Citrix Workspace app for Mac
Contents

What’s new in Citrix Workspace app for Mac 3
  What’s new in 1809 ............................................. 3
  What’s new in 1808 ............................................. 3

Fixed issues 4
  Fixed issues in 1809 ............................................. 4
  Fixed issues in 1808 ............................................. 4

Known issues 5
  Known issues in 1809 ............................................. 5
  Known issues in 1808 ............................................. 5

System requirements 5
  Supported operating systems .................................. 5
  Compatible Citrix products .................................. 5
  Compatible browsers ....................................... 6
  Connectivity ......................................................... 6
  Authentication ..................................................... 7

Install and configure 8
  Installation .......................................................... 8
  Upgrading Citrix Workspace app for Mac ................. 10
  About deploying and configuring Citrix Workspace app for Mac 10
  Uninstalling Citrix Workspace app for Mac ............ 11

Configuration 11
  Content Collaboration Service integration in Citrix Workspace app 11
  Configure USB redirection ................................ 12
  Configure session reliability and auto client reconnect 16
  Configuring CEIP ................................................... 23
  Configure your application delivery ....................... 24
  Configure self-service mode ................................ 25
  Configure StoreFront ............................................ 26
  Provide users with account information .................. 26
  Configuring auto-update ...................................... 27
  Configuring the enhanced client IME using the configuration file 29
  Keyboard layout synchronization ............................. 29
  Language bar ......................................................... 32

© 1999-2018 Citrix Systems, Inc. All rights reserved.
## Optimize
- Reconnecting users automatically .................................................. 32
- Restarting desktops ........................................................................ 33
- Providing session reliability ............................................................. 33
- Providing continuity for roaming users ............................................. 33
- Mapping client devices .................................................................... 34
- Mapping client drives ..................................................................... 34

## Improving the user experience
- Customer Experience Improvement Program (CEIP) ...................... 35
- ClearType font smoothing ............................................................... 35
- Client-side microphone input .......................................................... 36
- Windows special keys ..................................................................... 36
- Windows shortcuts and key combinations ....................................... 37
- Use Input Method Editors (IME) and international keyboard layouts ................................................................................. 39
- Using multiple monitors .................................................................. 40
- Using the Desktop toolbar ............................................................... 41

## Secure communications
- About certificates ........................................................................... 42
- Joint Server Certificate Validation Policy ....................................... 43
- Connecting with NetScaler Gateway .............................................. 45
- Using the UI to configure security settings ..................................... 51

## Requirements for smart card authentication
- About smart card authentication to Citrix Gateway ....................... 53
- Specifying a PKCS#11 module for smart card authentication .......... 53
- Supported readers, middleware, and smart card profiles .................. 54
- Restrictions .................................................................................... 54
What’s new in Citrix Workspace app for Mac

September 25, 2018

What’s new in 1809

macOS Mojave support

Citrix Workspace app for Mac fully supports macOS Mojave, including Dark Mode.

WebApp support

Secure Browser for Citrix Workspace app for Mac now supports cookies and redirects when using Citrix Gateway.

What’s new in 1808

64-bit support

Citrix Workspace app for Mac is now fully 64-bit.

Note:

Users who upgrade to Citrix Workspace app will not have an optimized Skype for Business (Lync) experience due to a bitness mismatch. Citrix Workspace app for Mac is 64-bit, while the currently installed version of RTME is 32-bit. The release of a 64-bit version of RTME is planned for late September. As a workaround, consider using the RTME Tech Preview release.

Note:

32-bit custom virtual channels no longer work and must be updated to 64-bit.

Federated authentication

Citrix Workspace app for Mac now supports federated authentication through Azure Active Directory.

Show or hide the remote language bar

Starting with this release, you can choose to show or hide the remote language bar in an application session using the graphical user interface. The language bar displays the preferred input language in a
Citrix Workspace app for Mac

session. In earlier releases, you could change this setting using only the registry keys on the VDA. Starting with Citrix Workspace app for Mac version 1808, you can change the settings using the Preferences dialog. The language bar appears in a session by default.

For more information, see Configuration and Knowledge Center article CTX231913.

Note:
This feature is available in sessions running on VDA 7.17 and later.

Support for Citrix Analytics

Citrix Workspace app is instrumented to securely transmit logs to Citrix Analytics. The logs are analyzed and stored on Citrix Analytics when enabled. For more information about Citrix Analytics, see Citrix Analytics documentation.

Fixed issues

September 25, 2018

Fixed issues in 1809

• Sessions that have reconnected might not stay connected. [RFMAC-1823]

Fixed issues in 1808

• On dual GPU Macs, the client might use the discrete GPU on battery power instead of the more power efficient integrated GPU. [RFMAC-1439]

• The client might not upgrade correctly when installed with JamF. [RFMAC-1523]

• USB devices might not appear in a session when attempting to use them for generic USB redirection. [RFMAC-1592]

• Checking for client updates might fail with a “Problem Checking for Updates” error. [RFMAC-1589]

• When more than one published app window is open, activating a published application window can result in a different published app window coming to the foreground. [RFMAC-1696]
Known issues

September 25, 2018

Known issues in 1809

- App and desktop sessions might not launch when using Safari version 12. As a workaround, see Knowledge Center article CTX238286. After the workaround, Safari asks for permissions which users have to allow every time to launch sessions.

Known issues in 1808

- When an error occurs with an app using Secure SaaS, the error that appears inside the browser is not localized. [RFMAC-1836]

System requirements

September 21, 2018

Supported operating systems

Citrix Workspace app for Mac supports the following operating systems:

- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- Mac OS X El Capitan (10.11)

Note:
Mac OS X releases prior to Mac OS X El Capitan are not supported.

Compatible Citrix products

Citrix Workspace app for Mac is compatible with all currently supported versions of the following Citrix products. For information about the Citrix product lifecycle, and to find out when Citrix stops supporting specific versions of products, see the Citrix Product Lifecycle Matrix.
Citrix Workspace app for Mac

Compatible browsers

Citrix Workspace app for Mac is compatible with the following browsers:

- Safari 7.0 and later
- Mozilla Firefox 22.x and later
- Google Chrome 28.x and later

Hardware requirements

- 257.7 MB of free disk space
- A working network or Internet connection to connect to servers

Software requirements

- Web Interface:
  - Web Interface 5.4 for Windows with XenApp Services sites, for access to applications natively from Citrix Workspace app for Mac rather than from a web browser.
- To deploy Citrix Workspace app for Mac:
  - Citrix Workspace for Web 2.1, 2.5 and 2.6
  - Citrix Web Interface 5.4
- StoreFront:
  StoreFront 2.x or later for access to applications natively from Citrix Workspace app for Mac or from a web browser.

Connectivity

Citrix Workspace app for Mac supports the following connections to Citrix Virtual Apps and Desktops:

- HTTP
- HTTPS
- ICA-over-TLS

Citrix Workspace app for Mac supports the following configurations:

<table>
<thead>
<tr>
<th>For LAN connections</th>
<th>For secure remote or local connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>StoreFront using StoreFront services or Citrix Workspace for Web site; Web Interface 5.4 for Windows, using XenApp Services sites</td>
<td>Citrix Citrix Gateway 10.5-12.0, including VPX; Enterprise Edition 9.x-10.x, including VPX; VPX; Citrix Secure Web Gateway 3.x (for use with Web Interface only)</td>
</tr>
</tbody>
</table>
Authentication

For connections to StoreFront, Citrix Workspace app for Mac supports the following authentication methods:

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Workspace for Web using browsers</th>
<th>StoreFront Services site (native)</th>
<th>StoreFront XenApp Services site (native)</th>
<th>Citrix Gateway to Workspace for Web (browser)</th>
<th>Citrix Gateway to StoreFront Services site (native)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>Domain</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>Domain pass-through</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security token</td>
<td></td>
<td>Yes*</td>
<td>Yes*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Two-factor (domain with security token)</td>
<td></td>
<td>Yes*</td>
<td>Yes*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS</td>
<td></td>
<td>Yes*</td>
<td>Yes*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User certificate</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes*</td>
<td>Yes (Citrix Gateway Plugin)</td>
</tr>
</tbody>
</table>

*Available only for Workspace for Web sites and for deployments that include Citrix Gateway, with or without installing the associated plug-in on the device.

For connections to Web Interface 5.4, Citrix Workspace app for Mac supports the following authentication methods:

**Note:**
Web Interface uses the term Explicit to represent domain and security token authentication.
## Citrix Workspace app for Mac

<table>
<thead>
<tr>
<th>Anonymous</th>
<th>Web Interface (browsers)</th>
<th>Web Interface XenApp Services site</th>
<th>Citrix Gateway to Web Interface (browser)</th>
<th>Citrix Gateway to Web Interface XenApp Services site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- **Domain pass-through**
  - Yes
  - Yes
  - Yes
  - Yes

- **Security token**
  - Yes*
  - Yes

- **Two-factor (domain with security token)**
  - Yes*
  - Yes

- **SMS**
  - Yes*
  - Yes

- **Smart card**
  - Yes
  - Yes

- **User certificate**
  - Yes (Require Citrix Gateway Plugin)
  - Yes (Require Citrix Gateway Plugin)

* Available only in deployments that include Citrix Gateway, with or without installing the associated plug-in on the device.

### Install and configure

**September 21, 2018**

### Installation

This release of Citrix Workspace app for Mac contains a single installation package and supports remote access through Citrix Gateway, and Secure Web Gateway.

