Waters

THE SCIENCE OF WHAT'S POSSIBLE.™

Empower 3 Service Release 3 Hotfix 3

Release Notes

715008442DD
Version / Revision A

General information

Copyright notice

The information in this document is subject to change without notice and should not be construed as a commitment by Waters Corporation. Waters Corporation assumes no responsibility for any errors that may appear in this document. This document is believed to be complete and accurate at the time of publication. In no event shall Waters Corporation be liable for incidental or consequential damages in connection with, or arising from, its use. For the most recent revision of this document, consult the Waters website (www.waters.com).

Trademarks

Citrix® is a registered trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Empower™ is a trademark of Waters Corporation.

LAC/E™ is a trademark of Waters Corporation.

Linux® is a registered trademark of Linus Torvalds.

NuGenesis™ is a trademark of Waters Corporation.

Oracle® is a registered trademark of Oracle Corporation and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, Inc.

THE SCIENCE OF WHAT'S POSSIBLE™ is a trademark of Waters Corporation.

Waters™ is a trademark of Waters Corporation.

Windows® is a registered trademark of Microsoft Corporation in the US and/or other countries.

XenApp® is a trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

All other trademarks are property of their respective owners.

About these release notes

This document contains information about the features and functions introduced, changed, or removed in this version of the product. It contains a list of major feature changes as well as descriptions of known defects, resolved defects, and observed product behaviors (concessions) that Waters deems of importance to customers. This document does not include:

- An exhaustive list of all changes to this version of the product
- Descriptions of defects that were not known to Waters at the time of the product's release
- Descriptions of defects that cannot be reproduced by Waters
- Information about customer requests for enhancements to the product
- Specific details of changes to proprietary aspects of product components, features, computational algorithms, and software code

The changes listed in this document are relative to the previous version of the product. If you are updating an older version of the product, review the release notes for all the intervening versions to ensure that you understand the cumulative impact of the product changes.

Carefully review the information in this document before the product is installed. If you have questions about how installing this product might affect your environment or if you need more information about this product, contact your Waters representative.

Contacting Waters

Contact Waters with technical questions regarding the use, transportation, removal, or disposal of any Waters product. You can reach us through the Internet, telephone, fax, or conventional mail.

Contact method	Information
www.waters.com	The Waters website includes contact information for Waters locations worldwide.
iRequest	iRequest is a secure Web service form that allows you to request support and service for Waters instruments and software or to schedule a planned service activity. These types of support and services may be included as part of your maintenance plan or support plan. You may be charged for the requested service if you do not have appropriate plan coverage for your product. **Note:** In areas managed by authorized distributors, iRequest may not be available.

Contact method	Information
	Contact your local distributor for more information.
Local office contact information	For worldwide locations, telephone, fax, and conventional mail information is available at the Local Offices website.
Corporate contact information	Waters Corporation Global Support Services 34 Maple Street Milford, MA 01757 USA From the USA or Canada, phone 800-252-4752 or fax 508-872-1990.

Updated information

Refer to the Waters website (www.waters.com) and click **Support** > **Support Documents and Downloads** for updates to this document.

Obtaining Waters software and software updates

To digitally obtain the software application you purchased, use the Waters Digital Software Delivery and License Entitlement platform. With an active Waters Software Maintenance Plan, the platform gives you email notifications of and immediate access to newly released software, including updates and hotfixes. This delivery platform allows you to securely search and share software entitlements, instrument drivers, release notes, and documentation.

To access the Digital Software Delivery and License Entitlement platform, contact the designated Software Manager for your organization. The Software Manager is typically a system administrator or someone responsible for implementing software and activating licenses, and they are the person responsible for the Waters digital entitlements (software and licenses) within your organization. From within the platform, the Software Manager can securely manage and grant access to software entitlements to others within your organization, providing organizational control of your software assets.

Access the software delivery and license entitlement platform through your waters.com user profile at **Waters.com** > **My Account [Hello, *username*]** > **Profile** > **Download Software Entitlements**.

If you have not yet arranged for access to this platform, send your Software Manager's contact information to Waters at customer_communication@waters.com, or work with your Waters sales representative to begin the secure onboarding process.

Table of contents

Empower 3 Service Release 3 Hotfix 3

Compliance recommendations

Any time you install, change, or uninstall software or system modules in a regulated environment, Waters recommends that you follow your organization's approved change control procedure.

You should assess the impact of the changes described in the release notes on the qualification status and validation for the intended use of your system, including any impact on personnel, methods, laboratory workflows, or connected equipment, and scale your activities accordingly.

Antivirus considerations

Some real-time virus scanners mistake normal data acquisition and instrument control for virus activity, and thus interfere with proper operations. Full-system scans and live updates can be network-intensive, disk-intensive, and CPU-intensive, and they can also interfere with normal data acquisition. Schedule scans and updates for idle times when data acquisition does not occur.

Certain antivirus program features such as "intrusion prevention", "tamper protection", and "heuristic analysis" can also interfere with normal operation. If you observe issues with the software, review and verify the antivirus logs. It may be necessary to white-list any affected components.

Empower installations

For Empower software installations, exclude the Empower installation folder (usually *C:\Empower*) and its sub-folders.

System and software requirements

Empower 3 Service Release 3 Hotfix 3 (Empower 3 SR3 HF3) software supports Windows 7 Service Pack 1 (SP1) (Personal, Acquisition Client, and LAC/E device), Windows 10 Professional and Enterprise (Personal, Acquisition Client, and LAC/E device), Windows Server 2008 R2 SP1 (Standard and Enterprise), and Windows Server 2012 R2 (Standard). Also, Empower 3 SR3 HF3 supports Amazon Web Services (AWS) 2012 R2 Server AMI, AWS WorkSpace 2008 R2 Datacenter Server with Windows 7 Experience, and AWS Windows 2016 Server with Windows 10 Experience.

Note: Support includes English, Japanese, Simplified Chinese, and Korean distributions of Empower software.

Specifically, Empower 3 SR3 HF3 supports these platforms and operating systems:

Platform[a]	Operating systems
Personal workstation or Client or LAC/E device	• Windows 7 Professional or Enterprise with SP1, 64-bit • Windows 10 Professional or Enterprise, 64-bit
Database server	• Windows Server 2008 R2, Enterprise or Standard Edition with SP1, 64-bit • Windows Server 2012 R2 Standard Edition, 64-bit • Red Hat Enterprise Linux Server 6.8 • Red Hat Enterprise Linux Server 7.4 • Red Hat Enterprise Linux Server 7.5
File server	• Windows Server 2012 R2 Standard Edition, 64-bit • Windows Server 2016 Datacenter and Standard
Citrix Server XenApp 7.6	• Windows Server 2008 R2, Enterprise or Standard Edition with SP1, 64-bit • Windows Server 2012 R2 Standard Edition, 64-bit
Citrix Server XenApp 7.15 LTSR CU2	• Windows Server 2016 Datacenter and Standard
LAC/E device	• Configuration 12 is supported if the operating system was upgraded to Windows 7 and the RAM was increased to 4GB. • Configuration 13 is supported if the operating system was upgraded to Windows 7 and the RAM was increased to 4GB. • Configuration 14 is supported with Windows 7 Professional 64-bit for Windows Embedded Enterprise, SP1 (English and Japanese).

