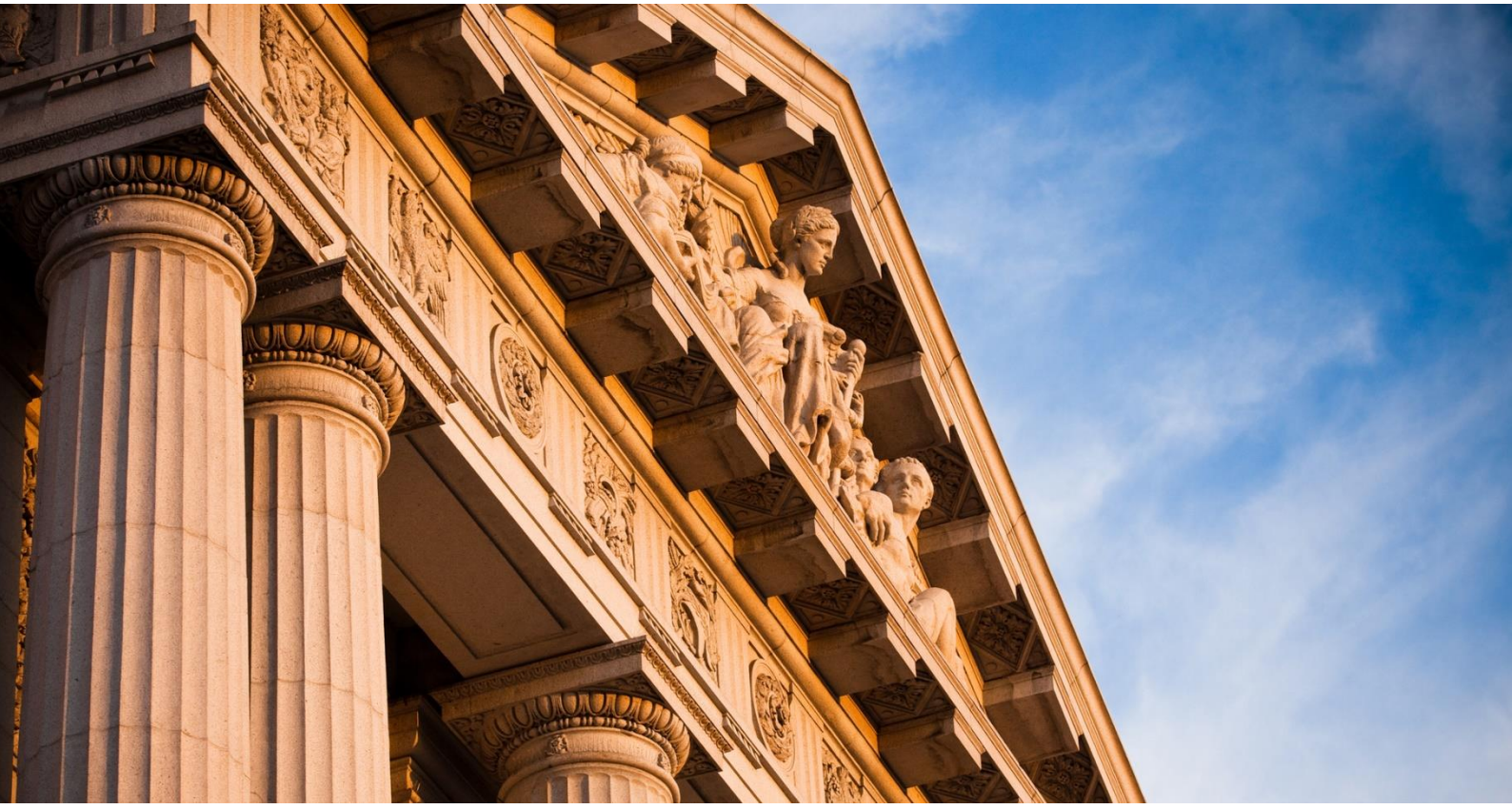
citrix

FIPS 140-2 Sample Deployments

for
Citrix Virtual Apps and Desktops 7 1912 LTSR



Contents

Introduction

When deploying Citrix Virtual Apps and Desktops within large organizations, particularly in government environments, security standards are an important consideration. Many government bodies specify a preference or requirement for applications to be compliant with Federal Information Processing Standards 140-2 (FIPS 140-2).

The document provides an overview of the security features that apply to Citrix Virtual Apps and Desktops, with an emphasis on FIPS 140-2. Sample deployments are shown, providing guidance on FIPS 140-2 compliance. For more information regarding details of the individual security features, refer to the relevant product or component documentation.