Citrix Workspace app for Mac can be installed by a user from the Citrix website, automatically from Workspace for Web or from Web Interface, or by using an Electronic Software Distribution (ESD) tool.
Citrix Workspace app for Mac

By a user from Citrix.com

- A first-time Citrix Workspace app for Mac user who obtains Citrix Workspace app for Mac from Citrix.com or your own download site can set up an account by entering an email address instead of a server URL. Citrix Workspace app for Mac determines the Citrix Gateway or StoreFront server associated with the email address and then prompts the user to log on and continue the installation. This feature is referred to as email-based account discovery.

Note:
A first-time user is a user who does not have Citrix Workspace app for Mac installed on their user device.

- Email-based account discovery for a first-time user does not apply if Citrix Workspace app for Mac is downloaded from a location other than Citrix.com (such as a Workspace for Website).
- If your site requires the configuration of Citrix Workspace app for Mac, use an alternate deployment method.

Automatically from Workspace for Web or from Web Interface

- A first-time Citrix Workspace app for Mac user can set up an account by entering a server URL or by downloading a provisioning file.

Using an Electronic Software Distribution (ESD) tool

- A first-time Citrix Workspace app for Mac user must enter a server URL to set up an account.

Installing Citrix Workspace app for Mac manually

Users can install Citrix Workspace app for Mac from the Web Interface, a network share, or directly on to the user device by downloading the file from the Citrix Web site at http://www.citrix.com.

To install Citrix Workspace app for Mac:

1. Download the .dmg file for the version of Citrix Workspace app for Mac you want to install from the Citrix web site and open it.
2. On the Introduction page, click Continue.
3. On the License page, click Continue.
4. Click Agree to accept the terms of the License Agreement.
5. On the Installation Type page, click Install.
6. Enter the username and password of an administrator on the local device.
Upgrading Citrix Workspace app for Mac

Upgrades are supported from versions 11.x of the Online Plug-in for Mac. You can upgrade Citrix Workspace app for Mac from any of the previous versions of Citrix Workspace app for Mac.

About deploying and configuring Citrix Workspace app for Mac

For deployments with StoreFront:

- A best practice is to configure Citrix Gateway and StoreFront 3.x as described in the documentation for those products on the Citrix Gateway and StoreFront documentation. Attach the provisioning file created by StoreFront to an email and inform users how to upgrade and how to open the provisioning file after installing Citrix Workspace app for Mac.
- As an alternative to using a provisioning file, tell users to enter either the URL of a Citrix Gateway. If you have configured email-based account discovery as described in the StoreFront documentation, tell users to enter their email address.
- Another method is to configure a Workspace for Web site as described in the StoreFront documentation. Inform users how to upgrade Citrix Workspace app for Mac, access the Workspace for Web site, and download the provisioning file from the Workspace for Web interface (click the user name and then click Activate).

For deployments with Web Interface:

- Upgrade your Web Interface site with Citrix Workspace app for Mac and let your users know how to upgrade Citrix Workspace app for Mac. You can, for example, provide users with installation captions on their Messages screen to let them know they need to upgrade to the latest version of Citrix Workspace app for Mac.

Deploying Citrix Workspace app for Mac from Workspace for Web

You can deploy Citrix Workspace app for Mac from Workspace for Web to ensure that users have it installed before they try to connect to an application from a browser. Workspace for Web sites enable users to access StoreFront stores through a Web page. If the Workspace for Web site detects that a user does not have a compatible version of Citrix Workspace app for Mac, the user is prompted to download and install Citrix Workspace app for Mac. For more information, see the StoreFront documentation.

Deploying Citrix Workspace app for Mac from a Web Interface logon screen

This feature is available only for Citrix Virtual Apps and Desktops releases that support Web Interface.
Citrix Workspace app for Mac

You can deploy Citrix Workspace app for Mac from a web page to ensure that users have it installed before they try to use the Web Interface. The Web Interface provides a client detection and deployment process that detects which Citrix clients can be deployed within the user’s environment and then guides them through the deployment procedure.

You can configure the client detection and deployment process to run automatically when users access a Citrix Virtual Apps website. If the Web Interface detects that a user does not have compatible version of Citrix Workspace app for Mac, the user is prompted to download and install Citrix Workspace app for Mac.

Uninstalling Citrix Workspace app for Mac

You can uninstall Citrix Workspace app for Mac manually by opening the .dmg file, select Uninstall Citrix Workspace App, and follow the on-screen instructions.

Configuration

September 21, 2018

After the Citrix Workspace app for Mac software is installed, the following configuration steps allow users to access their hosted applications and desktops.

If you have users who connect from outside the internal network (for example, users who connect from the Internet or from remote locations), configure authentication through Citrix Gateway.

Content Collaboration Service integration in Citrix Workspace app

Citrix Content Collaboration enables you to easily and securely exchange documents, send large documents by email, securely handle document transfers to third parties, and access a collaboration space. Citrix Content Collaboration provides many ways to work, including a web-based interface, mobile clients, desktop apps, and integration with Microsoft Outlook and Gmail.

You can access Citrix Content Collaboration functionality from the Citrix Workspace app using the Files tab displayed within Citrix Workspace app. You can view the Files tab only if Content Collaboration Service is enabled in the Workspace configuration in the Citrix Cloud console.

Note:

Citrix Content Collaboration integration in Citrix Workspace app is not supported on Windows Server 2012 and Windows Server 2016 due to a security option set in the operating system.
The following image displays example contents of the Files tab of the new Citrix Workspace app:

Limitations:

- Resetting Citrix Workspace app does not cause Citrix Content Collaboration to log off.
- Switching stores in Citrix Workspace app does not cause Citrix Content Collaboration to log off.

**Configure USB redirection**

HDX USB device redirection enables redirection of USB devices to and from a user device. For example, a user can connect a flash drive to a local computer and access it remotely from within a virtual desktop or a desktop hosted application. During a session, users can plug and play devices, including Picture Transfer Protocol (PTP) devices such as digital cameras, Media Transfer Protocol (MTP) devices such as digital audio players or portable media players, point-of-sale (POS) devices and other devices such as 3D Space Mice, Scanners, Signature Pads etc.
USB redirection is available for the following:

- Windows
- Linux
- Mac

By default, USB redirection is allowed for certain classes of USB devices, and denied for others. You can restrict the types of USB devices made available to a virtual desktop by updating the list of USB devices supported for redirection, as described later in this section.

Tip

In environments where security separation between the user device and server is needed, Citrix recommends that users are informed about the types of USB devices to avoid.

Optimized virtual channels are available to redirect most popular USB devices, and provide superior performance and bandwidth efficiency over a WAN. Optimized virtual channels are usually the best option, especially in high latency environments.

Note:

For USB redirection purposes, Citrix Workspace app for Mac handles a SMART board the same as a mouse.

The product supports optimized virtual channels with USB 3.0 devices and USB 3.0 ports, such as a CDM virtual channel used to view files on a camera or to provide audio to a headset. The product also supports Generic USB Redirection of USB 3.0 devices connected to a USB 2.0 port.

Some advanced device-specific features, such as Human Interface Device (HID) buttons on a webcam, may not work as expected with the optimized virtual channel; if this is an issue, use the Generic USB virtual channel.

Certain devices are not redirected by default, and are only available to the local session. For example, it would not be appropriate to redirect a network interface card that is directly attached via internal USB.

To use USB redirection:

1. Connect the USB device to the device where Citrix Workspace app for Mac is installed.

2. You will be prompted to select the available USB devices on your local system.
3. Select the device you wish to connect and click **Connect**. If the connection fails, an error message appears.

4. In the **Preferences** window **Devices** tab, the connected USB device is listed in the USB panel:
5. Select the type of virtual channel for the USB device, *Generic* or *Optimized*.

6. A message is displayed. Click to connect the USB device to your session:
Citrix Workspace app for Mac

Use and remove USB devices

Users can connect a USB device before or after starting a virtual session. When using Citrix Workspace app for Mac, the following apply:

- Devices connected after a session starts immediately appear in the USB menu of the Desktop Viewer.
- If a USB device is not redirecting properly, sometimes you can resolve the problem by waiting to connect the device until after the virtual session has started.
- To avoid data loss, use the Windows Safe removal menu before removing the USB device.

Configuring Enlightened Data Transport (EDT)

By default, EDT is enabled in Citrix Workspace app for Mac.

Citrix Workspace app for Mac reads the EDT settings as set in the default.ica file and applies it accordingly.

To disable EDT, run the following command in a terminal:

```bash
defaults write com.citrix.receiver.nomas HDXOverUDPAAllowed -bool NO
```

Configure session reliability and auto client reconnect

Session reliability keeps sessions active and on the user’s screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes.

With session reliability, the session remains active on the server. To indicate that connectivity is lost, the user’s display freezes until connectivity resumes on the other side of the tunnel. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored. Session reliability reconnects users without reauthentication prompts.

**Important**

Citrix Workspace app for Mac users cannot override the server setting.

You can use session reliability with Transport Layer Security (TLS).

**Note**

TLS encrypts only the data sent between the user device and Citrix Gateway.
Using session reliability policies

The session reliability connections policy setting allows or prevents session reliability.

The session reliability timeout policy setting has a default of 180 seconds, or three minutes. Though you can extend the amount of time session reliability keeps a session open, this feature is designed to be convenient to the user and it does not, therefore, prompt the user for reauthentication.