Platform[a]	Operating systems
	• Configuration 15 is supported with Windows 7 Professional (64-bit, for Windows Embedded Enterprise) SP1 and Windows 10 Enterprise LTSB (Long Term Service Branch) Build 1607, 64-bit. • Configuration 16 is supported with Windows 7 Professional (64-bit, for Windows Embedded Enterprise) SP1 and Windows 10 Enterprise LTSB Build 1607, 64-bit.

a. All platforms run on Oracle version 12.1.0.2.0.

Note: Solaris 10 is no longer supported, starting with Empower 3 SR3.

See also: The *Empower 3 Installation, Configuration, and Upgrade Guide* (715005266).

In addition to testing on the platforms listed above, Empower 3 SR3 HF3 was also tested in a VMware vSphere v6 environment.

NuGenesis SDMS and NuGenesis LMS compatibility

Empower 3 SR3 HF3 supports the same compatibility matrix as the Empower 3 Service Release 3 release.

See the *Empower 3 Service Release 3 Release Notes* (716005266) for details.

Driver compatibility

Empower 3 SR3 HF3 supports Driver Pack 2017 Release 2 on Windows 7 only, and Driver Pack 2018 Release 1 and Driver Pack 2019 Release 1 on both Windows 7 and Windows 10.

See also: For information on the drivers, refer to *Waters Driver Pack 2017 Release 2 Release Notes* (716005259), *Waters Driver Pack 2018 Release 1 Release Notes* (716005632), or *Waters Driver Pack 2019 Release 1 Release Notes* (716006125).

Deployment notes

Before you install Empower 3 Service Release 3 Hotfix 3

Before you install Empower 3 SR3 HF3, back up all Empower software projects, library information, and databases, and restart the enterprise or personal computer.

Upgrade path: You must upgrade to Empower 3 SR3 HF3 from Empower 3 Service Release 3 Hotfix 2 (Empower 3 SR3 HF2). The complete upgrade path is Empower 3 SR3 > Empower 3 Service Release 3 Hotfix 1 (Empower 3 SR3 HF1) > Empower 3 SR3 HF2 > Empower 3 SR3 HF3. If you are currently using a version of Empower other than Empower 3 SR3, you must upgrade according to the upgrade path.

See also: The *Empower 3 Installation, Configuration, and Upgrade Guide* (715005266) for complete installation instructions.

Install Empower 3 Service Release 3 Hotfix 3

You can install Empower 3 SR3 HF3 software after downloading it from the Waters Digital Software Delivery and License Entitlement platform as described in the section Obtaining Waters software and software updates (Page iv).

Restriction: You cannot roll back or remove an Empower 3 SR3 HF3 installation. If you want to uninstall Empower 3 SR3 HF3, you must uninstall Empower software.

Requirements:

- You must upgrade to Empower 3 SR3 HF3 from Empower 3 SR3 HF2. The complete upgrade path is Empower 3 SR3 > Empower 3 SR3 HF1 > Empower 3 SR3 HF2 > Empower 3 SR3 HF3.
- If you are currently using a version of Empower prior to Empower 3 SR3 HF2, refer to the *Empower 3 Service Release 3 Release Notes* (716005266) and to the *Empower 3 Service Release 3 Hotfix 2 Release Notes* (715007439) for the upgrade path from your version of Empower software.
- You must have local administrator privileges to install Empower 3 SR3 HF3.

You can install Empower 3 SR3 HF3 in the following ways, depending on your system configuration:

Computer configuration	Installation process
Single computer running a supported Windows operating system	• Installation wizard • Silent installation (Command line interface)
Multiple computers: Clients, LAC/E devices, or Citrix servers	• Installation wizard • Silent installation (Command line interface) • Push installation (PsExec utility)

Note:

- Empower 3 SR3 HF3 should install on an Empower node for personal workstations, and on all nodes in workgroup or enterprise environments for servers, LACEs, clients, and acquisition clients.
- If you install Empower 3 SR3 HF3 on an Empower node, the configuration is valid only for that node. If your network includes multiple Empower nodes, you must perform the following procedure on each node individually.

To install Empower 3 SR3 HF3 on an Empower node:

1. In Windows Explorer, browse to the folder containing the *Empower3SR3Hotfix3Setup.exe* file and double-click the *Empower3SR3Hotfix3Setup.exe* file.

   Requirement: Ensure that you are logged in to the computer as a local administrator. If necessary, right-click the *Empower3SR3Hotfix3Setup.exe* file and select **Run as Administrator**.
2. Follow all the prompts to complete the installation.

   Note: If you encounter issues installing Empower 3 SR3 HF3 due to a Verify Files issue, contact your local Waters Support organization.
3. After the installation finishes, restart the computer.
4. Log on to the computer, and then log on to Empower software.

Performing a silent installation

You can install Empower 3 SR3 HF3 by using command line options.

To perform a silent installation from a command line:

1. In a Command Prompt window, if required, change to the directory that contains the file *Empower3SR3Hotfix3Setup.exe*.
2. At the command prompt, specify the following command, along with the required line options and any other options you want to use, as listed in the following table:

   ```
   Empower3SR3Hotfix3Setup.exe /s /v" /qn"
   ```

Full command line:

```
Empower3SR3Hotfix3Setup.exe /s /v"WAT_RESTART=NO
WAT_LOG_FILE_NETWORK_LOCATION="<SHARE>\e3_Logs" /qn"
```

Command line with language selection:

```
Empower3SR3Hotfix3Setup.exe /s /L1033 /v"WAT_RESTART=NO
WAT_LOG_FILE_NETWORK_LOCATION="<SHARE>\e3_Logs" /qn"
```

Table 1: Command line options

Option	Description	Required	Default value
/s	Silent mode	Yes	
/L	Installer language: • L1033 is English • L1041 is Japanese • L1042 is Korean • L2052 is Chinese	Yes	
/v	Installer arguments. Passes one or more command line options to notification services.msi. When including multiple command line options, enclose them in quotation marks. **Rule:** Do not include a space between the /v and the command line option.	Yes	
/qn	Installs the software without displaying the user interface.	Yes	
WAT_LOG_FILE_NETWORK_LOCATION	Destination share for the installation log. This share must be writable by everyone.	No	None
WAT_RESTART	Restart system.	No	Do not restart

The WAT_LOG_FILE_NETWORK_LOCATION option copies the installation log to the network share. If the installation is successful, the name of the log file is *computername_datetime_empower3.log* (for example, *AS-27_2022-12-5_12-55-17-235_Empower3.log*). If the share is not accessible, the installation log file is created in the local Windows directory. If you do not supply the WAT_LOG_FILE_NETWORK_LOCATION option, the log is created locally.

