix XenServer; see [www.citrix.com/go/vGPU](http://www.citrix.com/go/vGPU) (Citrix My Account credentials required).

Citrix recommends that the host computer have at least 4 GB of RAM and four virtual CPUs with a clock speed of 2.3 GHz or higher.

**Graphical Processing Unit (GPU):**

• For CPU-based compression (including lossless compression), HDX 3D Pro supports any display adapter on the host computer that is compatible with the application being delivered.
• For optimized GPU frame buffer access using the NVIDIA GRID API, HDX 3D Pro requires NVIDIA Quadro cards with the latest NVIDIA drivers. The NVIDIA GRID delivers a high frame rate, resulting in a highly interactive user experience.
For vGPU using XenServer, HDX 3D Pro requirements include NVIDIA GRID K1 and K2 cards.

User device:

- HDX 3D Pro supports all monitor resolutions that are supported by the GPU on the host computer. However, for optimum performance with the minimum recommended user device and GPU specifications, Citrix recommends a maximum monitor resolution for user devices of 1920 x 1200 pixels for LAN connections, and 1280 x 1024 pixels for WAN connections.
- Citrix recommends that user devices have at least 1 GB of RAM and a CPU with a clock speed of 1.6 GHz or higher. Use of the default deep compression codec, which is required on low-bandwidth connections, requires a more powerful CPU unless the decoding is done in hardware. For optimum performance, Citrix recommends that user devices have at least 2 GB of RAM and a dual-core CPU with a clock speed of 3 GHz or higher.
- For multi-monitor access, Citrix recommends user devices with quad-core CPUs.
- User devices do not need a dedicated GPU to access desktops or applications delivered with HDX 3D Pro.
- Citrix Receiver must be installed.

**HDX - Video conferencing requirements for webcam video compression**


Supported video conferencing applications:

- Citrix GoToMeeting HDFaces
- Adobe Connect
- Cisco WebEx
- IBM Sametime
- Microsoft Lync 2010 and 2013
- Microsoft Office Communicator
- Google+ Hangouts
- Skype 6.7. To use Skype on a Windows client, edit the registry on the client and the server:
  - Client registry key HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
    - Name: DefaultHeight, Type: REG_DWORD, Data: 240
    - Name: DefaultWidth, Type: REG_DWORD, Data: 320
  - Server registry key HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility
    - Name: skype.exe, Type: REG_DWORD, Data: Set to 0

Other user device requirements:

- Appropriate hardware to produce sound.
• DirectShow-compatible webcam (use the webcam default settings). Webcams that are hardware encoding-capable reduces client-side CPU usage.

• Webcam drivers, obtained from the camera manufacturer if possible.

**HDX - Other**

UDP audio for Multi-Stream ICA is supported on Receiver for Windows and Receiver for Linux 13.

Echo cancellation is supported on Citrix Receiver for Windows.

**Universal Print Server Requirements**

• Universal Print Server - The Universal Print Server comprises client and server components. The UPClient component is included in the VDA installation. The UPServer component (which you install on each print server where the shared printers reside that you want to provision with the Citrix Universal Print Driver in user sessions) is supported on:
  – Windows Server 2008 R2 SP1

• The following are prerequisites for installing the UPServer component on the print server:
  – Microsoft Visual Studio 2013 Runtime (both 32-bit and 64-bit)
  – Microsoft .NET Framework 4.5.2
  – CDF_x64.msi
  – UpsServer_x64.msi

User authentication during printing operations requires the Universal Print Server to be joined to the same domain as the Remote Desktop Services VDA.

**Other**

• Citrix recommends installing or upgrading to the component software versions provided on the installation media for this release.
  – StoreFront requires 2 GB of memory. See the StoreFront documentation for system requirements. StoreFront 2.6 is the minimum supported version with this release.
  – When using Provisioning Services with this release, the minimum supported Provisioning Services version is 7.0.
  – The Citrix License Server requires 40 MB of disk space. See the licensing documentation for system requirements. Only Citrix License Server for Windows is supported. The minimum supported version is 11.13.1.
• The Microsoft Group Policy Management Console (GPMC) is required if you store Citrix policy information in Active Directory rather than the Site Configuration database. For more information, see the Microsoft documentation.

• By default, the Receiver for Windows is installed when you install a VDA. For system requirements information on other platforms, see the Receiver for Windows documentation.

• The Receiver for Linux and the Receiver for Mac are provided on the product installation media. See their documentation for system requirements.

• When using Access Gateway versions earlier than 10.0 with this release, Windows 8.1 and Windows 8 clients are not supported.

• Desktop Lock - Supported operating systems:
  – Windows 7, including Embedded Edition
  – Windows XP Embedded
  – Windows Vista

User devices must be connected to a local area network (LAN).

Supported Receiver: Citrix Receiver for Windows Enterprise 3.4 package (minimum).

• Client folder redirection - Supported operating systems:
  – Client (with latest Citrix Receiver for Windows): Windows 7, Windows 8, and Windows 8.1

• Multiple network interface cards are supported.