Tip
As you extend the amount of time a session is kept open, chances increase that a user may get distracted and walk away from the user device, potentially leaving the session accessible to unauthorized users.

Incoming session reliability connections use port 2598, unless you change the port number defined in the session reliability port number policy setting.

If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, use the Auto Client Reconnect feature. You can configure the Auto client reconnect authentication policy setting to prompt users to reauthenticate when reconnecting to interrupted sessions.

If you use both session reliability and auto client reconnect, the two features work in sequence. Session reliability closes, or disconnects, the user session after the amount of time you specify in the Session reliability timeout policy setting. After that, the auto client reconnect policy settings take effect, attempting to reconnect the user to the disconnected session.

Note
Session reliability is enabled by default at the server. To disable this feature, configure the policy managed by the server.

Configuring session reliability

By default, session reliability is enabled.

To disable session reliability:

1. Launch Citrix Studio.
2. Open the Session Reliability connections policy.
3. Set the policy to Prohibited.
Configuring session reliability timeout

By default, session reliability timeout is set to 180 seconds.

Note:
Session reliability timeout policy can be configured only with XenApp/XenDesktop 7.11 and later.

To modify session reliability timeout:

1. Launch Citrix Studio.
2. Open the Session reliability timeout policy.
3. Edit the timeout value.
4. Click OK.

Configuring auto client reconnection

By default, auto client reconnection is enabled.

To disable auto client reconnection:
1. Launch Citrix Studio.
2. Open the **Auto client reconnect policy**.
3. Set the policy to **Prohibited**.

### Configuring Auto client reconnection timeout

By default, Auto client reconnection timeout is set to 120 seconds.

**Note:**

Auto client reconnect timeout policy can be configured only with XenApp/XenDesktop 7.11 and later.

To modify auto client reconnect timeout:

1. Launch Citrix Studio.
2. Open the **Auto client reconnect** policy.
3. Edit the timeout value.
4. Click **OK**.
Limitations:
On a Terminal Server VDA, Citrix Workspace app for Mac uses 120 seconds as timeout value irrespective of the user settings.

Configuring the Reconnect user interface transparency level

The Session User Interface is displayed during a session reliability and auto client reconnect attempts. The transparency level of the user interface can be modified using Studio policy.

By default, Reconnect UI transparency is set to 80%.

To modify Reconnect user interface transparency level:

1. Launch Citrix Studio.
2. Open the Reconnect UI transparency level policy.
3. Edit the value.
4. Click OK.

Auto client reconnect and session reliability interaction

Mobility challenges associated with switching between various access points, network disruptions and display timeouts related to latency create challenging environments when trying to maintain link integrity for active Citrix Workspace app for Mac sessions. To resolve this issue, Citrix enhanced session reliability and auto reconnection technologies present in this version of Workspace app for Mac.

Auto client reconnection, along with session reliability, allows users to automatically reconnect to their Citrix Workspace app for Mac sessions after recovering from network disruptions. These features, enabled by policies in Citrix Studio, can be used to vastly improve the user experience.

Note:
Auto client reconnection and session reliability timeout values can be modified using the default.ica file in StoreFront.

Auto client reconnection

Auto client reconnection can be enabled or disabled using Citrix Studio policies. By default, this feature is enabled. For information about modifying this policy, see the auto client reconnection section earlier in this article.

Use the default.ica file in StoreFront to modify the connection timeout for AutoClientReconnect; by default, this timeout is set to 120 seconds (or two minutes).
Session reliability

Session reliability can be enabled or disabled using Citrix Studio policies. By default, this feature is enabled.

Use the `default.ica` file in StoreFront to modify the connection timeout for session reliability; by default, this timeout is set to 180 seconds (or three minutes).

### How auto client reconnection and session reliability works

When auto client reconnection and session reliability are enabled for a Citrix Workspace app for Mac, consider the following:

- A session window is greyed out when a reconnection is in progress; a countdown timer displays the amount of time remaining before the session is reconnected. Once a session is timed out, it is disconnected.

By default, the reconnect countdown timer notification starts at 5 minutes; this time value represents the combined default values for each of the timers (auto client reconnection and session reliability), 2 and 3 minutes respectively. The image below illustrates the countdown timer notification which appears in the upper right portion of the session interface:
Tip

You can alter the greyscale brightness used for an inactive session using a command prompt. For example, defaults write com.citrix.receiver.nomas NetDisruptBrightness 80. By default, this value is set to 80. The maximum value cannot exceed 100 (indicates a transparent window) and the minimum value can be set to 0 (a fully blacked out screen).

- Users are notified when a session successfully reconnects (or when a session is disconnected). This notification appears in the upper right portion of the session interface:
A session window which is under auto client reconnect and session reliability control provides an informational message indicating the state of the session connection. Click **Cancel Reconnection** to move back to an active session.

### Configuring CEIP

CEIP is scheduled to collect and securely upload data to Citrix at an interval of 7 days by default. You can change your participation in CEIP anytime using the Citrix Workspace app for Mac **Security** > **Preferences** screen.

**Tip**

When CEIP is disabled, minimal information containing only the installed Citrix Workspace app for Mac version is uploaded; this happens only once. This minimal information is valuable to Citrix because it provides the distribution of different versions used by customers. This happens only once as soon as CEIP is disabled.

To disable CEIP, or to forego participation:

1. In the **Preferences** window, select **Security and Privacy**.
2. Select the **Privacy** tab.
3. Change the appropriate radio button. For example, to disable CEIP, click **"No, Thanks."**
4. Click **OK**.
Configure your application delivery

When delivering applications with Citrix Virtual Apps and Desktops, consider the following options to enhance the experience for your users when they access their applications:

**Web access mode**

Without any configuration, Citrix Workspace app for Mac provides web access mode: browser-based access to applications and desktops. Users simply open a browser to a Workspace for Web or Web Interface site and select and use the applications that they want. In web access mode, no app shortcuts are placed in the App Folder on your user’s device.
Self-service mode

By adding a StoreFront account to Citrix Workspace app for Mac or configuring Citrix Workspace app for Mac to point to a StoreFront site, you can configure self-service mode, which enables your users to subscribe to applications through Citrix Workspace app for Mac. This enhanced user experience is similar to that of a mobile app store. In self-service mode you can configure mandatory, auto-provisioned, and featured app keyword settings as needed. When one of your users selects an application, a shortcut to that application is placed in the App Folder on the user device.

When accessing a StoreFront 3.0 site, your users see the Citrix Workspace app for Mac Tech Preview user experience.

When publishing applications on your Citrix Virtual Apps farms, to enhance the experience for users accessing those applications through StoreFront stores, ensure that you include meaningful descriptions for published applications. The descriptions are visible to your users through Citrix Workspace app for Mac.

Configure self-service mode

As mentioned previously, by adding a StoreFront account to Citrix Workspace app for Mac or configuring Citrix Workspace app for Mac to point to a StoreFront site, you can configure self-service mode, which allows users to subscribe to applications from the Citrix Workspace app for Mac user interface. This enhanced user experience is similar to that of a mobile app store.

In self-service mode, you can configure mandatory, auto-provisioned and featured app keyword settings as needed.

- To automatically subscribe all users of a store to an application, append the string KEYWORDS:Auto to the description you provide when you publish the application in Citrix Virtual Apps. When users log on to the store, the application is automatically provisioned without the need for users to manually subscribe to the application.
- To advertise applications to users or make commonly used applications easier to find by listing them in the Citrix Workspace app for Mac Featured list, append the string KEYWORDS:Featured to the application description.

For more information, see the StoreFront documentation.

If the Web Interface of your Citrix Virtual Apps deployment does not have a XenApp Services site, create a site. The name of the site and how you create the site depends on the version of the Web Interface you have installed. For more information, see the Web Interface documentation.
Configure StoreFront

With StoreFront, the stores you create consist of services that provide authentication and resource delivery infrastructure for Citrix Workspace app for Mac. Create stores that enumerate and aggregate desktops and applications from Citrix Virtual Apps and Desktops sites and Citrix Virtual Apps farms, making these resources available to users.

1. Install and configure StoreFront. For more information, see the StoreFront documentation.

   Note: For administrators who need more control, Citrix provides a template you can use to create a download site for Citrix Workspace app for Mac.

2. Configure stores for CloudGateway just as you would for other Citrix Virtual Apps and Desktops applications. No special configuration is needed for Citrix Workspace app for Mac. For more information, see Configuring Stores in the StoreFront documentation.

Provide users with account information

After installation, you must provide users with the account information they need to access their hosted applications and desktops. You can provide this information by:

- Configuring email-based account discovery
- Providing users with a provisioning file
- Providing users with an auto-generated setup URL
- Providing users with account information to enter manually

Configuring email-based account discovery

You can configure Citrix Workspace app for Mac to use email-based account discovery. When configured, users enter their email address rather than a server URL during initial Citrix Workspace app for Mac installation and configuration. Citrix Workspace app for Mac determines the Citrix Gateway, or StoreFront server associated with the email address based on Domain Name System (DNS) Service (SRV) records and then prompts the user to log on to access their hosted applications and desktops.

To configure your DNS server to support email-based discovery, see the topic Configuring Email-based Account Discovery in the StoreFront documentation.

To configure Citrix Gateway to accept user connections by using an email address to discover the StoreFront, Citrix Gateway, see Connecting to StoreFront by Using Email-Based Discovery in the Citrix Gateway documentation.
**Provide users with a provisioning file**

You can use StoreFront to create provisioning files containing connection details for accounts. You make these files available to your users to enable them to configure Citrix Workspace app for Mac automatically. After installing Citrix Workspace app for Mac, users simply open the file to configure Citrix Workspace app for Mac. If you configure Workspace for Web sites, users can also obtain Citrix Workspace app for Mac provisioning files from those sites.