3. After the installation finishes, restart the computer.
4. Log on to the computer.

5. Log on to Empower software.

Performing a push installation

When installing Empower 3 SR3 HF3 on multiple computers (push installation), use the PsExec utility. You can download the latest version from http://technet.microsoft.com.

Requirements:

- Install the PsExec utility on the system from which you execute the push installation. To install this utility, copy it to any file path.
- You must have administrator privileges for each client or LAC/E device.
- You must use a domain user who is part of the local administrator group.

To perform a push installation of Empower 3 SR3 HF3:

1. Create a text file and, within it, specify the name or IP address of each client computer or LAC/E device on a separate line, and then save the file.
2. Run the following commands from a Command prompt or create a batch file containing the Empower 3 SR3 HF3 upgrade push install options:

Using the administrator account:

```
PsExec @<PATH_A>\File.txt -u DOMAIN\USER -p PASSWORD -s
-d <PATH_B>\Empower3SR3Hotfix3Setup.exe /s /v" WAT_RESTART=NO
WAT_LOG_FILE_NETWORK_LOCATION="<PATH_C>" /qn"
```

Selecting a language:

```
PsExec @<PATH_A>\File.txt -u DOMAIN\USER -p PASSWORD -s -d
<PATH_B>\Empower3SR3Hotfix3Setup.exe /s /L1033 /v" WAT_RESTART=NO
WAT_LOG_FILE_NETWORK_LOCATION="<PATH_C>" /qn"
```

PsExec command line options	Definition	Required
PATH_A	Path to the text file that contains the names or IP addresses of the clients or LAC/E devices	Yes
File	Name of the text file that contains the names or specified IP addresses	Yes
PATH_B	Path to the Empower 3 SR3 media should be network share	Yes
PATH_C	Path to copy the installation log located on a network share	Yes

PsExec command line options	Definition	Required
-p	Password	Yes
-u	Username	Yes
-d	Do not wait for process to terminate (non-interactive); this command launches installation on multiple machines simultaneously	Yes

3. After the installation finishes, restart the computer.
4. Log on to the computer, and then log on to Empower software.

Push installation of Empower 3 Service Release 3 Hotfix 3 on multiple Empower Citrix servers

When installing Empower 3 SR3 HF3 on multiple Empower Citrix servers, use the PsExec utility and the Waters command line interface and options. You can type the commands in a command window or in a batch file.

Requirement: Confirm that the default admin$ share is enabled on all Empower Citrix servers on which you plan to install Empower 3 SR3 HF3.

To perform a push installation of Empower 3 SR3 HF3 on multiple Empower Citrix servers:

1. From the following website, download the currently available version of the PsExec utility into any folder on a host machine: http://technet.microsoft.com

   Requirement: To perform a push installation, you must have a domain user with administrator privileges on each Empower Citrix server.
2. Using a text editor, create a text file (such as *filename.txt*) and, within it, specify the name or IP address of each Empower Citrix server on a separate line, and then save the file.
3. To set the mode to install, use a text editor to create a batch file (such as *PushCitrix.bat*). Within this file, specify the following commands:

```
change user /install
PsExec @<PATH_A>\File.txt -u DOMAIN\USER -p PASSWORD -s -d
<PATH_B>\Empower3SR3Hotfix3Setup.exe /s /v" WAT_RESTART=NO
WAT_LOG_FILE_NETWORK_LOCATION="<PATH_C>" /qn"
```

- For *path_to_Empower_media*, specify a valid path to the Empower 3 SR3 HF3 software. This path must be accessible by the Empower Citrix server.
- For *path_to_log_file*, specify a valid path to the location where the installation log files will be stored. This location must be on a share that is write-accessible to the domain users who will perform the push install and who have write access to the share.

Tip: The above is an example batch file. The Restart command and log file location are optional. If Restart is not included in the command line, users are prompted to restart the computer after installation. If the file location is not specified, the log file is created locally, wherever Empower software is installed. A message appears to notify users that the file was created.

4. On the host computer, run the batch file using the following command line syntax:

```
PsExec @<PATH_A>\File.txt -u DOMAIN\USER -p PASSWORD -s -d
<PATH_B>\Empower3SR3Hotfix3Setup.exe /s /L1033 /v" WAT_RESTART=NO
WAT_LOG_FILE_NETWORK_LOCATION="<PATH_C>" /qn"
```

   - For *path_to_filename.txt*, specify a valid path to the text file on the host machine that contains the Empower Citrix server names.
   - For *path_to_batch_file*, specify a valid path to the location of the share that contains the batch file.
5. Log on to each Empower Citrix server.
6. Log on to Empower software.

Verify the Empower 3 Service Release 3 installation

You can verify that Empower 3 SR3 HF3 installed successfully by running the **Verify Files** utility.

To verify your Empower installation:

Click **Start** > **All Programs or All Apps** > **Empower** > **Verify Files**.

To view the *checksum.txt* file for the Empower 3 SR3 HF3 installation:

From Windows Explorer, navigate to the *\Empower\Script* directory, and then double-click the *checksum.txt* file. Locate the file with the time stamp that contains the Empower 3 SR3 HF3 installation time in the file name.

To confirm that Empower 3 SR3 HF3 is installed on the computer:

Click **Start** > **All Programs** > **Empower** > **Empower Installation Log** and search for lines similar to these:

```
=== Logging Started: 29-11-2022 12:19:53 - Empower 3 Service Release
3 Hotfix 3 ===
******* Product: Empower 3 Service Release 3 Hotfix 3
```

```
******* Mode: Silent
******* CommandLine:  WAT_RESTART=Yes WAT_LOG_FILE_NETWORK_LOCATION=\
\EMP3WIN10VM3\PushInstall\EmpowerLog
[12:19:53]: Empower 3 Service Release 3 Hotfix 3 Installer Setup was
initialized.
[12:21:01]: The setup has successfully completed installing Empower
3 Service Release 3 Hotfix 3 on this computer.
[12:21:01]: Empower 3 Service Release 3 Hotfix 3 Installer has
completed.
[12:21:01]: User has requested to restart the system.
=== Logging Stopped: 29-11-2022 12:21:01 ===
```

Empower Cloud deployment guidelines

Waters supports installing the Empower software in an Amazon Web Services (AWS) cloud environment. Specific policies control the AWS services required to run the Empower services in the cloud.