• See the App-V article for supported versions.

• In CU4, the software version provided on the media for Microsoft Visual C++ 2008 SP1 (9.0.30729.4148) was updated to Microsoft Visual C++ 2008 SP1 (9.0.30729.5677).

Install VDAs using the standalone package

February 15, 2019

As an alternative to using the full-product XenApp or XenDesktop ISO to install Virtual Delivery Agents (VDAs), you can use a standalone VDA installation package. The smaller package more easily accommodates deployments using Electronic Software Delivery (ESD) packages that are staged or copied locally, have physical machines, or have remote offices.

The standalone VDA package is intended primarily for deployments that use command-line (silent) installation - it supports the same command line parameters as the XenDesktopVdaSetup.exe command, which is used by the full-product installer. The package also offers a graphical interface that is very similar to the VDA installer on the full-product ISO.
There are two self-extracting standalone VDA packages: one for installation on supported server OS machines, and another for supported workstation (desktop) OS machines.

**Prerequisites and considerations**

The supported operating systems for VDAs, plus other requirements before installation, are listed in [System requirements](#). See [Prepare to install](#) for details about the information you provide and choices you make during VDA installation.

The VDA package automatically deploys prerequisites, if the machine does not already have them; this includes Visual C++ 2008, 2010 and 2013 Runtimes (32-bit and 64-bit) and .NET Framework 4.5.1.

When installing on a supported server OS machine, the Remote Desktop Services (RDS) role services are installed and enabled before installing the VDA. Alternatively, you can install the prerequisites yourself before installing the VDA.

Exception: Verify that Windows Server 2008 R2 and Windows 7 machines have at least .NET 3.5.1 installed before you start the VDA installation.

About restarts

- A restart is required at the end of the VDA installation.
- To minimize the number of additional restarts needed during the installation sequence, ensure that .NET Framework 4.5.1 or 4.5.2 is installed before beginning the VDA installation. Also, for Windows Server OS machines, install and enable the RDS role services before installing the VDA. (Other prerequisites do not typically require machine restarts, so you can let the installer take care of those for you.)
- If you do not install prerequisites before beginning the VDA installation, and you specify the /noreboot option for a command line installation, you must manage the restarts. For example, when using automatic prerequisite deployment, the installer will suspend after installing RDS, waiting for a restart; be sure to run the command again after the restart, to continue with the VDA installation.

If you use the graphical interface or the command line interface option that runs the package, the files in the package are extracted to the Temp folder. More disk space is required on the machine when extracting to the Temp folder than when using the full-product ISO. Files extracted to the Temp folder are not automatically deleted, but you can manually delete them (from C:\Windows\Temp\Ctx-$, where $ is a random Globally Unique Identifier) after the installation completes.

Alternatively, use a third party utility that can extract cabinet archives from EXE files (such as 7-Zip) to extract the files to a directory of your choice, and then run the XenDesktopVdaSetup.exe command. You can use the /extract command with an absolute path. For more information, see How to use in the section below.
If your deployment uses Microsoft System Center Configuration Manager, a VDA installation might appear to fail with exit code 3, even though the VDA installed successfully. To avoid the misleading message, you can wrap your installation in a CMD script or change the success codes in your Configuration Manager package. For more information, see the forum discussion here.

**Citrix Display Only Driver**

The Citrix Display Only Driver (DOD) is the only installed and supported display driver on the XenDesktop Standard VDA on Windows 10.

The Citrix DOD has no GPU assist, even if a GPU or vGPU is present. All rendering is performed by the MS Basic Renderer in the software using the CPU. The Citrix DOD does not support Desktop Composition Redirection (DCR). The Citrix DOD is not installed or supported on XenApp.

**How to use**

Important: You must either have elevated administrative privileges before starting the installation, or use “Run as administrator.”

1. Determine which VDA installer package to use. Use VDAServerSetup.exe if you’re installing on a supported server OS machine. Use VDAWorkstationSetup.exe if you’re installing on a supported desktop OS machine. For single user, single server OS deployments (for example, delivering Windows Server 2012 to one user for web development), use the VDAWorkstationSetup.exe package. For more information, see Server VDI.

2. Install the VDA using the graphical interface or the command line interface.

Remember: You must either have elevated administrative privileges before starting the installation, or use Run as administrator.

**Using the graphical interface:**

Disable User Account Control (UAC), then right-click the downloaded package and choose Run as administrator. The installer launches and proceeds through the installation wizard. The restart at the end of the wizard is required before the VDA can be used in a site. (The wizard is the same as the one used in the full-product ISO to install a VDA; you will not encounter anything different.)

**Using the command line interface:**

Extract the files from the package and then run XenDesktopVdaSetup.exe.

To extract the files before installing, use /extract with the absolute path, for example:

```
\VDAWorkstationSetup.exe /extract %temp%\CitrixVDAInstallMedia
```

Then, in a separate command, run XenDesktopVdaSetup.exe from the directory containing the extracted content. See Install using the command line and CTX140972 for parameter information.
Run the appropriate VDA installer package as if it was the XenDesktopVdaSetup.exe command in everything except its name. See Install using the command line and CTX140972 for parameter information.