For more information, see the StoreFront documentation.

**Provide users with an auto-generated setup URL**

You can use the Citrix Workspace app for Mac Setup URL Generator to create a URL containing account information. After installing Citrix Workspace app for Mac, users simply click on the URL to configure their account and access their resources. Use the utility to configure settings for accounts and email or post that information to all your users at once.

**Provide users with account information to enter manually**

If providing users with account details to enter manually, ensure you distribute the following information to enable them to connect to their hosted and desktops successfully:

- The URL for the StoreFront store or XenApp Services site hosting resources; for example: https://servername.example.com
- For access using Citrix Gateway: the Citrix Gateway address, product edition, and required authentication method

For more information about configuring Citrix Gateway, see the Citrix Gateway documentation.

When a user enters the details for a new account, Citrix Workspace app for Mac attempts to verify the connection. If successful, Citrix Workspace app for Mac prompts the user to log on to the account.

**Configuring auto-update**

**Configuring using the graphical user interface**

An individual user can override the Citrix Workspace Updates setting using the Preferences dialog. This is a per-user configuration and the settings apply only to the current user.

1. Go to the Preferences dialog in Citrix Workspace app for Mac.
2. In the Advanced pane, click Auto Update. The Citrix Workspace Updates dialog appears.
3. Select one of the following options:
   - Yes, notify me
   - No, don’t notify me
   - Use administrator specified settings

4. Close the dialog box to save the changes.

**Configuring Citrix Workspace Updates using StoreFront**

Administrators can configure Citrix Workspace Updates using StoreFront. Citrix Workspace app for Mac only uses this configuration for users who have selected “Use administrator specified settings.” To manually configure it, follow the steps below.

1. Use a text editor to open the web.config file. The default location is C:\inetpub\wwwroot\Citrix\Roaming\web.config
2. Locate the user account element in the file (Store is the account name of your deployment)
   For example: <account id=… name="Store">
   Before the </account> tag, navigate to the properties of that user account:
   <properties>
   <clear />
   </properties>
3. Add the auto-update tag after <clear /> tag.

**auto-update-Check**

This determines that Citrix Workspace app for Mac can detect if updates are available.

**Valid values:**

- Auto – Use this option to get notifications when updates are available.
- Manual – Use this option to not get any notification when updates are available. Users need to check manually for updates by selecting Check for Updates.
- Disabled – Use this option to disable Citrix Workspace Updates.

**auto-update-DeferUpdate-Count**

This determines the number of times the end user will be notified to upgrade before they are forced to update to the latest version of Citrix Workspace app for Mac. By default, this value is 7.

**Valid values:**
Citrix Workspace app for Mac

-1 – The end user will always have the option of getting reminded later when an update is available.
0 – The end user will be forced to update to the latest version of Citrix Workspace app for Mac as soon as the update is available.
Positive integer – The end user will be reminded this many number of times before being forced to update. Citrix recommends not to set this value higher than 7.

**auto-update-Rollout-Priority**
This determines how quickly a device will see that an update is available.

**Valid values:**
- Auto – The Citrix Workspace Updates system will decide when available updates are rolled out to users.
- Fast – Available updates will be rolled out to users on high priority as determined by Citrix Workspace app for Mac.
- Medium – Available updates will be rolled out to users on medium priority as determined by Citrix Workspace app for Mac.
- Slow – Available updates will be rolled out to users on low priority as determined by Citrix Workspace app for Mac.

**Configuring the enhanced client IME using the configuration file**
The enhanced client IME is dependent on the keyboard layout synchronization feature. By default, the enhanced IME feature is enabled when the keyboard layout synchronization feature is turned on. To control this feature alone, open the Config file in the ~/Library/Application Support/Citrix Workspace/ folder, locate the “EnableIMEEnhancement” setting and turn the feature on or off by setting the value to “true” or “false,” respectively.

**Note:**
The setting change takes effect after restarting the session.

**Keyboard layout synchronization**
Keyboard layout synchronization enables users to switch among preferred keyboard layouts on the client device. This feature is disabled by default.

To enable keyboard layout synchronization, go to Preferences > Keyboard and select “Use local keyboard layout, rather than the remote server keyboard layout.”
Note:

1. Using the local keyboard layout option activates the client IME (Input Method Editor). If users working in Japanese, Chinese or Korean prefer to use the server IME, they must disable the local keyboard layout option by clearing the option in Preferences > Keyboard. The session will revert to the keyboard layout provided by the remote server when they connect to the next session.

2. The feature works in the session only when the toggle in the client is turned on and the corresponding feature enabled on the VDA; a menu item, “Use Client Keyboard Layout,” in Devices > Keyboard > International is added to show the enabled state.

Limitations:

- Using the keyboard layouts listed in “Supported Keyboard Layouts in Mac” works while using this feature. When you change the client keyboard layout to a non-compatible layout, the layout might be synced on the VDA side, but functionality cannot be confirmed.

- Remote applications that run with elevated privileges (for example, running applications as an administrator) can’t be synchronized with the client keyboard layout. To work around this issue, manually change the keyboard layout on the VDA or disable UAC.

- When RDP is deployed as an application and the user is working within an RDP session, it is not possible to change the keyboard layout using the Alt + Shift shortcuts. To work around this issue, users can use the language bar in the RDP session to switch the keyboard layout.
## Supported keyboard layouts on Mac

<table>
<thead>
<tr>
<th>Language on Mac</th>
<th>Input source on Mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>US.</td>
</tr>
<tr>
<td></td>
<td>U.S. International - PC</td>
</tr>
<tr>
<td></td>
<td>Dvorak</td>
</tr>
<tr>
<td></td>
<td>Dvorak - Left</td>
</tr>
<tr>
<td></td>
<td>Dvorak - Right</td>
</tr>
<tr>
<td></td>
<td>British</td>
</tr>
<tr>
<td></td>
<td>British - PC</td>
</tr>
<tr>
<td></td>
<td>Canadian English</td>
</tr>
<tr>
<td></td>
<td>Australian</td>
</tr>
<tr>
<td></td>
<td>Irish</td>
</tr>
<tr>
<td>French</td>
<td>French</td>
</tr>
<tr>
<td></td>
<td>French - Numerical</td>
</tr>
<tr>
<td></td>
<td>Canadian French - CSA</td>
</tr>
<tr>
<td></td>
<td>Swiss French</td>
</tr>
<tr>
<td></td>
<td>French - PC</td>
</tr>
<tr>
<td>German</td>
<td>German</td>
</tr>
<tr>
<td></td>
<td>Austrian</td>
</tr>
<tr>
<td></td>
<td>Swiss German</td>
</tr>
<tr>
<td>Spanish</td>
<td>Spanish</td>
</tr>
<tr>
<td></td>
<td>Spanish - ISO</td>
</tr>
<tr>
<td>Bulgarian</td>
<td>Bulgarian</td>
</tr>
<tr>
<td>Swedish</td>
<td>Swedish</td>
</tr>
<tr>
<td>Czech</td>
<td>Czech</td>
</tr>
<tr>
<td>Danish</td>
<td>Danish</td>
</tr>
<tr>
<td>Finnish</td>
<td>Finnish</td>
</tr>
<tr>
<td>Hungarian</td>
<td>Hungarian</td>
</tr>
<tr>
<td>Italian</td>
<td>Italian</td>
</tr>
<tr>
<td>Greek</td>
<td>Greek</td>
</tr>
<tr>
<td>Dutch</td>
<td>Belgian</td>
</tr>
<tr>
<td></td>
<td>Dutch</td>
</tr>
<tr>
<td>Romanian</td>
<td>Romanian - Standard</td>
</tr>
<tr>
<td>Russian</td>
<td>Russian - PC</td>
</tr>
<tr>
<td>Croatian</td>
<td>Croatian - PC</td>
</tr>
<tr>
<td>Slovak</td>
<td>Slovak</td>
</tr>
<tr>
<td></td>
<td>Slovak - QWERTY</td>
</tr>
<tr>
<td>Turkish</td>
<td>Turkish</td>
</tr>
<tr>
<td></td>
<td>Turkish - QWERTY PC</td>
</tr>
<tr>
<td>Portuguese</td>
<td>Brazilian</td>
</tr>
<tr>
<td></td>
<td>Brazilian - ABNT2</td>
</tr>
<tr>
<td></td>
<td>Portuguese</td>
</tr>
<tr>
<td>Ukrainian</td>
<td>Ukrainian - PC</td>
</tr>
<tr>
<td>Belarusian</td>
<td>Belarusian</td>
</tr>
<tr>
<td>Slovenian</td>
<td>Slovenian</td>
</tr>
<tr>
<td>Estonian</td>
<td>Estonian</td>
</tr>
<tr>
<td>Latvian</td>
<td>Latvian</td>
</tr>
<tr>
<td>Polish</td>
<td>Polish</td>
</tr>
<tr>
<td></td>
<td>Polish Pro</td>
</tr>
<tr>
<td>Icelandic</td>
<td>Icelandic</td>
</tr>
<tr>
<td>Norwegian</td>
<td>Norwegian</td>
</tr>
<tr>
<td>Japanese</td>
<td>Hiragana</td>
</tr>
<tr>
<td></td>
<td>Katakana</td>
</tr>
<tr>
<td></td>
<td>Romaji</td>
</tr>
<tr>
<td>Korean</td>
<td>2-Set Korean</td>
</tr>
<tr>
<td></td>
<td>3-Set Korean</td>
</tr>
<tr>
<td>Chinese, Simplified</td>
<td></td>
</tr>
<tr>
<td>Chinese, Traditional</td>
<td></td>
</tr>
</tbody>
</table>
Language bar

You can choose to show or hide the remote language bar in an application session using the graphical user interface. The language bar displays the preferred input language in a session. In earlier releases, you might change this setting using only the registry keys on the VDA. Starting with Citrix Workspace for Mac version 1808, you can change the settings using the Preferences dialog. The language bar appears in a session by default.