For a list of all available AWS policies, see the AWS website. For additional information about using Empower software in an AWS cloud environment and the services used and policies accessed while deploying Empower software in an AWS environment, see the *Empower Cloud Release Notes* (716005296), the *Empower Cloud Deployment Guide*, and the *Empower 3 Service Release 3 Release Notes* (716005266).

Note: Empower software installed in an AWS cloud environment functions the same as Empower software installed in an on-premise (non-cloud) environment.

Issues resolved in this release

This section lists the problems resolved in this release. The numbers identify issues that Waters personnel monitor within a system change request tracking tool.

INFEMP-27259 (CRI-1775)

Previously, in Citrix environments where the System Policy **Save Report (as PDF) after Signoff** was enabled, the creation of the PDF report could fail, resulting in an `Unable to store the PDF file in the database for result sign off ID: xxxx` error message. This issue occurred more frequently with large reports.

Signoff Results now works consistently in Citrix environments with larger PDF reports. The PDF is successfully created and stored in the Empower database.

INFEMP-27260 (CRI-2484, CRI-2679)

Previously, a Channel Status could be set to Data Incomplete and the Injection Status was Complete; however, the data was available, although it should not be, and the Verify Incomplete Data option was unavailable, although it should be.

Now, if a Channel Status is Data Incomplete, the acquisition data is not available, but the Verify Incomplete Data option is available and, after the channel is verified as complete, the status changes to Verified as Complete and the action is recorded in the Project Audit Trail.

INFEMP-27267 (CRI-2094)

Previously, in Citrix environments, when you saved a PDF copy of a report generated in Report Publisher to the destination folder, the PDF took longer to save than in previous versions of Empower software.

Now, the Microsoft Print to PDF driver replaces the Waters UNIFY Printer in Empower software and the time to save a PDF report to the destination folder in Citrix environments is reduced.

Known issues in this release

At the time of this product's release, there were no related known issues requiring documentation.

Program files modified in this release

Program files

The following program files in the *Empower\Bin* directory were modified for Empower 3 SR3 HF3.

File name	Description	File version	Product version
Mil0.dll	Contains base objects that implement database connection, security, user and user type objects, and others	7.0.3471.913	7,0,3471,913.3
Mil1.dll	Contains base objects that implement higher-level objects such as methods, results, and others	7.0.3471.913	7,0,3471,913.3

File name	Description	File version	Product version
Mil2.dll	Contains base objects that implement higher-level objects including data processing, integration, calibration, and others	7.0.3471.913	7,0,3471,913.3

Test configurations

This application update was tested on the following system configurations.

Empower Server

Windows Server 2008 R2 Standard

Microsoft Windows Version

6.1.7601 SP1 Build 7601

Microsoft Windows Hotfixes:

KB981391, KB981392, KB977236, KB981111, KB977238, KB2849697, KB2849696, KB2841134, KB977239, KB2670838, KB2830477, KB2592687, KB981390, KB2386667, KB2425227, KB2446710, KB2479943, KB2484033, KB2488113, KB2492386, KB2497640, KB2503665, KB2505438, KB2506014, KB2506212, KB2506223, KB2506928, KB2507618, KB2508272, KB2508429, KB2509553, KB2510531, KB2511250, KB2511455, KB2515325, KB2518869, KB2522422, KB2524375, KB2529073, KB2533552, KB2534366, KB2536275, KB2536276, KB2539635, KB2541014, KB2544893, KB2545698, KB2547666, KB2552343, KB2556532, KB2560656, KB2563227, KB2564958, KB2567680, KB2570947, KB2572077, KB2574819, KB2584146, KB2585542, KB2588516, KB2603229, KB2604115, KB2607047, KB2608658, KB2618451, KB2620704, KB2620712, KB2621440, KB2631813, KB2633873, KB2633952, KB2636573, KB2639308, KB2639417, KB2640148, KB2641653, KB2641690, KB2643719, KB2644615, KB2645640, KB2647518, KB2647753, KB2653956, KB2654428, KB2655992, KB2656356, KB2656373, KB2658846, KB2659262, KB2660075, KB2660649, KB2661254, KB2665364, KB2667402, KB2676562, KB2679255, KB2685811, KB2685813, KB2685939, KB2686831, KB2688338, KB2690533, KB2691442, KB2695962, KB2698365, KB2699779, KB2705219, KB2709630, KB2709981, KB2712808, KB2718704, KB2719857, KB2719985, KB2724197, KB2726535, KB2727528, KB2729094, KB2729452, KB2731771, KB2731847, KB2732059, KB2735855, KB2736233, KB2736422, KB2739159, KB2741355, KB2742599, KB2743555, KB2749655, KB2750841, KB2753842, KB2756822, KB2757638, KB2758857, KB2761217, KB2762895, KB2763523, KB2765809, KB2769369, KB2770660, KB2778344, KB2778930, KB2779562, KB2785220, KB2786081, KB2786400, KB2789645, KB2790113,