For example, the most common installation command used for Remote PC Access installs a VDA on a physical office PC, without installing Citrix Receiver or Citrix Profile Manager. The machine will not automatically be restarted after the VDA is installed; however, a restart is required before the VDA can be used. The VDA will register initially with the Controller on the server named ‘Contr-East’. Ports will be opened if the Windows Firewall Service is detected.

```
VDAWorkstationSetup.exe /quiet /components vda /exclude "Citrix User Profile Manager", "Citrix User Profile Manager WMI Plugin" /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot
```

**Note**

Excluding Citrix Profile management from the installation (Using the X:> XenDesktopVDASetup.exe /EXCLUDE “Personal vDisk”,”Citrix User Profile Manager”, “Citrix User Profile Manager WMI Plugin” option) will affect monitoring and troubleshooting of VDAs with Citrix Director. On the User details and EndPoint pages, the Personalization panel and the Logon Duration panel will fail. On the Dashboard and Trends pages, the Average Logon Duration panel will display data only for machines that have Profile management installed.

Even if you are using a third party user profile management solution, it is recommended that you install and run the Citrix Profile management Service to avoid loss of monitoring and troubleshooting in Citrix Director (enabling the Citrix Profile management Service is not required).

**Upgrade a deployment**

February 19, 2019

You can upgrade certain deployments to newer versions without having to first set up new machines or Sites; this is called an in-place upgrade. You can upgrade:

- From XenDesktop version 5.6 (or a later version) to the latest version of 7.6 LTSR
- From XenApp version 7.5 to the latest version of 7.6 LTSR

You can also use the latest XenApp 7.6 LTSR installer to upgrade a XenApp 6.5 worker server to the latest XenApp 7.6 LTSR VDA for Windows Server OS. This is a supplementary activity to migrating XenApp 6.5; see Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS.

To start an upgrade, you run the installer from the new version to upgrade previously installed core components (Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server) and VDAs. The
installer determines which components require upgrading and then starts the upgrade at your command. After upgrading the components, you use the newly upgraded Studio to upgrade the Site database and the Site.

Be sure to review all the information in this article before beginning the upgrade.

**Upgrade sequence**

The following diagram summarizes the upgrade sequence. Details are provided in Upgrade procedure below. For example, if you have more than one core component installed on a server, running the installer on that machine will upgrade all components that have new versions. You might want to upgrade the VDA used in a master image, and then update the image. Then, update the catalog that uses that image and the Delivery Group that uses that catalog. Details also cover how to upgrade the Site databases and the Site automatically or manually.

**Which product component versions can be upgraded**

Using the product installer and Studio, you can upgrade:

- Citrix License Server, Studio, and StoreFront
- Delivery Controllers 5.6 or later
- VDA 5.6 or later
  - Unlike earlier VDA releases, you must use the product installer to upgrade VDAs; you cannot use MSIs.
  - If the installer detects Receiver for Windows (Receiver.exe) on the machine, it is upgraded to the Receiver version included on the product installation media.
- Director 1.0 or later
- Database: This Studio action upgrades the schema and migrates data for the Site database (plus the Configuration Logging and Monitoring databases, if you’re upgrading from an earlier 7.x version)

Using the guidance in the feature/product documentation, upgrade the following if needed:

- Provisioning Services (for XenApp 7.x and XenDesktop 7.x, Citrix recommends using the latest released version; the minimum supported version is Provisioning Services 7.0).
  - Upgrade the Provisioning Services server using the server rolling upgrade, and the clients using vDisk versioning.
  - Provisioning Services 7.x does not support creating new desktops with XenDesktop 5 versions. So, although existing desktops will continue to work, you cannot use Provisioning Services 7.x to create new desktops until you upgrade XenDesktop. Therefore, if you plan a mixed environment of XenDesktop 5.6 and 7.x Sites, do not upgrade Provisioning Services to version 7.
• Microsoft System Center Virtual Machine Manager SCVMM. The current product supports SCVMM 2012 and SCVMM 2012 SP1; XenDesktop 5.x supports earlier versions. Use the following upgrade sequence to avoid downtime:
  1. If you have Controllers running versions earlier than XenDesktop 5.6 FP1, upgrade them to XenDesktop 5.6 FP1 (see the XenDesktop documentation for that version).
  2. Upgrade the SCVMM server to SCVMM 2012; see the Microsoft documentation for instructions.
  3. Upgrade XenDesktop components to the current version.
  4. Optionally, upgrade the SCVMM server to SCVMM 2012 SP1.
• StoreFront.

Limits

The following limits apply to upgrades:

Selective component install

If you install or upgrade any components to the new version but choose not to upgrade other components (on different machines) that require upgrade, Studio will remind you. For example, let’s say an upgrade includes new versions of the Controller and Studio. You upgrade the Controller but you do not run the installer on the machine where Studio is installed. Studio will not let you continue to manage the Site until you upgrade Studio.