Note:
This feature is available in sessions running on VDA 7.17 and later.

Configure showing or hiding the remote language bar

1. Open Preferences.
2. Click Keyboard.
3. Click or unclick Show the remote language bar for the published applications.

Note:
The setting changes take effect immediately. You can change the settings in an active session. The remote language bar does not appear in a session if there is only one input language.

Optimize

September 21, 2018

Reconnecting users automatically

Users can be disconnected from their sessions because of unreliable networks, highly variable network latency, or range limitations of wireless devices. With the auto-client reconnection feature, Citrix Workspace app for Mac can detect unintended disconnections of ICA sessions and reconnect users to the affected sessions automatically.

When this feature is enabled on the server, users do not have to reconnect manually to continue working. Citrix Workspace app for Mac attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts. If user authentication is required, a dialog box requesting credentials appears to a user during automatic reconnection. Automatic reconnection does not occur if users exit applications without logging off.

You configure auto-client reconnect using policy settings on the server.
**Restarting desktops**

Users can restart a virtual desktop if it fails to start, takes too long to connect to, or becomes corrupted. You configure this feature in Citrix Virtual Apps and Desktops.

The contextual menu item **Restart** is available on all of the desktops that users subscribe to, and on users' App page. The menu item is disabled if restart is not enabled for the desktop. When the user chooses Restart, Citrix Workspace app for Mac shuts down the desktop and then starts it.

**Important**

Make users aware that restarting desktops can result in data loss.

**Providing session reliability**

With the Session Reliability feature, users continue to see hosted application and desktop windows if the connection experiences an interruption. For example, wireless users entering a tunnel may lose their connection when they enter the tunnel and regain it when they emerge on the other side. During such interruptions, the session reliability feature enables the session window to remain displayed while the connection is being restored.

You can configure your system to display a warning dialog box to users when the connection is unavailable.

You configure Session Reliability using policy settings on the server.

**Tip**

Citrix Workspace app for Mac users cannot override the server settings for Session Reliability.

**Important**

If Session Reliability is enabled, the default port used for session communication switches from 1494 to 2598.

**Providing continuity for roaming users**

Workspace control lets desktops and applications follow users as they move between devices. This enables, for example, clinicians in hospitals to move from workstation to workstation without having to restart their desktops and applications on each device.

Policies and client drive mappings change appropriately when you move to a new user device. Policies and mappings are applied according to the user device where you are currently logged on to the session. For example, if a health care worker logs off from a user device in the emergency room of a
hospital and then logs on to a workstation in the hospital's X-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the X-ray laboratory go into effect for the session as soon as the user logs on to the user device in the X-ray laboratory.

**To configure workspace control settings**

1. Click the down arrow icon in the Citrix Workspace app for Mac window and choose Preferences.
2. Click General tab.
3. Choose one of the following:
   - Reconnect apps when I start Citrix Workspace app. Allows users to reconnect to disconnected apps when they start Citrix Workspace app.
   - Reconnect apps when I start or refresh apps. Allows users to reconnect to disconnected apps either when they start apps or when they select Refresh Apps from the Citrix Workspace app for Mac menu.

**Mapping client devices**

Citrix Workspace app for Mac maps local drives and devices automatically so that they are available from within a session. If enabled on the server, client device mapping allows a remote application or desktop running on the server to access devices attached to the local user device. You can:

- Access local drives, COM ports, and printers
- Hear audio (system sounds and audio files) played from the session

**Note**

Client audio mapping and client printer mapping do not require any configuration on the user device.

**Mapping client drives**

Client drive mapping allows you to access local drives on the user device, for example, CD-ROM drives, DVDs, and USB memory sticks, during sessions. When a server is configured to allow client drive mapping, users can access their locally stored files, work with them during sessions, and then save them either on a local drive or on a drive on the server.

Citrix Workspace app for Mac monitors the directories in which hardware devices such as CD-ROMs, DVDs and USB memory sticks are typically mounted on the user device and automatically maps any new ones that appear during a session to the next available drive letter on the server.
You can configure the level of read and write access for mapped drives using Citrix Workspace app for Mac preferences.

**To configure read and write access for mapped drives**

1. On the Citrix Workspace app for Mac home page, click the down arrow icon, and then click **Preferences**.
2. Click **Devices**.
3. Select the level of read and write access for mapped drives from the following options:
   - Read and Write
   - Read only
   - No access
   - Ask me each time
4. Log off from any open sessions and reconnect to apply the changes.

**Improving the user experience**

September 21, 2018

**Customer Experience Improvement Program (CEIP)**

The Citrix Customer Experience Improvement Program (CEIP) gathers anonymous configuration and usage data from Citrix Workspace app for Mac and automatically sends the data to Citrix. This data helps Citrix improve the quality, reliability, and performance of Citrix Workspace app for Mac.

**ClearType font smoothing**

ClearType font smoothing (also known as Sub-pixel font rendering) improves the quality of displayed fonts beyond that available through traditional font smoothing or anti-aliasing.

If you enable ClearType font smoothing on the server, you are not forcing user devices to use ClearType font smoothing. You are enabling the server to support ClearType font smoothing on user devices that have it enabled locally and are using Citrix Workspace app for Mac.

Citrix Workspace app for Mac automatically detects the user device's font smoothing setting and sends it to the server. The session connects using this setting. When the session is disconnected or terminated, the server's setting reverts to its original setting.
**Client-side microphone input**

Citrix Workspace app for Mac supports multiple client-side microphone input. Locally installed microphones can be used for:

- Real-time activities, such as softphone calls and Web conferences.
- Hosted recording applications, such as dictation programs.
- Video and audio recordings.

Digital dictation support is available with Citrix Workspace app for Mac.

You can select whether or not to use microphones attached to your user device in sessions by choosing one of the following options from the Mic & Webcam tab in Citrix Workspace app for Mac > Preferences:

- Use my microphone and webcam
- Don’t use my microphone and webcam
- Ask me each time

If you select **Ask me each time**, a dialog box appears each time you connect to a hosted application or desktop asking whether or not you want to use your microphone in that session.

**Windows special keys**

Citrix Workspace app for Mac provides a number of extra options and easier ways to substitute special keys such as function keys in Windows applications with Mac keys. Use the Keyboard tab to configure the options you want to use, as follows:

- “Send Control character using” lets you choose whether or not to send Command-character keystroke combinations as Ctrl+character key combinations in a session. If you select “Command or Control” from the pop-up menu, you can send familiar Command-character or Ctrl-character keystroke combinations on the Mac as Ctrl+character key combinations to the PC. If you select Control, you must use Ctrl-character keystroke combinations.
- “Send Alt character using” lets you choose how to replicate the Alt key within a session. If you select Command-Option, you can send Command-Option-keystroke combinations as Alt+key combinations within a session. Alternatively, if you select Command, you can use the Command key as the Alt key.
- “Send Windows logo key using Command (right)” lets you send the Windows logo key to your remote desktops and applications by pressing the Command key situated on the right side of the keyboard. If this option is disabled, the right Command key has the same behavior as the left Command key according to the above two settings in the preferences panel, but you can still send the Windows logo key using the Keyboard menu; choose Keyboard > Send Windows Shortcut > Start.
- “Send special keys unchanged” lets you disable the conversion of special keys. For example, the combination Option-1 (on the numeric keypad) is equivalent to the special key F1. You can
change this behavior and set this special key to represent 1 (the number one on the keypad) in
the session by selecting the “Send special keys unchanged” checkbox. By default, this checkbox
is not selected so Option-1 is sent to the session as F1.

You send function and other special keys to a session using the Keyboard menu.

If your keyboard includes a numeric keypad, you can also use the following keystrokes:

<table>
<thead>
<tr>
<th>PC key or action</th>
<th>Mac options</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSERT</td>
<td>0 (the number zero) on the numeric keypad. Num Lock must be off; you can turn this on and off using the Clear key; Option-Help</td>
</tr>
<tr>
<td>DELETE</td>
<td>Decimal point on the numeric keypad. Num Lock must be off; you can turn this on and off using the Clear key; Clear</td>
</tr>
<tr>
<td>F1 to F9</td>
<td>Option-1 to -9 (the numbers one to nine) on the numeric keypad</td>
</tr>
<tr>
<td>F10</td>
<td>Option-0 (the number zero) on the numeric keypad</td>
</tr>
<tr>
<td>F11</td>
<td>Option-Minus Sign on the numeric keypad</td>
</tr>
<tr>
<td>F12</td>
<td>Option-Plus Sign on the numeric keypad</td>
</tr>
</tbody>
</table>

Windows shortcuts and key combinations

Remote sessions recognize most Mac keyboard combinations for text input, such as Option-G to input the copyright symbol ©. Some keystrokes you make during a session, however, do not appear on the remote application or desktop and instead are interpreted by the Mac operating system. This can result in keys triggering Mac responses instead.