KB2790655, KB2791765, KB2798162, KB2799494, KB2800095, KB2803821, KB2804579, KB2807986, KB2808679, KB2813170, KB2813347, KB2813430, KB2820197, KB2820331, KB2829361, KB2830290, KB2833946, KB2834140, KB2834886, KB2835361, KB2835364, KB2836502, KB2836943, KB2839894, KB2840149, KB2840631, KB2843630, KB2844286, KB2845187, KB2846960, KB2847077, KB2847311, KB2847927, KB2849470, KB2852386, KB2853952, KB2857650, KB2861698, KB2861855, KB2862152, KB2862330, KB2862335, KB2862966, KB2862973, KB2863058, KB2863240, KB2864058, KB2864202, KB2868038, KB2868116, KB2868623, KB2868626, KB2868725, KB2871997, KB2872339, KB2875783, KB2876284, KB2876315, KB2876331, KB2882822, KB2883150, KB2884256, KB2887069, KB2888049, KB2891804, KB2892074, KB2893294, KB2893519, KB2893984, KB2894844, KB2898857, KB2900986, KB2901112, KB2904266, KB2908783, KB2911501, KB2912390, KB2913152, KB2913431, KB2913602, KB2916036, KB2918614, KB2919469, KB2922229, KB2923545, KB2926765, KB2928562, KB2929733, KB2929755, KB2929961, KB2930275, KB2931356, KB2937610, KB2939576, KB2943357, KB2957189, KB2957503, KB2957509, KB2961072, KB2966583, KB2968294, KB2970228, KB2971850, KB2972100, KB2972211, KB2972280, KB2973201, KB2973337, KB2973351, KB2976897, KB2977292, KB2977728, KB2978092 KB2978120, KB2978668, KB2979570, KB2980245, KB2981580, KB2984972, KB2984981, KB2985461, KB2987107, KB2990214, KB2991963, KB2992611, KB2993651, KB2993958, KB2994023, KB2998527, KB3000483, KB3002657, KB3002885, KB3003743, KB3004361, KB3004375, KB3004394, KB3005607, KB3006121, KB3006137, KB3006226, KB3006625, KB3008627, KB3009736, KB3010788, KB3011780, KB3013126, KB3013410, KB3013455, KB3013531, KB3014029, KB3014406, KB3018238, KB3019215, KB3020338, KB3020369, KB3020370, KB3020388, KB3021674, KB3022345, KB3022777, KB3023215, KB3023562, KB3029944, KB3030377, KB3031432, KB3032323, KB3032655, KB3033889, KB3033890, KB3033929, KB3034344, KB3035126, KB3035131, KB3035132, KB3037574, KB3039066, KB3040272, KB3042058, KB3042553, KB3045171, KB3045645, KB3045685, KB3045999, KB3046002, KB3046017, KB3046049, KB3046269, KB3046306, KB3046482, KB3048761, KB3050265, KB3051768, KB3054205, KB3054476, KB3055642, KB3057154, KB3057839, KB3059317, KB3060716, KB3061518, KB3063858, KB3064209, KB3065979, KB3065987, KB3067505, KB3067903, KB3068457, KB3068708, KB3069392, KB3070102, KB3070738, KB3071756, KB3072305, KB3072595, KB3072630, KB3072633, KB3074543, KB3075226, KB3075249, KB3075851, KB3076895, KB3076949, KB3077657, KB3077715, KB3078601, KB3078667, KB3079757, KB3080079, KB3080149, KB3080446, KB3084135, KB3086255, KB3087039, KB3092601, KB3092627, KB3097966, KB3097989, KB3101722, KB3102429, KB3107998, KB3108371, KB3108381, KB3108664, KB3108670, KB3109094, KB3109103, KB3109560, KB3110329, KB3112148, KB3115858, KB3118401, KB3121255, KB3122648, KB3123479, KB3124001, KB3124280, KB3126587, KB3126593, KB3127220, KB3133043, KB3133977, KB3135983, KB3137061, KB3138378, KB3138612, KB3138901, KB3138910, KB3138962, KB3139398, KB3139852, KB3139914, KB3139923, KB3139940, KB3140245, KB3140410, KB3140735, KB3142024, KB3145739, KB3146706, KB3146963, KB3147071, KB3149090, KB3153171, KB3153199, KB3153731, KB3156013, KB3156016, KB3156017, KB3156019, KB3156417, KB3159398, KB3161561, KB3161949, KB3161958, KB3163245, KB3164033, KB3164035, KB3170455, KB3172605, KB3177186, KB3177467, KB3179573, KB3181988, KB3182203, KB3184122, KB3185319, KB3185911, KB3210131, KB4014504, KB4014579, KB4014596, KB4015193, KB4019990, KB4020322, KB4022722, KB4025337, KB4034679, KB4038779, KB4040966, KB4040980, KB4041678, KB4047206,

KB4048960, KB4049068, KB4054521, KB4093108, KB4095514, KB4103712, KB4130978, KB4284867, KB4338423, KB4338612, KB4338823, KB4339093, KB4339284, KB4343205, KB4343899, KB4344177, KB4457008, KB4457044, KB4468323, KB4474419, KB4480063, KB4483187, KB4483483, B4486459, KB4486564, KB4489885, KB4490128, KB4493448, KB4495606, KB4495612, KB4499175, KB4501226, KB4503269, KB4506976, KB4507456, KB4507704, KB976902, KB976932, KB982018, KB4480955

Windows Server 2012 R2 Standard

Microsoft Windows Version

6.3.9600 N/A Build 9600

Microsoft Windows Hotfixes:

KB2868626, KB2883200, KB2887595, KB2894852, KB2894856, KB2896496, KB2903939, KB2911106, KB2919355, KB2919394, KB2919442, KB2920189, KB2928680, KB2934520, KB2938066, KB2954879, KB2955164, KB2959626, KB2965500, KB2966826, KB2966828, KB2967917, KB2968296, KB2971203, KB2972103, KB2973448, KB2975061, KB2975719, KB2976627, KB2984006, KB2989930, KB2993100, KB2995004, KB2995388, KB2996799, KB2998174, KB2999226, KB3000483, KB3000850, KB3003057, KB3004545, KB3012199, KB3012235, KB3012702, KB3013172, KB3013531, KB3013538, KB3013769, KB3013791, KB3013816, KB3014442, KB3015696, KB3018133, KB3019978, KB3021910, KB3021952, KB3023219, KB3023266, KB3024751, KB3024755, KB3030947, KB3032359, KB3033446, KB3036612, KB3037576, KB3038002, KB3042085, KB3044374, KB3044673, KB3045634, KB3045685, KB3045717, KB3045719, KB3045999, KB3046017, KB3046737, KB3050267, KB3054169, KB3054203, KB3054256, KB3054464, KB3055323, KB3058515, KB3059317, KB3060681, KB3060793, KB3061512, KB3063843, KB3064209, KB3065822, KB3065988, KB3068708, KB3071756, KB3072307, KB3074228, KB3074545, KB3075853, KB3076949, KB3077715, KB3078071, KB3078405, KB3080149, KB3083325, KB3083711, KB3084135, KB3084905, KB3086255, KB3087038, KB3087040, KB3087137, KB3087916, KB3089023, KB3091297, KB3093983, KB3094486, KB3097992, KB3099406, KB3099834, KB3100473, KB3102429, KB3103616, KB3103696, KB3103709, KB3109103, KB3109560, KB3109976, KB3110329, KB3115224, KB3118401, KB3121261, KB3123245, KB3126434, KB3126587, KB3127222, KB3133043, KB3133690, KB3134179, KB3134815, KB3137728, KB3138378, KB3138602, KB3138615, KB3138910, KB3138962, KB3139398, KB3139914, KB3140219, KB3140234, KB3145384, KB3145432, KB3146604, KB3146723, KB3146751, KB3147071, KB3148851, KB3154070, KB3156059, KB3157993, KB3159398, KB3160005, KB3161949, KB3162835, KB3163207, KB3172614, KB3172729, KB3173424, KB3175024, KB3178539, KB3179574, KB3185319, KB3192392, KB3197873, KB3205400, KB3210137, KB3214628, KB4033428, KB4040974, KB4040981, KB4054566, KB4095517, KB4338415, KB4338419, KB4338424, KB4338600, KB4338605, KB4338832, KB4339284, KB4343888, KB4344166, KB4344178, KB4457034, KB4457045, KB4457143, KB4459935, KB4459941, KB4462901, KB4462930, KB4462941, KB4462949, KB4467694, KB4467703, KB4468323, KB4486105, KB4486459, KB4490128, KB4495608, KB4495624, KB4501226, KB4535680, KB4569768, KB4576486, KB4577586, KB4578953, KB4580325, KB4601058, KB4601275, KB5001403,