You do not have to upgrade VDAs, but Citrix recommends upgrading all VDAs to enable you to use all available features. If you do not plan to upgrade all VDAs to the latest version, review Mixed VDA support.

XenApp version earlier than 7.5

You cannot upgrade from a XenApp version earlier than 7.5. You can migrate from XenApp 6.x; see Migrate XenApp 6.x.

Although you cannot upgrade a XenApp 6.5 farm, you can replace the XenApp 6.5 software on a Windows Server 2008 R2 machine with a current VDA for Server OS. See Upgrade a XenApp 6.5 worker to a new VDA.

XenDesktop version earlier than 5.6

You cannot upgrade from a XenDesktop version earlier than 5.6.
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

XenDesktop Express Edition

You cannot upgrade XenDesktop Express edition. Obtain and install a license for a currently supported edition, and then upgrade it.

Early Release or Technology Preview versions

You cannot upgrade from a XenApp or XenDesktop Early Release or Technology Preview version.

Windows XP/Vista

If you have VDAs installed on Windows XP or Windows Vista machines, see VDAs on machines running Windows XP or Windows Vista.

Product selection

When you upgrade from an earlier 7.x version, you do not choose or specify the product (XenApp or XenDesktop) that was set during the initial installation.

Mixed environments/sites

If you must continue to run earlier version Sites and current version Sites, see Mixed environment considerations.

Preparation

Before beginning an upgrade:

Decide which interface to use

Use the installer’s graphical or command-line interface to upgrade core components and VDAs. You cannot import or migrate data from an earlier version.

Check your Site’s health

Ensure the Site is in a stable and functional state before starting an upgrade. If a Site has issues, upgrading will not fix them, and can leave the Site in a complex state that is difficult to recover from. To test the Site, select the Site entry in the Studio navigation pane. In the Site configuration portion of the middle pane, click Test site.
Back up the Site, monitoring, and Configuration Logging databases

Follow the instructions in CTX135207. If any issues are discovered after the upgrade, you can restore the backup.

Optionally, back up templates and upgrade hypervisors, if needed.

Complete any other preparation tasks dictated by your business continuity plan.

In a high availability environment, ensure that the Site, monitoring, and Configuration Logging databases are running on the primary database server before starting an upgrade.

Ensure your Citrix licensing is up to date

Before upgrading the Citrix License Server, be sure your Subscription Advantage date is valid for the new product version. If you are upgrading from an earlier 7.x product version, the date must be at least 2016.0420.

Close applications and consoles

Before starting an upgrade, close all programs that might potentially cause file locks, including administration consoles and PowerShell sessions. (Restarting the machine ensures that any file locks are cleared, and that there are no Windows updates pending.)

Important: Before starting an upgrade, stop and disable any third-party monitoring agent services.

Ensure you have proper permissions

In addition to being a domain user, you must be a local administrator on the machines where you are upgrading product components.

The Site database and the Site can be upgraded automatically or manually. For an automatic database upgrade, the Studio user’s permissions must include the ability to update the SQL Server database schema (for example, the db_securityadmin or db_owner database role). If the Studio user does not have those permissions, initiating a manual database upgrade will generate scripts. The Studio user runs some of the scripts from Studio; the database administrator runs other scripts using a tool such as SQL Server Management Studio.

Use StoreFront

If you deployment includes Web Interface, Citrix recommends using StoreFront.
Mixed environment considerations

When your environment contains Sites/farms with different product versions (a mixed environment), Citrix recommends using StoreFront to aggregate applications and desktops from different product versions (for example, if you have a XenDesktop 7.1 Site and a XenDesktop 7.5 Site). For details, see the StoreFront documentation.

- In a mixed environment, continue using the Studio and Director versions for each release, but ensure that different versions are installed on separate machines.
- If you plan to run XenDesktop 5.6 and 7.x Sites simultaneously and use Provisioning Services for both, either deploy a new Provisioning Services for use with the 7.x Site, or upgrade the current Provisioning Services and be unable to provision new workloads in the XenDesktop 5.6 Site.

Within each Site, Citrix recommends upgrading all components. Although you can use earlier versions of some components, all the features in the latest version might not be available. For example, although you can use current VDAs in deployments containing earlier Controller versions, new features in the current release may not be available. VDA registration issues can also occur when using non-current versions.

- Sites with Controllers at version 5.x and VDAs at version 7.x should remain in that state only temporarily. Ideally, you should complete the upgrade of all components as soon as possible.
- Do not upgrade a standalone Studio version until you are ready to use the new version.