You might also want to use certain Windows keys, such as Insert, that many Mac keyboards do not have. Similarly, some Windows 8 keyboard shortcuts display charms and app commands, and snap and switch apps. These shortcuts are not mimicked natively by Mac keyboards but can be sent to the remote desktop or application using the Keyboard menu.

Keyboards and the ways keys are configured can differ widely between machines. Citrix Workspace app for Mac therefore offers several choices to ensure that keystrokes can be forwarded correctly to hosted applications and desktops. These are listed in the table. The default behavior is described. If you adjust the defaults (using Citrix Workspace app for Mac or other preferences), different keystroke combinations may be forwarded and other behavior may be observed on the remote PC.
## Important

Certain key combinations listed in the table are not available when using newer Mac keyboards. In most of these cases, keyboard input can be sent to the session using the Keyboard menu.

**Conventions used in the table:**

- Letter keys are capitalized and do not imply that the Shift key should be pressed simultaneously.
- Hyphens between keystrokes indicate that keys should be pressed together (for example, Control-C).
- Character keys are those that create text input and include all letters, numbers, and punctuation marks; special keys are those that do not create input by themselves but act as modifiers or controllers. Special keys include Control, Alt, Shift, Command, Option, arrow keys, and function keys.
- Menu instructions relate to the menus in the session.
- Depending on the configuration of the user device, some key combinations might not work as expected, and alternative combinations are listed.
- Fn refers to the Fn (Function) key on a Mac keyboard; function key refers to F1 to F12 on either a PC or Mac keyboard.

<table>
<thead>
<tr>
<th>Windows key or key combination</th>
<th>Mac equivalents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alt+character key</td>
<td>Command–Option–character key (for example, to send Alt-C, use Command-Option-C)</td>
</tr>
<tr>
<td>Alt+special key</td>
<td>Option–special key (for example, Option-Tab); Command–Option–special key (for example, Command-Option-Tab)</td>
</tr>
<tr>
<td>Ctrl+character key</td>
<td>Command–character key (for example, Command-C); Control–character key (for example, Control-C)</td>
</tr>
<tr>
<td>Ctrl+special key</td>
<td>Control–special key (for example, Control-F4); Command–special key (for example, Command-F4)</td>
</tr>
<tr>
<td>Ctrl/Alt/Shift/Windows logo + function key</td>
<td>Choose Keyboard &gt; Send Function key &gt; Control/Alt/Shift/Command-Function key</td>
</tr>
<tr>
<td>Ctrl+Alt</td>
<td>Control-Option-Command</td>
</tr>
<tr>
<td>Ctrl+Alt+Delete</td>
<td>Control–Option–Forward Delete; Control-Option-Fn-Delete (on MacBook keyboards); Choose Keyboard &gt; Send Ctrl-Alt-Del</td>
</tr>
<tr>
<td>Windows key or key combination</td>
<td>Mac equivalents</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete; Choose Keyboard &gt; Send Key &gt; Delete; Fn-Backspace (Fn-Delete on some US keyboards)</td>
</tr>
<tr>
<td>End</td>
<td>End; Fn-Right Arrow</td>
</tr>
<tr>
<td>Esc</td>
<td>Escape; Choose Keyboard &gt; Send Key &gt; Escape</td>
</tr>
<tr>
<td>F1 to F12</td>
<td>F1 to F12; Choose Keyboard &gt; Send Function Key &gt; F1 to F12</td>
</tr>
<tr>
<td>Home</td>
<td>Home; Fn-Left Arrow</td>
</tr>
<tr>
<td>Insert</td>
<td>Choose Keyboard &gt; Send Key &gt; Insert</td>
</tr>
<tr>
<td>Num Lock</td>
<td>Clear</td>
</tr>
<tr>
<td>Page Down</td>
<td>Page Down; Fn-Down Arrow</td>
</tr>
<tr>
<td>Page Up</td>
<td>Page Up; Fn-Up Arrow</td>
</tr>
<tr>
<td>Spacebar</td>
<td>Choose Keyboard &gt; Send Key &gt; Space</td>
</tr>
<tr>
<td>Tab</td>
<td>Choose Keyboard &gt; Send Key &gt; Tab</td>
</tr>
<tr>
<td>Windows logo</td>
<td>Right Command key (a keyboard preference, enabled by default); Choose Keyboard &gt; Send Windows Shortcut &gt; Start</td>
</tr>
<tr>
<td>Key combination to display charms</td>
<td>Choose Keyboard &gt; Send Windows Shortcut &gt; Charms</td>
</tr>
<tr>
<td>Key combination to display app commands</td>
<td>Choose Keyboard &gt; Send Windows Shortcut &gt; App Commands</td>
</tr>
<tr>
<td>Key combination to snap apps</td>
<td>Choose Keyboard &gt; Send Windows Shortcut &gt; Snap</td>
</tr>
<tr>
<td>Key combination to switch apps</td>
<td>Choose Keyboard &gt; Send Windows Shortcut &gt; Switch Apps</td>
</tr>
</tbody>
</table>

**Use Input Method Editors (IME) and international keyboard layouts**

Citrix Workspace app for Mac allows you to use an Input Method Editor (IME) on either the user device or on the server.

When client-side IME is enabled, users can compose text at the insertion point rather than in a separate window.
Citrix Workspace app for Mac

Citrix Workspace app for Mac also allows users to specify the keyboard layout they wish to use.

**To enable client-side IME**

1. From the Citrix Viewer menu bar, choose **Keyboard > International > Use Client IME**.
2. Ensure the server-side IME is set to direct input or alphanumeric mode.
3. Use the Mac IME to compose text.

**To indicate explicitly the starting point when composing text**

- From the Citrix Viewer menu bar, choose **Keyboard > International > Use Composing Mark**.

**To use server-side IME**

- Ensure the client-side IME is set to alphanumeric mode.

**Mapped server-side IME input mode keys**

Citrix Workspace app for Mac provides keyboard mappings for server-side Windows IME input mode keys that are not available on Mac keyboards. On Mac keyboards, the Option key is mapped to the following server-side IME input mode keys, depending on the server-side locale:

<table>
<thead>
<tr>
<th>Server-side system locale</th>
<th>Server-side IME input mode key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japanese</td>
<td>Kanji key (Alt + Hankaku/Zenkaku in Japanese keyboard)</td>
</tr>
<tr>
<td>Korean</td>
<td>Right-Alt key (Hangul/English toggle on Korean keyboard)</td>
</tr>
</tbody>
</table>

**To use international keyboard layouts**

- Ensure both client-side and server-side keyboard layouts are set to the same locale as the default server-side input language.

**Using multiple monitors**

Users can set Citrix Workspace app for Mac to work in full-screen mode across multiple monitors through the menu option, **Use All Displays In Full Screen**.
Known Limitations

Full-screen mode is only supported on one monitor or all monitors, which is configurable through a menu item.

Using the Desktop toolbar

Users can now access the Desktop Toolbar in both windowed and full-screen mode. Previously, the toolbar was only visible in full-screen mode. Additional toolbar changes include:

- The Home button has been removed from the toolbar. This function can be executed by using the following commands:
  - Cmd-Tab to switch to the previous active application.
  - Ctrl-Left Arrow to switch to the previous Space.
  - Using the built-in trackpad or Magic Mouse gestures to switch to a different Space.
  - Moving the cursor to the edge of screen while in full-screen mode will display a Dock where you can choose which applications to make active.
- The Windowed button has been removed from the toolbar. Leaving full-screen mode for windowed mode can be executed by the following methods:
  - For OS X 10.10, clicking the green window button on the drop-down menu bar.
  - For OS X 10.9, clicking the blue menu button on the drop-down menu bar.
  - For all versions of OS X, selecting Exit Full Screen from the View menu of the drop-down menu bar.
- The toolbar drag behavior is updated to support dragging between windows in full screen with multiple monitors.

Secure communications

September 21, 2018

To secure the communication between your server farm and Citrix Workspace app for Mac, you can integrate your connections to the server farm with a range of security technologies, including Citrix NetScaler Gateway. For information about configuring this with Citrix StoreFront, see the StoreFront documentation.

Note:

Citrix recommends using NetScaler Gateway to secure communications between StoreFront servers and users’ devices.
• A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server). You can use proxy servers to limit access to and from your network and to handle connections between Citrix Workspace and servers. Citrix Workspace app for Mac supports SOCKS and secure proxy protocols.
• Secure Gateway. You can use Secure Gateway with the Web Interface to provide a single, secure, encrypted point of access through the Internet to servers on internal corporate networks.
• SSL Relay solutions with Transport Layer Security (TLS) protocols
• A firewall. Network firewalls can allow or block packets based on the destination address and port. If you are using Citrix Workspace app for Mac through a network firewall that maps the server’s internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.

About certificates

Private (Self-signed) certificates

If a private certificate is installed on the remote gateway, the root certificate for the organization’s certificate authority must be installed on the user device to successfully access Citrix resources using Citrix Workspace app for Mac.

Note:

If the remote gateway’s certificate cannot be verified upon connection (because the root certificate is not included in the local keystore), an untrusted certificate warning appears. If a user chooses to continue through the warning, a list of applications is displayed; however, applications fail to launch.

Importing root certificates on Citrix Workspace app for Mac devices

Obtain the certificate issuer’s root certificate and email it to an account configured on your device. When clicking the attachment, you are asked to import the root certificate.