KB5001845, KB5001850, KB5003681, KB5004285, KB5004958, KB5005106, KB5005627, KB5006729, KB5007255, KB5008285, KB5009595, KB5010395, KB5011560, KB5012144, KB5012152, KB5012639, KB5013616, KB5013621, KB5014001, KB5014746, KB5015877, KB5016268, KB5016683, KB5017365, KB5018476, KB5019958, KB5020010, KB5020608, KB5020620, KB5020023, KB2959936, KB2928120, KB2933826, KB2938772, KB2949621, KB2966407, KB2972213, KB2973114, KB2973351, KB2977629, KB2977765, KB2978122, KB2978126, KB2987107, KB2989647, KB3004365, KB3004361, KB3022777, KB3023222, KB3029603, KB3030377, KB3031044, KB3035126, KB3037579, KB3037924, KB3041857, KB3045685, KB3045755, KB3045992, KB3048043, KB3055343, KB3055642, KB3059316, KB3074548, KB3075220, KB3078676, KB3080042, KB3082089, KB3083992, KB3087041, KB3092601, KB3092627, KB3095701, KB3096433, KB3097997, KB3098779, KB3100956, KB3102467, KB3102483, KB3112148, KB3112336, KB3121255, KB3121461, KB3121918, KB3122651, KB3122654, KB3123242, KB3124275, KB3125424, KB3126033, KB3126434, KB3126587, KB3126593, KB3127222, KB3127226, KB3128650, KB3132372, KB3133043, KB3133431, KB3133681, KB3133690, KB3133924, KB3134179, KB3134815, KB3135456, KB3135985, KB3135994, KB3136019, KB3137061, KB3137725, KB3137728, KB3138378, KB3138602, KB3138615, KB3138910, KB3138962, KB3139164, KB3139398, KB3139914, KB3140219, KB3140234, KB3142026, KB3142030, KB3145384, KB3145432, KB3146604, KB3146723, KB3146751, KB3146963, KB3147071, KB3149090, KB3153704, KB3155784, KB3156017, KB3156019, KB3156059, KB3159398, KB3161949, KB3161958, KB3162343, KB3162835, KB3164294, KB3169704, KB3170455, KB3172614, KB3173424, KB3174644, KB3175024, KB3178539, KB3179574, KB3179948, KB3184122, KB3184943, KB3185319, KB3186539, KB3192392, KB3194343, KB3195387, KB3197873, KB3201860, KB3202790, KB3205400, KB3209498, KB3210132, KB3210135, KB3214628, KB4012213, KB4014556, KB4014574, KB4014581, KB4014590, KB4015547, KB4019213, KB4020322, KB4022717, KB4025333, KB4034672, KB4036586, KB4038793, KB4038806, KB4040956, KB4040967, KB4040972, KB4040981, KB4054522, KB4103715, KB4344166, KB4344178, KB4462901, KB4467703, KB4470499, KB4470602, KB4471322, KB4483469, KB4483484, KB4486105, KB4486459, KB4489883, KB4493467, KB4495586, KB4495615, KB4501226, KB4503290, KB4506962, KB4506977, KB4512489, KB4514338, KB4514350, KB4525250, KB4530730, KB4532961, KB4532970, KB4534309, KB4541505, KB4556853, KB4561673, KB4569768, KB4576614, KB4577071, KB4578623, KB4578981, KB4578986, KB4580358, KB4586823, KB4592495, KB5003220, KB5004285, KB5004958, KB5005106, KB5005627, KB5006729, KB5008285, KB5011560, KB5012147, KB5012152, KB5012639, KB5014746, KB5015877, KB5016268, KB5016683, KB5017365, KB5018476, KB5019958, KB5020010, KB2868626, KB2883200, KB2887595, KB2894852, KB2903939, KB2911106, KB2919355, KB2919394, KB2920189, KB2928680, KB2934520, KB2938066, KB2954879, KB2961908, KB2966826, KB2966828, KB2967917, KB2968296, KB2972103, KB2972213, KB2973114, KB2975061, KB2978122, KB2989930, KB2999226, KB3000483, KB3000850, KB3003057, KB3004365, KB3004545, KB3012235, KB3012702, KB3013172, KB3013531, KB3013538, KB3013769, KB3013791, KB3013816, KB3014442, KB3015696, KB3018133, KB3019978, KB3021910, KB3023219, KB3024751, KB3024755, KB3029603, KB3030947, KB3033446, KB3035126, KB3036612, KB3037576, KB3037924, KB3038002, KB3042085, KB3044374, KB3044673, KB3045634, KB3045685, KB3045717, KB3045719, KB3045755, KB3045999, KB3046017, KB3046737, KB3054169, KB3054203, KB3054256, KB3054464, KB3055323, KB3055343, KB3055642, KB3059317, KB3060681, KB3060793, KB3061512, KB3063843, KB3071756,

KB3072307, KB3074545, KB3076949, KB3077715, KB3078405, KB3078676, KB3080149, KB3082089, KB3083325, KB3084135, KB3084905, KB3086255, KB3087038, KB3087041, KB3087137, KB3087916, KB3089023, KB3091297, KB3094486, KB3095701, KB3097992, KB3099834, KB3100473, KB3102429, KB3102467, KB3103616, KB3103696, KB3103709, KB3109103, KB3109560, KB3109976, KB3110329, KB3112148, KB3112336, KB3115224, KB3118401, KB3121261, KB3121461, KB3122651, KB3123245, KB3124275, KB3126434, KB3126587, KB3132372, KB3133043, KB3138602, KB3138910, KB3139164, KB3140219, KB3145384, KB3145432, KB3155784, KB3159398, KB3161949, KB3162343, KB3172729, KB3174060, KB3175443, KB3179574, KB3185319, KB3186539, KB3186555, KB3195792, KB4014505, KB4014510, KB4014581, KB4022717, KB4025252, KB4025333, KB4025376, KB4033428, KB4040967, KB4041687, KB4041777, KB4048961, KB4093115, KB4095515, KB4095875, KB4096236, KB4096417, KB4130978, KB4230450, KB4284878, KB4287903, KB4338419, KB4338424, KB4338605, KB4338613, KB4338824, KB4339284, KB4343888, KB4457143, KB4462941, KB4467703, KB4468323, KB4480964, KB4486119, KB4486459, KB4487028, KB4490128, KB4495585, KB4495586, KB4495608, KB4495615, KB4495624, KB4499165, KB4501226, KB4506977, KB4507457, KB4507704, KB4512489, KB4516064, KB4519108, KB4519990, KB4530730, KB4535680, KB4537803, KB4550970, KB4552959, KB4552966, KB4556853, KB4557900, KB4561673, KB4565540, KB4565580, KB4565585, KB4566371, KB4569737, KB4569739, KB4576486, KB4577586, KB4578623, KB4578953, KB4578986, KB4580325, KB4580358, KB4586823, KB4598275, KB4601048, KB4601058, KB4601094, KB4601275, KB4601349, KB5000853, KB5001393, KB5001403, KB5001845, KB5001850, KB5003165, KB5003209, KB5003220, KB5003681, KB5004958, KB5005627, KB5007255, KB5008285, KB5009595, KB5010395, KB5011560, KB5012144, KB5012639, KB5013616, KB5013621, KB5014001, KB5015877, KB5016268, KB5017365, KB5020010, KB5020608, KB5020620, KB5020023