VDAs on machines running Windows XP or Windows Vista

You cannot upgrade VDAs installed on machines running Windows XP or Windows Vista to a 7.x version. You must use VDA 5.6 FP1 with certain hotfixes; see CTX140941 for instructions. Although earlier-version VDAs will run in a 7.x Site, they cannot use many of its features, including:

- Features noted in Studio that require a newer VDA version.
- Configuring App-V applications from Studio.
- Configuring Receiver StoreFront addresses from Studio.
- Automatic support for Microsoft Windows KMS licensing when using Machine Creation Services. See CTX128580.
- Information in Director:
  - Logon times and logon end events impacting the logon duration times in the Dashboard, Trends, and User Detail views.
  - Logon duration breakdown details for HDX connection and authentication time, plus duration details for profile load, GPO load, logon script, and interactive session establishment.
  - Several categories of machine and connection failure rates.
  - Activity Manager in the Help Desk and User Details views.
Citrix recommends reimaging Windows XP and Windows Vista machines to a supported operating system version and then installing the latest VDA.

**VDAs on machines running Windows 8.x and Windows 7**

To upgrade VDAs installed on machines running Windows 8.x or Windows 7 to Windows 10, Citrix recommends reimaging Windows 7 and Windows 8.x machines to Windows 10 and then installing the supported VDA for Windows 10, using the standalone VDA installation package delivered with XenApp and XenDesktop 7.6 FP3. If reimaging is not an option, uninstall the VDA prior to upgrading the operating system, otherwise the VDA will be in an unsupported state.

**Mixed VDA support**

When you upgrade the product to a later version, Citrix recommends you upgrade all the core components and VDAs so you can access all the new and enhanced features in your edition.

In some environments, you may not be able to upgrade all VDAs to the most current version. In this scenario, when you create a machine catalog, you can specify the VDA version installed on the machines. By default, this setting specifies the latest recommended VDA version. Consider changing this setting only if the machine catalog contains machines with earlier VDA versions. Mixing VDA versions in a machine catalog is not recommended.

If a machine catalog is created with the default recommended VDA version setting, and any of the machines in the catalog has an earlier VDA version installed, those machines will not be able to register with the Controller and will not work.

For example, you create a machine catalog with the default VDA setting: “7.6 (recommended, to access the latest features).” You add three machines to that catalog: two with VDA 7.6 and one with VDA 7.1. The VDA 7.1 machine will not register with the Controller. If you cannot upgrade that VDA, consider creating a separate machine catalog configured with a VDA setting of “version 7.0 or later” and adding that machine. Although that machine will not be able to take advantage of new 7.6 features, it will be able to register with the Controller.

**Upgrade procedure**

To run the product installer graphical interface, log on to the machine and then insert the media or mount the ISO drive for the new release. Double-click **AutoSelect**. To use the command-line interface, see **Install using the command line**.

**Step 1.** If more than one core component is installed on the same server (for example, the Controller, Studio, and License Server) and several of those components have new versions available, they will all be upgraded when you run the installer on that server.
If any core components are installed on machines other than the Controller, run the installer on each of those machines. The recommended order is: License Server, StoreFront, and then Director.

**Step 2.** If you use Provisioning Services, upgrade the PVS servers and target devices, using the guidance in the Provisioning Services documentation.

**Step 3.** Run the product installer on machines containing VDAs. (See Step 12 if you use master images and Machine Creation Services.)

When upgrading VDAs from an earlier 7.x version that are installed on physical machines (including Remote PC Access), use the command-line interface with the option /exclude “Personal vDisk”, ”Machine Identity Service”. For example:

```
C:\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /exclude “Personal vDisk”, ”Machine Identity Service”
```

**Step 4.** Run the product installer on half of the Controllers. (This also upgrades any other core components installed on those servers.) For example, if your Site has four Controllers, run the installer on two of them.

- Leaving half of the Controllers active allows users to access the Site. VDAs can register with the remaining Controllers. There may be times when the Site has reduced capacity because fewer Controllers are available. The upgrade causes only a brief interruption in establishing new client connections during the final database upgrade steps. The upgraded Controllers cannot process requests until the entire Site is upgraded.
- If your Site has only one Controller, the Site is inoperable during the upgrade.

**Step 5.** If Studio is installed on a different machine than one you’ve already upgraded, run the installer on the machine where Studio is installed.

**Step 6.** From the newly upgraded Studio, upgrade the Site database. For details, see Upgrade the databases and the Site below.

**Step 7.** From the newly upgraded Studio, select Citrix Studio site-name in the navigation pane. Select the Common Tasks tab. Select Upgrade remaining Delivery Controllers.

**Step 8.** After completing the upgrade and confirming completion, close and then reopen Studio.

**Step 9.** In the Site Configuration section of the Common Tasks page, select Perform registration. Registering the Controllers makes them available to the Site.

**Step 10.** After you select Finish when the upgrade completes, you are offered the opportunity to enroll in the Citrix telemetry programs, which collect information about your deployment. That information is used to improve product quality, reliability, and performance.

**Step 11.** After upgrading components, the database, and the Site, test the newly-upgraded Site. From Studio, select Citrix Studio site-name in the navigation pane. Select the Common Tasks tab and then
select Test Site. These tests were run automatically after you upgraded the database, but you can run them again at any time.