Wildcard certificates

Wildcard certificates are used in place of individual server certificates for any server within the same domain. Citrix Workspace app for Mac supports wildcard certificates.

Intermediate certificates with NetScaler Gateway

If your certificate chain includes an intermediate certificate, the intermediate certificate must be mapped to the NetScaler Gateway server certificate. For information on this task, see NetScaler
Gateway documentation. For more information about installing and linking an intermediate certificate with Primary CA on a NetScaler Gateway appliance, refer to the article How to Install and Link Intermediate Certificate with Primary CA on NetScaler Gateway.

Joint Server Certificate Validation Policy

Citrix Workspace app for Mac has a stricter validation policy for server certificates.

Important

Before installing this version of Citrix Workspace app for Mac, confirm that the certificates at the server or gateway are correctly configured as described here. Connections may fail if:
- the server or gateway configuration includes a wrong root certificate
- the server or gateway configuration does not include all intermediate certificates
- the server or gateway configuration includes an expired or otherwise invalid intermediate certificate
- the server or gateway configuration includes a cross-signed intermediate certificate

When validating a server certificate, Citrix Workspace app for Mac now uses all the certificates supplied by the server (or gateway) when validating the server certificate. As in previous Citrix Workspace app for Mac releases, it then also checks that the certificates are trusted. If the certificates are not all trusted, the connection fails.

This policy is stricter than the certificate policy in web browsers. Many web browsers include a large set of root certificates that they trust.

The server (or gateway) must be configured with the correct set of certificates. An incorrect set of certificates might cause Citrix Workspace app for Mac’s connection to fail.

Suppose a gateway is configured with these valid certificates. This configuration is recommended for customers who require stricter validation, by determining exactly which root certificate is used by Citrix Workspace app for Mac:
- “Example Server Certificate”
- “Example Intermediate Certificate”
- “Example Root Certificate”

Then, Citrix Workspace app for Mac will check that all these certificates are valid. Citrix Workspace app for Mac will also check that it already trusts “Example Root Certificate”. If Citrix Workspace app for Mac does not trust “Example Root Certificate”, the connection fails.

Important

Some certificate authorities have more than one root certificate. If you require this stricter validation, make sure that your configuration uses the appropriate root certificate. For example, there
are currently two certificates (“DigiCert”/“GTE CyberTrust Global Root”, and “DigiCert Baltimore Root”/“Baltimore CyberTrust Root”) that can validate the same server certificates. On some user devices, both root certificates are available. On other devices, only one is available (“DigiCert Baltimore Root”/“Baltimore CyberTrust Root”). If you configure “GTE CyberTrust Global Root” at the gateway, Citrix Workspace app for Mac connections on those user devices will fail. Consult the certificate authority’s documentation to determine which root certificate should be used. Also note that root certificates eventually expire, as do all certificates.

Note

Some servers and gateways never send the root certificate, even if configured. Stricter validation is then not possible.

Now suppose a gateway is configured with these valid certificates. This configuration, omitting the root certificate, is normally recommended:

- “Example Server Certificate”
- “Example Intermediate Certificate”

Then, Citrix Workspace app for Mac will use these two certificates. It will then search for a root certificate on the user device. If it finds one that validates correctly, and is also trusted (such as “Example Root Certificate”), the connection succeeds. Otherwise, the connection fails. Note that this configuration supplies the intermediate certificate that Citrix Workspace app for Mac needs, but also allows Citrix Workspace app for Mac to choose any valid, trusted, root certificate.

Now suppose a gateway is configured with these certificates:

- “Example Server Certificate”
- “Example Intermediate Certificate”
- “Wrong Root Certificate”

A web browser may ignore the wrong root certificate. However, Citrix Workspace app for Mac will not ignore the wrong root certificate, and the connection will fail.

Some certificate authorities use more than one intermediate certificate. In this case, the gateway is normally configured with all the intermediate certificates (but not the root certificate) such as:

- “Example Server Certificate”
- “Example Intermediate Certificate 1”
- “Example Intermediate Certificate 2”

Important

Some certificate authorities use a cross-signed intermediate certificate. This is intended for situations there is more than one root certificate, and a earlier root certificate is still in use at the same time as a later root certificate. In this case, there will be at least two intermediate certificates. For example, the earlier root certificate “Class 3 Public Primary Certification Authority” has the cor-
responding cross-signed intermediate certificate “VeriSign Class 3 Public Primary Certification Authority - G5”. However, a corresponding later root certificate “VeriSign Class 3 Public Primary Certification Authority - G5” is also available, which replaces “Class 3 Public Primary Certification Authority”. The later root certificate does not use a cross-signed intermediate certificate.

**Note**

The cross-signed intermediate certificate and the root certificate have the same Subject name (Issued To), but the cross-signed intermediate certificate has a different Issuer name (Issued By). This distinguishes the cross-signed intermediate certificate from an ordinary intermediate certificate (such “Example Intermediate Certificate 2”).

This configuration, omitting the root certificate and the cross-signed intermediate certificate, is normally recommended:

- “Example Server Certificate”
- “Example Intermediate Certificate”

Avoid configuring the gateway to use the cross-signed intermediate certificate, as it will select the earlier root certificate:

- “Example Server Certificate”
- “Example Intermediate Certificate”
- “Example Cross-signed Intermediate Certificate” [not recommended]

It is not recommended to configure the gateway with only the server certificate:

- “Example Server Certificate”

In this case, if Citrix Workspace app for Mac cannot locate all the intermediate certificates, the connection will fail.

**Connecting with NetScaler Gateway**

To enable remote users to connect to your XenMobile deployment through NetScaler Gateway, you can configure these to work with StoreFront. The method for enabling access depends on the edition of XenMobile in your deployment.

If you deploy XenMobile in your network, allow connections from internal or remote users to StoreFront through NetScaler Gateway by integrating NetScaler Gateway with StoreFront. This deployment allows users to connect to StoreFront to access published applications from XenApp and virtual desktops from XenDesktop. Users connect through Citrix Workspace app for Mac.

**Connecting with the Secure Gateway**

This topic applies only to deployments using the Web Interface.
You can use the Secure Gateway in either Normal mode or Relay mode to provide a secure channel for communication between Citrix Workspace app for Mac and the server. No configuration of Citrix Workspace app for Mac is required if you are using the Secure Gateway in Normal mode and users are connecting through the Web Interface.

Citrix Workspace app for Mac uses settings that are configured remotely on the Web Interface server to connect to servers running the Secure Gateway. For more information about configuring proxy server settings for Citrix Workspace app for Mac, see the Web Interface documentation.

If the Secure Gateway Proxy is installed on a server in the secure network, you can use the Secure Gateway Proxy in Relay mode. For more information about Relay mode, see the XenApp and Secure Gateway documentation.

If you are using Relay mode, the Secure Gateway server functions as a proxy and you must configure Citrix Workspace app for Mac to use:

- The fully qualified domain name (FQDN) of the Secure Gateway server.
- The port number of the Secure Gateway server. Note that Relay mode is not supported by Secure Gateway Version 2.0.

The FQDN must list, in sequence, the following three components:

- Host name
- Intermediate domain
- Top-level domain

For example, my_computer.example.com is a FQDN, because it lists, in sequence, a host name (my_computer), an intermediate domain (example), and a top-level domain (com). The combination of intermediate and top-level domain (example.com) is generally referred to as the domain name.

Connecting through a proxy server

Proxy servers are used to limit access to and from your network, and to handle connections between Citrix Workspace app for Mac and servers. Citrix Workspace app for Mac supports both SOCKS and secure proxy protocols.

When communicating with the XenApp or XenDesktop server, Citrix Workspace app for Mac uses proxy server settings that are configured remotely on the Web Interface server. For information about configuring proxy server settings for Citrix Workspace, see the Web Interface documentation.

When communicating with the Web server, Citrix Workspace app for Mac uses the proxy server settings that are configured for the default web browser on the user device. You must configure the proxy server settings for the default Web browser on the user device accordingly.
Connecting through a firewall

Network firewalls can allow or block packets based on the destination address and port. If you are using a firewall in your deployment, Citrix Workspace app for Mac must be able to communicate through the firewall with both the Web server and Citrix server. The firewall must permit HTTP traffic (often over the standard HTTP port 80 or 443 if a secure Web server is in use) for user device to Web server communication. For Citrix Workspace to Citrix server communication, the firewall must permit inbound ICA traffic on ports 1494 and 2598.

If the firewall is configured for Network Address Translation (NAT), you can use the Web Interface to define mappings from internal addresses to external addresses and ports. For example, if your XenApp or XenDesktop server is not configured with an alternate address, you can configure the Web Interface to provide an alternate address to Citrix Workspace app for Mac. Citrix Workspace app for Mac then connects to the server using the external address and port number. For more information, see the Web Interface documentation.

Connecting using TLS

Citrix Workspace app for Mac supports TLS 1.0, 1.1 and 1.2 with the following cipher suites for TLS connections to XenApp/XenDesktop:

**TLS:**
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

**DTLS:**
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

**Note:**

Citrix Workspace app for Mac running on Mac OS Sierra does not support the following TLS cipher suites:
- TLS_RSA_WITH_RC4_128_SHA
Transport Layer Security (TLS) is the latest, standardized version of the TLS protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of TLS as an open standard.

TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations may also require the use of validated cryptography, such as Federal Information Processing Standard (FIPS) 140. FIPS 140 is a standard for cryptography.