Empower client

Windows 7 Pro SP1

Microsoft Windows Version

6.1.7601 SP1 Build 7601

Microsoft Windows Hotfixes:

KB2849697, KB2849696, KB2841134, KB2670838, KB2830477, KB2592687, KB971033, KB2305420, KB2393802, KB2479943, KB2491683, KB2492386, KB2506014, KB2506212, KB2506928, KB2509553, KB2511455, KB2515325, KB2533552, KB2536275, KB2544893, KB2545698, KB2547666, KB2552343, KB2556532, KB2560656, KB2563227, KB2564958, KB2570947, KB2574819, KB2579686, KB2585542, KB2603229, KB2604115, KB2619339, KB2620704, KB2621440, KB2631813, KB2639308, KB2640148, KB2644615, KB2647753, KB2654428, KB2660075, KB2661254, KB2667402, KB2676562, KB2679255, KB2685811, KB2685813, KB2690533, KB2698365, KB2705219, KB2709715, KB2712808, KB2719857, KB2724197, KB2726535, KB2727528, KB2729094, KB2732059, KB2732487, KB2736422,

KB2742599, KB2750841, KB2761217, KB2763523, KB2770660, KB2773072, KB2786081, KB2791765, KB2799494, KB2799926, KB2800095, KB2807986, KB2808679, KB2813170, KB2813347, KB2813430, KB2834140, KB2839894, KB2840631, KB2843630, KB2847927, KB2852386, KB2853952, KB2857650, KB2861698, KB2862152, KB2862330, KB2862335, KB2862973, KB2864202, KB2868038, KB2868116, KB2871997, KB2884256, KB2888049, KB2891804, KB2892074, KB2893294, KB2893519, KB2894844, KB2900986, KB2908783, KB2911501, KB2912390, KB2913431, KB2918077, KB2919469, KB2923545, KB2928562, KB2929437, KB2929733, KB2931356, KB2937610, KB2943357, KB2952664, KB2957189, KB2957689, KB2966583, KB2968294, KB2970228, KB2972100, KB2972211, KB2973112, KB2973201, KB2973351, KB2976897, KB2977292, KB2978120, KB2978742, KB2984972, KB2985461, KB2990214, KB2991963, KB2992611, KB2999226, KB3000483, KB3003743, KB3004361, KB3004375, KB3006121, KB3006137, KB3006625, KB3010788, KB3011780, KB3013531, KB3019215, KB3020338, KB3020369, KB3020370, KB3020388, KB3021674, KB3021917, KB3022345, KB3022777, KB3023215, KB3030377, KB3032655, KB3033889, KB3033890, KB3033929, KB3035126, KB3035132, KB3037574, KB3040272, KB3042058, KB3042553, KB3045685, KB3046017, KB3046269, KB3050265, KB3054476, KB3055642, KB3059317, KB3060716, KB3061518, KB3064209, KB3067903, KB3069762, KB3071756, KB3072305, KB3072630, KB3072633, KB3074543, KB3075226, KB3075249, KB3075851, KB3076949, KB3078601, KB3078667, KB3080079, KB3080149, KB3080446, KB3084135, KB3086255, KB3087039, KB3092601, KB3092627, KB3093513, KB3097966, KB3097989, KB3099862, KB3100213, KB3101722, KB3102429, KB3102810, KB3107998, KB3108371, KB3108381, KB3108664, KB3108669, KB3108670, KB3109094, KB3109103, KB3109560, KB3110329, KB3112148, KB3112343, KB3115858, KB3118401, KB3121212, KB3121255, KB3121461, KB3121918, KB3122648, KB3123479, KB3124000, KB3124001, KB3126446, KB3126587, KB3127220, KB3133977, KB3135983, KB3137061, KB3138378, KB3138612, KB3138901, KB3138910, KB3139398, KB3139914, KB3140245, KB3142024, KB3146706, KB3146963, KB3147071, KB3149090, KB3150220, KB3150513, KB3155178, KB3156016, KB3156017, KB3156019, KB3159398, KB3161102, KB3161561, KB3161949, KB3161958, KB3163245, KB3164035, KB3170455, KB3170735, KB3172605, KB3177186, KB3177467, KB3179573, KB3181988, KB3184143, KB3185319, KB3185911, KB3188730, KB3188740, KB3210131, KB4012212, KB4014504, KB4014573, KB4014579, KB4015546, KB4019263, KB4019990, KB4022722, KB4025337, KB4034679, KB4038779, KB4040980, KB4041678, KB4048960, KB4049068, KB4051956, KB4054521, KB4095514, KB4338423, KB4338612, KB4339284, KB4344152, KB4344177, KB4457008, KB4457044, KB4459934, KB4470600, KB4471328, KB4474419, KB4480960, KB4483483, KB4486459, KB4486564, KB4489885, KB4490128, KB4490628, KB4493448, KB4495606, KB4495612, KB4498206, KB4499175, KB4501226, B4503269, KB4505050, KB4506976, KB4507456, KB4507704, KB4519108, KB4532960, KB958488, KB976002, KB976902, KB976932, KB982018, KB4499178

Windows 10 Pro

Microsoft Windows Version

10.0.18363 N/A Build 18363

Microsoft Windows Hotfixes:

KB4578974, KB4517245, KB4561600, KB4576751, KB4580325, KB4586863, KB4592449, KB4601556, KB4497727, KB4535680, KB4565554, KB4577586, KB4589211, KB4598479, KB4601395, KB5000908, KB5000808, KB4497165, KB4598229