Step 12. If you use Machine Creation Services and want to use upgraded VDAs: After you upgrade and test the deployment, update the VDA used in the master images (if you haven’t done that already). Update master images that use those VDAs. Then update machine catalogs that use those master images, and upgrade Delivery Groups that use those catalogs.

Note:
Steps 7 through 9 are optional during an upgrade, unless you are prompted for a Dbschema upgrade.

Upgrade the database and Site

After upgrading the core components and VDAs, use the newly upgraded Studio to initiate an automatic or manual database and Site upgrade.

- For an automatic database upgrade, the Studio user’s permissions must include the ability to update the SQL Server database schema (for example, the db_securityadmin or db_owner database role).
- If the Studio user does not have those permissions, initiating a manual database upgrade will generate scripts. The Studio user runs some of the scripts from Studio. The database administrator runs other scripts using a tool such as SQL Server Management Studio. If the SQL scripts are run manually, they should be run using either the SQLCMD utility or the SQL Management Studio in SQLCMD mode. Inaccurate errors may result otherwise.

Important: Citrix strongly recommends you back up the databases before upgrading, as described in CTX135207.

During a database upgrade, product services are disabled. During that time, Controllers cannot broker new connections for the Site, so plan carefully.

After the database upgrade completes and product services are enabled, Studio tests the environment and configuration, and then generates an HTML report. If problems are identified, you can restore the database backup. After resolving issues, you can upgrade the database again.

Upgrade the databases and Site automatically

Launch the newly upgraded Studio. After you choose to start the Site upgrade automatically and confirm that you are ready, the database and Site upgrade proceeds.
Upgrade the databases and Site manually

This process includes generating and running scripts.

**Step 1.** Launch the newly created Studio. After you choose to manually upgrade the Site, the wizard prompts to confirm that you have backed up the databases. Then, the wizard generates and displays the scripts and a checklist of upgrade steps.

**Step 2.** Run the following scripts in the order shown.

- **DisableServices.ps1**: PowerShell script to be run by the Studio user on a Controller to disable product services.
- **UpgradeSiteDatabase.sql**: SQL script to be run by the database administrator on the server containing the Site database.
- **UpgradeMonitorDatabase.sql**: SQL script to be run by the database administrator on the server containing the Monitor database.
- **UpgradeLoggingDatabase.sql**: SQL script to be run by the database administrator on the server containing the Configuration logging database. Run this script only if this database changes (for example, after applying a hotfix).
- **EnableServices.ps1**: PowerShell script to be run by the Studio user on a Controller to enable product services.

**Step 3.** After completing all the checklist tasks shown in the wizard, click **Finish upgrade**.

Dbschema upgrade

When you update your deployment to a new CU, several of your database schemas are upgraded. Consult the following table for information about which database schemas are being upgraded in the process:
### Definition of terms:

- **Site** = Site Datastore; Dbschema update is made to the Site Datastore.
- **Monitor** = Monitor Datastore; Dbschema update is made to the Monitor Datastore.
- **Config** = Configuration table; Desktop Studio version, License Server version, or both are updated in the Configuration table.

### SSL

February 19, 2019
Configuring a XenApp or XenDesktop Site to use the Secure Sockets Layer (SSL) security protocol includes the following procedures:

- Obtain, install, and register a server certificate on all Delivery Controllers, and configure a port with the SSL certificate. For details, see Install SSL server certificates on Controllers.

  Optionally, you can change the ports the Controller uses to listen for HTTP and HTTPS traffic.

- Enable SSL connections between users and Virtual Delivery Agents (VDAs) by completing the following tasks:
  - Configure SSL on the machines where the VDAs are installed. (For convenience, further references to machines where VDAs are installed are simply called “VDAs.”) You can use a PowerShell script supplied by Citrix, or configure it manually. For general information, see About SSL settings on VDAs. For details, see Configure SSL on a VDA using the PowerShell script and Manually configure SSL on a VDA.
  - Configure SSL in the Delivery Groups containing the VDAs by running a set of PowerShell cmdlets in Studio. For details, see Configure SSL on Delivery Groups.

Requirements and considerations:

- Enabling SSL connections between users and VDAs is valid only for XenApp 7.6 and XenDesktop 7.6 Sites, plus later supported releases.
- Configure SSL in the Delivery Groups and on the VDAs after you install components, create a Site, create Machine Catalogs, and create Delivery Groups.
- To configure SSL in the Delivery Groups, you must have permission to change Controller access rules; a Full Administrator has this permission.
- To configure SSL on the VDAs, you must be a Windows administrator on the machine where the VDA is installed.
- If you intend to configure SSL on VDAs that have been upgraded from earlier versions, uninstall any SSL relay software on those machines before upgrading them.
- The PowerShell script configures SSL on static VDAs; it does not configure SSL on pooled VDAs that are provisioned by Machine Creation Services or Provisioning Services, where the machine image resets on each restart.