Citrix Workspace app for Mac supports RSA keys of 1024, 2048, and 3072-bit lengths. Root certificates with RSA keys of 4096-bit length are also supported.

**Note**

Citrix Workspace app for Mac uses platform (OS X) crypto for connections between Citrix Workspace app for Mac and StoreFront.

### Configuring and enabling Citrix Workspace app for Mac for TLS

There are two main steps involved in setting up TLS:

1. Set up SSL Relay on your XenApp or XenDesktop server and your Web Interface server and obtain and install the necessary server certificate.
2. Install the equivalent root certificate on the user device.

### Installing root certificates on user devices

To use TLS to secure communications between TLS-enabled Citrix Workspace app for Mac and the server farm, you need a root certificate on the user device that can verify the signature of the Certificate Authority on the server certificate.

Mac OS X comes with about 100 commercial root certificates already installed, but if you want to use another certificate, you can obtain one from the Certificate Authority and install it on each user device.

Depending on your organization’s policies and procedures, you may want to install the root certificate on each user device instead of directing users to install it. The easiest and safest way is to add root certificates to the Mac OS X keychain.
To add a root certificate to the keychain

1. Double-click the file containing the certificate. This automatically starts the Keychain Access application.
2. In the Add Certificates dialog box, choose one of the following from the Keychain pop-up menu:
   - login (The certificate applies only to the current user.)
   - System (The certificate applies to all users of a device.)
3. Click OK.
4. Type your password in the Authenticate dialog box and then click OK.

The root certificate is installed and can be used by TLS-enabled clients and by any other application using TLS.

About TLS policies

This section provides information for configuring security policies for ICA sessions over TLS in Citrix Workspace app for Mac. You can configure certain TLS settings used for ICA connections in Citrix Workspace app for Mac. These settings are not exposed in the user interface; changing them requires running a command on the device running Citrix Workspace app for Mac.

Note

TLS policies can be managed in other ways, such as when devices are controlled by OS X server or another mobile device management solution.

TLS policies include the following settings:

**SecurityComplianceMode.** Sets the security compliance mode for the policy. If you don’t configure SecurityComplianceMode, FIPS is used as the default value. Applicable values for this setting include:

- **None.** No compliance mode is enforced
- **FIPS.** FIPS cryptographic modules are used
- **SP800-52.** NIST SP800-52r1 compliance is enforced

```bash
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52```

**SecurityAllowedTLSVersions.** This setting specifies the TLS protocol versions that should be accepted during protocol negotiation. This information is represented as an array and any combination of the possible values is supported. When this setting is not configured, the values TLS10, TLS11 and TLS12 are used as the default values. Applicable values for this setting include:

- **TLS10.** Specifies that the TLS 1.0 protocol is allowed.
- **TLS11.** Specifies that the TLS 1.1 protocol is allowed.
- **TLS12.** Specifies that the TLS 1.2 protocol is allowed.
SSLertificateRevocationCheckPolicy. This feature improves the cryptographic authentication of the Citrix server and improves the overall security of the SSL/TLS connections between a client and a server. This setting governs how a given trusted root certificate authority is treated during an attempt to open a remote session through SSL when using the client for OS X.

When you enable this setting, the client checks whether or not the server’s certificate is revoked. There are several levels of certificate revocation list checking. For example, the client can be configured to check only its local certificate list, or to check the local and network certificate lists. In addition, certificate checking can be configured to allow users to log on only if all Certificate Revocation lists are verified.

Certificate Revocation List (CRL) checking is an advanced feature supported by some certificate issuers. It allows an administrator to revoke security certificates (invalidated before their expiry date) in the case of cryptographic compromise of the certificate private key, or simply an unexpected change in DNS name.

Applicable values for this setting include:

- **NoCheck.** No Certificate Revocation List check is performed.
- **CheckWithNoNetworkAccess.** Certificate revocation list check is performed. Only local certificate revocation list stores are used. All distribution points are ignored. Finding a Certificate Revocation List is not critical for verification of the server certificate presented by the target SSL Relay/Secure Gateway server.
- **FullAccessCheck.** Certificate Revocation List check is performed. Local Certificate Revocation List stores and all distribution points are used. Finding a Certificate Revocation List is not critical for verification of the server certificate presented by the target SSL Relay/Secure Gateway server.
- **FullAccessCheckAndCRLRequired.** Certificate Revocation List check is performed, excluding the root CA. Local Certificate Revocation List stores and all distribution points are used. Finding all required Certificate Revocation Lists is critical for verification.
- **FullAccessCheckAndCRLRequiredAll.** Certificate Revocation List check is performed, including the root CA. Local Certificate Revocation List stores and all distribution points are used. Finding all required Certificate Revocation Lists is critical for verification.

**Note**

If you don’t set SSLCertificateRevocationCheckPolicy, FullAccessCheck is used as the default value.

defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy
    FullAccessCheckAndCRLRequired
Configuring TLS policies

To configure TLS settings on an unmanaged computer, run the `defaults` command in Terminal.app. `defaults` is a command line application that you can use to add, edit, and delete app settings in an OS X preferences plist file.

To change settings:

1. Open Applications > Utilities > Terminal.
2. In Terminal, run the command:

```
defaults write com.citrix.receiver.nomas \<name\> \<type\> \<value\>
```

Where:

\<name\>: The name of the setting as described above.
\<type\>: A switch identifying the type of the setting, either -string or -array. If the setting type is a string, this can be omitted.
\<value\>: The value for the setting. If the value is an array and you are specifying multiple values, the values must be separated by a space.

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

Reverting to the default configuration

To reset a setting back to its default:

1. Open Applications > Utilities > Terminal.
2. In Terminal, run the command:

```
defaults delete com.citrix.receiver.nomas \<name\>
```

Where:

\<name\>: The name of the setting as described above.

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```

Using the UI to configure security settings

Numerous security improvements and enhancements were introduced with Citrix Receiver for Mac version 12.3, including:
Citrix Workspace app for Mac

• improved security configuration user interface. In previous releases, the command line was the preferred method to make security-related changes; configuration settings related to session security are now simple and accessible from the UI, which improves the user experience while creating a seamless method for the adoption of security-related preferences.

• view TLS connections. Citrix Workspace app for Mac allows you to verify connections made to servers that are using a specific TLS version, with additional information including the encryption algorithm used for the connection, mode, key size and whether SecureICA is enabled. In addition, you can view the server certificate for TLS connections.

The improved **Security and Privacy** screen includes the following new options in the **TLS** tab:

• set the compliance mode
• configure the crypto module
• select the appropriate TLS version
• select the certificate revocation list
• enable settings for all TLS connections

The image below illustrates the Security and Privacy settings accessible from the UI:
Requirements for smart card authentication

September 21, 2018

Citrix Workspace app for Mac supports smart card authentication in the following configurations:

- Smart card authentication to Workspace for Web/StoreFront 2.x and later, Citrix Virtual Apps and Desktops 7 1808 and later, and XenDesktop 7.1 and later or XenApp 6.5 and later.

- Smart card-enabled applications, such as Microsoft Outlook and Microsoft Office, allow users to digitally sign or encrypt documents available in virtual desktop or application sessions.

- With multiple certificates— Citrix Workspace app for Mac supports using multiple certificates with a single smart card or with multiple smart cards. When your user inserts a smart card into a card reader, the certificates are available to all applications running on the device, including Citrix Workspace app for Mac.

- In double-hop sessions— if a double-hop is required, a further connection is established between Citrix Workspace app for Mac and your user’s virtual desktop.

About smart card authentication to Citrix Gateway

When using a smart card to authenticate a connection when there are multiple usable certificates on the smart card, Citrix Workspace app for Mac prompts you to select a certificate. Upon selecting a certificate, Citrix Workspace app for Mac prompts you to enter the smart card password; once authenticated, the session launches.

If there is only one suitable certificate on the smart card, Citrix Workspace app for Mac uses that certificate and will not prompt you to select it. However, you must still enter the password associated with the smart card to authenticate the connection and to start the session.

Specifying a PKCS#11 module for smart card authentication

To specify PKCS#11 module for smart card authentication:

1. In Citrix Workspace app for Mac, select Preferences.
2. Click Security & Privacy.
3. In the Security & Privacy section, click Smart Card.
4. In the PKCS#11 field, select the appropriate module; click Other to browse to the location of the PKCS#11 module if the desired one is not listed.
5. After selecting the appropriate module, click Add.

**Supported readers, middleware, and smart card profiles**

Citrix Workspace app for Mac supports most macOS-compatible smart card readers and cryptographic middleware. Citrix has validated operation with the following.

Supported readers:

- Common USB connect smart card readers

Supported middleware:

- Clarify
- Activeidentity client version
- Charismathics client version

Supported smart cards:

- PIV cards
- Common Access Card (CAC)
- Gemalto .NET cards

Follow the instructions provided by your vendor’s macOS-compatible smart card reader and cryptographic middleware for configuring user devices.

**Restrictions**

- Certificates must be stored on a smart card, not on the user device.
- Citrix Workspace app for Mac does not save the user certificate choice.
- Citrix Workspace app for Mac does not store or save the user’s smart card PIN. PIN acquisitions is handled by the OS, which may have its own caching mechanism.
- Citrix Workspace app for Mac does not reconnect sessions when a smart card is inserted.
- To use VPN tunnels with smart card authentication, users must install the Citrix Gateway Plug-in and log on through a web page, using their smart cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the Citrix Gateway Plug-in is not available for smart card users.