Microsoft Windows Version

10.0.17134 N/A Build 17134

Microsoft Windows Hotfixes:

KB4456655, KB4485449, KB4493478, KB4493464

Windows 10 Enterprise Long Term Servicing Channel (LTSC) (ver. 1809)

Microsoft Windows Version

10.0.17763 N/A Build 17763

Microsoft Windows Hotfixes:

KB5020627, KB4465065, KB4470788, KB4487038, KB4577586, KB4580325, KB5001404, KB4487044, KB5020374

LAC/E device

Windows 7 Professional SP1

Microsoft Windows Version

6.1.7601 SP1 Build 7601

Microsoft Windows Hotfixes:

KB2849697, KB2849696, KB2841134, KB2670838, KB971033, KB2479943, KB2491683, KB2506014, KB2506212, KB2506928, KB2532531, KB2533552, KB2533623, KB2534111, KB2545698, KB2547666, KB2552343, KB2560656, KB2564958, KB2579686, KB2585542, KB2603229, KB2604115, KB2620704, KB2621440, KB2631813, KB2639308, KB2640148, KB2653956, KB2654428, KB2656356, KB2660075, KB2667402, KB2685811, KB2685813, KB2690533, KB2698365, KB2705219, KB2706045, KB2719857, KB2726535, KB2727528, KB2729094, KB2729452, KB2731771, KB2732059, KB2736422, KB2742599, KB2750841, KB2758857, KB2761217, KB2770660, KB2773072, KB2786081, KB2789645, KB2791765, KB2799926, KB2800095, KB2807986, KB2808679, KB2813430, KB2834140, KB2836942, KB2836943, KB2840631, KB2843630, KB2847927, KB2852386, KB2853952, KB2861698, KB2862330, KB2862335, KB2864202, KB2868038, KB2871997, KB2882822, KB2884256, KB2888049, KB2891804, KB2893294, KB2893519, KB2894844, KB2900986, KB2908783,

KB2911501, KB2912390, KB2918077, KB2919469, KB2931356, KB2937610, KB2943357, KB2968294, KB2970228, KB2972100, KB2972211, KB2973112, KB2973201, KB2977292, KB2978742, KB2984972, KB2985461, KB2991963, KB2992611, KB2999226, KB3000483, KB3004375, KB3006121, KB3006137, KB3010788, KB3011780, KB3013531, KB3019978, KB3020370, KB3021674, KB3023215, KB3030377, KB3031432, KB3035126, KB3037574, KB3045685, KB3046017, KB3046269, KB3054476, KB3055642, KB3059317, KB3060716, KB3067903, KB3068708, KB3071756, KB3072305, KB3074543, KB3075220, KB3078667, KB3080149, KB3086255, KB3092601, KB3093513, KB3097989, KB3101722, KB3107998, KB3108371, KB3108664, KB3109103, KB3109560, KB3110329, KB3115858, KB3122648, KB3124275, KB3126587, KB3127220, KB3133977, KB3137061, KB3138378, KB3138612, KB3138910, KB3139398, KB3139914, KB3140245, KB3147071, KB3150220, KB3150513, KB3155178, KB3156016, KB3159398, KB3161102, KB3161949, KB3170735, KB3179573, KB3184143, KB3185319, KB3192391, KB3197867, KB3205394, KB4012212, KB4014573, KB4014579, KB4015546, KB4019263, KB4019990, KB4022722, KB4025337, KB4034679, KB4038779, KB4040966, KB4040980, KB4041678, KB4048960, KB4054521, KB4093108, KB4095514, KB4103712, KB4284867, KB4338423, KB4338612, KB4338823, KB4343899, KB4344177, KB4457145, KB4462915, KB4467106, KB4470600, KB4471328, KB4474419, KB4480960, KB4483483, KB4486459, KB4486564, KB4489885, KB4490128, KB4490628, KB4491113, KB4493448, KB4495606, KB4495612, KB4496880, KB4499175, KB4501226, KB4503269, KB4506976, KB4507456, KB4507704, KB4534251, KB958488, KB976902, KB982018, KB4457144

Windows 10 Pro

Microsoft Windows Version

10.0.19045 N/A Build 19045

Microsoft Windows Hotfixes:

KB5017022, KB4562830, KB5007401, KB5015684, KB5019959, KB5014032, KB5016705, KB5018506

Microsoft Windows Version

10.0.18363 N/A Build 18363

Microsoft Windows Hotfixes:

KB4580980, KB4497165, KB4513661, KB4516115, KB4517245, KB4524569, KB4537759, KB4552152, KB4559309, KB4560959, KB4561600, KB4576751, KB4580325, KB4586863, KB4586786

Windows 10 Enterprise Long Term Service Branch (LTSB) (Build 1607, Config 16 eLAC/E)

Microsoft Windows Version

10.0.14393 N/A Build 14393

Microsoft Windows Hotfixes:

KB4033631, KB4049411, KB4346087, KB4535680, KB4580325, KB5001078, KB5000803

Standalone/Personal Workstation

Windows 10 Pro

Microsoft Windows Version

10.0.18363 N/A Build 18363

Microsoft Windows Hotfixes:

KB4578974, KB4497165, KB4517245, KB4535680, KB4561600, KB4565554, KB4580325, KB4598479, KB4598229, KB4576751, KB4576947, KB4574727

Citrix Server (XenApp Server 7.15 Enterprise)

Citrix Presentation Server

Microsoft Windows Server 2016 Standard

Microsoft Windows Version

10.0.14393 N/A Build 14393

Microsoft Windows Hotfixes:

KB5008877, KB3186568, KB3192137, KB3199986, KB4035631, KB4049065, KB4093137, KB4132216, KB4486129, KB4520724, KB4535680, KB4550993, KB4550994, KB4576750, KB4577586, KB4589210, KB5001078, KB5001402, KB5005698, KB5011570, KB5011495

Citrix App Server

Microsoft Windows Server 2016 Standard (Citrix Server XenApp 7.15 LTSR CU2)

Microsoft Windows Version

10.0.14393 N/A Build 14393

Microsoft Windows Hotfixes:

KB3186568, KB3192137, KB3199986, KB4035631, KB4049065, KB4093137, KB4132216, KB4535680, KB4550994, KB5001402, KB5005698, KB5011570, KB5011495

Citrix Client

Microsoft Windows 10 Pro (Interface Citrix Workspace 2210 and Interface Citrix Workspace 2212)

Microsoft Windows Version

10.0.18363 N/A Build 18363

Microsoft Windows Hotfixes:

KB4578974, KB4497165, KB4517245, KB4535680, KB4561600, KB4565554, KB4580325, KB4598479, KB4598229