For tasks that include working in the Windows registry:

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

For information about enabling SSL to the Site database, see CTX137556.
Install SSL server certificates on Controllers

For HTTPS, the XML Service supports SSL features through the use of server certificates, not client certificates. To obtain, install, and register a certificate on a Controller, and to configure a port with the SSL certificate:

- If the Controller has IIS installed, follow the guidance in https://technet.microsoft.com/en-us/library/cc771438%28v=ws.10%29.aspx.
- If the Controller does not have IIS installed, one method of configuring the certificate is:
     If you intend to use the PowerShell script to configure SSL on VDAs, and unless you intend on specifying the SSL certificate’s thumbprint, make sure the certificate is located in the Local Computer > Personal > Certificates area of the certificate store. If more than one certificate resides in that location, the first one found will be used.
  2. Configure a port with the certificate; see http://msdn.microsoft.com/en-us/library/ms733791%28v=vs.110%29.aspx.

Change HTTP or HTTPS ports

By default, the XML Service on the Controller listens on port 80 for HTTP traffic and port 443 for HTTPS traffic. Although you can use non-default ports, be aware of the security risks of exposing a Controller to untrusted networks. Deploying a standalone StoreFront server is preferable to changing the defaults.

To change the default HTTP or HTTPS ports used by the Controller, run the following command from Studio: BrokerService.exe -WIPORT <http-port> -WISSLPOR <https-port>

where <http-port> is the port number for HTTP traffic and <https-port> is the port number for HTTPS traffic.

Note: After changing a port, Studio might display a message about license compatibility and upgrading. To resolve the issue, re-register service instances using the following PowerShell cmdlet sequence:

```powershell
1. Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
2. XML_HTTPS | Unregister-ConfigRegisteredServiceInstance
3. Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
4. Register-ConfigServiceInstance
```
**Enforce HTTPS traffic only**

If you want the XML Service to ignore HTTP traffic, set the following registry value in HKLM\Software\Citrix\DesktopServer\ on the Controller and then restart the Broker Service.

To ignore HTTP traffic, set XmlServicesEnableNonSsl to 0.

There is a corresponding registry value to ignore HTTPS traffic: XmlServicesEnableSsl. Ensure that this is not set to 0.

**About SSL settings on VDAs**

When you configure SSL on VDAs, it changes permissions on the installed SSL certificate, giving the ICA Service read access to the certificate’s private key, and informing the ICA Service of the following:

- **Which certificate in the certificate store to use for SSL.**

- **Which TCP port number to use for SSL connections.**

  The Windows Firewall (if it is enabled) must be configured to allow incoming connection on this TCP port. This configuration is done for you when you use the PowerShell script.

- **Which versions of the SSL protocol to allow.**

  The supported SSL protocol versions follow a hierarchy (lowest to highest): SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. You specify the minimum allowed version; all protocol connections using that version or a higher version are allowed.

  For example, if you specify TLS 1.1 as the minimum version, then TLS 1.1 and TLS 1.2 protocol connections are allowed. If you specify SSL 3.0 as the minimum version, then connections for all the supported versions are allowed. If you specify TLS 1.2 as the minimum version, only TLS 1.2 connections are allowed.

- **Which SSL ciphers to allow.**

  A cipher suite is a list of common SSL ciphers. When a client connects and sends a list of supported SSL ciphers, the VDA matches one of the client’s ciphers with one of the ciphers in its configured cipher suite and accepts the connection. If the client sends a cipher that is not in the VDA’s cipher suite, the VDA rejects the connection.

  Three cipher suites are supported: GOV(ernment), COM(ercial), and ALL. The ciphers in those cipher suites depend on the Windows FIPS mode; see [http://support.microsoft.com/kb/811833](http://support.microsoft.com/kb/811833) for information about Windows FIPS mode. The following table lists the ciphers in each supported cipher suite.
A Delivery Group cannot have a mixture of some VDAs with SSL configured and some VDAs without SSL configured. When you configure SSL for a Delivery Group, you should have already configured SSL for all of the VDAs in that Delivery Group.

**Configure SSL on a VDA using the PowerShell script**

The Enable-VdaSSL.ps1 script enables or disables the SSL listener on a VDA. This script is available in the Support >Tools > SslSupport folder on the installation media.

When you enable SSL, the script disables all existing Windows Firewall rules for the specified TCP port before adding a new rule that allows the ICA Service to accept incoming connections only on the SSL TCP port. It also disables the Windows Firewall rules for:

- Citrix ICA (default: 1494)
- Citrix CGP (default: 2598)
- Citrix WebSocket (default: 8008)

The result is that users can connect only over SSL; they cannot use raw ICA, CGP, or WebSocket to connect.

The script contains the following syntax descriptions, plus additional examples; you can use a tool such as Notepad++ to review this information.
XenApp and XenDesktop 7.6 Long Term Service Release (LTSR)

You must specify either the –Enable or –Disable parameter; all other parameters are optional.

Syntax:

```
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Enable</td>
<td>Installs and enables the SSL listener on the VDA. Either this parameter or the –Disable parameter is required.</td>
</tr>
<tr>
<td>-Disable</td>
<td>Disables the SSL listener on the VDA. Either this parameter or the –Enable parameter is required. If you specify this parameter, no other parameters are valid.</td>
</tr>
<tr>
<td>–SSLPort &lt;port&gt;</td>
<td>SSL port. Default: 443</td>
</tr>
<tr>
<td>-SSLMinVersion &quot;&lt;min-ssl-version&gt;&quot;</td>
<td>Minimum SSL protocol version, enclosed in quotation marks. Valid values: “SSL_3.0”, “TLS_1.0”, “TLS_1.1”, and “TLS_1.2”. Default: “TLS_1.0”</td>
</tr>
<tr>
<td>-CertificateThumbPrint &quot;&lt;thumbprint&gt;&quot;</td>
<td>Thumbprint of the SSL certificate in the certificate store, enclosed in quotation marks. This parameter is generally used when the certificate store has multiple certificates; the script uses the thumbprint to select the certificate you want to use. Default: the first available certificate found in the Local Computer &gt; Personal &gt; Certificates area of the certificate store.</td>
</tr>
</tbody>
</table>

Examples:
The following script installs and enables the SSL listener, using default values for all optional parameters.

```
1 Enable-VdaSSL - Enable
```

The following script installs and enables the SSL listener, and specifies SSL port 400, the GOV cipher suite, and a minimum TLS 1.2 SSL protocol value.

```
1 Enable-VdaSSL - Enable
2 SSLPort 400
2 SSLCipherSuite "GOV"
2 SSLMinVersion "TLS_1.2"
```

The following script disables the SSL listener on the VDA.

```
1 Enable-VdaSSL - Disable
```

**Manually configure SSL on a VDA**

When configuring SSL on a VDA manually, you grant generic read access to the SSL certificate’s private key for the appropriate service on each VDA: NT SERVICE\PorticaService for a VDA for Windows Desktop OS, or NT SERVICE\TermService for a VDA for Windows Server OS. On the machine where the VDA is installed:

1. Launch the Microsoft Management Console (MMC): Start > Run > mmc.exe.
2. Add the Certificates snap-in to the MMC:
   a) Select File > Add/Remove Snap-in.
   b) Select Certificates and then click Add.
   c) When prompted with “This snap-in will always manage certificates for:” choose “Computer account” and then click Next.
   d) When prompted with “Select the computer you want this snap-in to manage” choose “Local computer” and then click Finish.
3. Under Certificates (Local Computer) > Personal > Certificates, right-click the certificate and then select All Tasks > Manage Private Keys.
4. The Access Control List Editor displays “Permissions for (FriendlyName) private keys” where (FriendlyName) is the name of your SSL certificate. Add one of the following services and give it Read access:
   • For a VDA for Windows Desktop OS, “PORTICASERVICE”
   • For a VDA for Windows Server OS, “TERMSERVICE”
5. Double-click the installed SSL certificate. In the certificate dialog, select the Details tab and then scroll to the bottom. Click Thumbprint.
6. Run regedit and go to HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.
a) Edit the SSL Thumbprint key and copy the value of the SSL certificate’s thumbprint into this binary value. You can safely ignore unknown items in the Edit Binary Value dialog box (such as ‘0000’ and special characters).
b) Edit the SSLEnabled key and change the DWORD value to 1. (To disable SSL later, change the DWORD value to 0.)
c) If you want to change the default settings (optional), use the following in the same registry path:
   • SSLPort DWORD – SSL port number. Default: 443.
   • SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Default: 2 (TLS 1.0).
   • SSLCipherSuite DWORD – 1 = GOV, 2 = COM, 3 = ALL. Default: 3 (ALL).
7. Ensure the SSL TCP port is open in the Windows Firewall if it is not the default 443. (When you create the inbound rule in Windows Firewall, make sure its properties have the “Allow the connection” and “Enabled” entries selected.)
8. Ensure that no other applications or services (such as IIS) are using the SSL TCP port.
9. For VDAs for Windows Server OS, restart the machine for the changes to take effect. (You do not need to restart machines containing VDAs for Windows Desktop OS.)

**Configure SSL on Delivery Groups**

Complete this procedure for each Delivery Group that contains VDAs you have configured for SSL connections.

1. From Studio, open the PowerShell console.
2. Run `asnp Citrix.*` to load the Citrix product cmdlets.

```plaintext
Run Get-BrokerAccessPolicyRule
-DesktopGroupName '<delivery-group-name>'
Set-BrokerAccessPolicyRule
-HdxSslEnabled $true.
```
3. where `<delivery-group-name>` is the name of the Delivery Group containing VDAs.
4. Run `Set-BrokerSite –DnsResolutionEnabled $true`.

**Troubleshooting**

If a connection error occurs, check the VDA’s system event log.

When using Receiver for Windows, if you receive a connection error (such as 1030) that indicates an SSL error, disable Desktop Viewer and then try connecting again; although the connection will still fail,
an explanation of the underlying SSL issue might be provided (for example, you specified an incorrect template when requesting a certificate from the certificate authority).
Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2018 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).