What's new

- In this document, references to *Citrix Receiver* are replaced by references to *Citrix Workspace app*, which replaces it. Citrix Workspace app works similar to Citrix Receiver and is fully backward-compatible.

Audience

This document is designed to meet the needs of security specialists, systems integrators, and consultants, particularly those working with government organizations worldwide.

Security features introduced in Citrix Virtual Apps and Desktops 7 1912 LTSR

The new security features and enhancements in Citrix Virtual Apps and Desktops 7 1912 LTSR, since the previous Long Term Service Release, provide a more streamlined route to deploy Citrix products securely and in accordance with FIPS 140-2. The new features provide the following benefits:

- We now support Windows Local Security Authority (LSA) protection, which maintains information about all aspects of local security on a system. This support provides the LSA level of system protection to hosted desktops.
- There is a broader choice of TLS 1.2 cipher suites (see Sample deployments on page 4).

FIPS 140-2 with Citrix Virtual Apps and Desktops

FIPS 140-2 is a U.S. federal government standard that details a benchmark for implementing cryptographic software. The Cryptographic Module Validation Program

(CMVP), that is administered by the U.S. National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security, allows encryption product suppliers to demonstrate the extent to which they comply with the standard and thus, the trustworthiness of their implementation.

Some U.S. government organizations restrict purchases of products and use of services from suppliers and nonfederal organizations.

The security community at large values products that follow the guidelines detailed in FIPS 140-2 and the use of FIPS 140-2-validated cryptographic modules.

To facilitate implementing secure application server access and to meet the FIPS requirements, Citrix products can use cryptographic modules that are FIPS 140-2-validated for implementations of secure TLS connections.

The following Citrix products and components included in the sample deployments can use cryptographic modules that are FIPS 140-validated:

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix ADC 12.1 MPX 1406014060 FIPS appliance
- StoreFront 1912
- Citrix Workspace app for Windows 19.11.0.50

When using these products with the TLS connections enabled, the cryptographic modules that are used are FIPS 140-2-validated. Citrix Virtual Apps and Desktops, StoreFront and Citrix Workspace app, use cryptographic modules provided by the Microsoft Windows operating system. Citrix ADC uses the FIPS 140-2-validated Cavium cryptographic module.

Sample deployments

To ensure Citrix Virtual Apps and Desktops are FIPS 140-2 compliant, you need to consider each communication channel within the deployment. The following sample deployments show how users can connect and access resources on Citrix Virtual Apps and Desktops with different configurations of components and firewalls. In particular, the samples provide general guidance on how to make each communication channel secure using TLS so that the system as a whole is FIPS 140-2 compliant.

The following sample deployments are shown:

Product	Deployment
Citrix Virtual Apps	Direct internal access [LAN] External remote access [via Internet]
Citrix Virtual Desktops	Direct internal access [LAN] External remote access [via Internet]

These deployment scenarios utilize the following components to secure data

communications using the TLS protocol. TLS provides server authentication, encryption of the data stream, and message integrity checks.

The Citrix ADC MPX FIPS hardware appliance is deployed in the DMZ to provide secure remote access to Citrix Virtual Apps and Desktops environments. It provides FIPS 140-2 Level 2 TLS encryption of traffic to encrypt and secure communication between:

- Citrix Workspace app, and the Citrix ADC MPX FIPS hardware appliance
- The Citrix ADC MPX FIPS hardware appliance and Storefront, Delivery Controller, and VDA

StoreFront provides TLS encryption and secure communication between:

- Citrix Workspace app, and the Citrix Virtual Apps and Desktops VDA (for the internal access deployment scenarios)
- Citrix Workspace app, and StoreFront (for the remote access deployment scenarios)
- Delivery Controller and StoreFront

Virtual Desktop Agent (VDA) runs on Citrix Virtual Apps and Desktops and provides encryption and secure communication between:

- Citrix Workspace app, and the Citrix Virtual Apps and Desktops VDA (for the internal access deployment scenarios)
- Citrix ADC MPX FIPS hardware appliance and the Citrix Virtual Apps and Desktops VDA (for the remote access deployment scenarios)

Citrix Virtual Apps and Desktops and Storefront can be configured to use government approved cryptography to protect data by using the applicable cipher suites:

- TLS_ECHDE_RSA_WITH_AES_256_GCM_SHA384 supports ECDHE key agreement and 256-bit keys in GCM mode for TLS connections, as defined in FIPS 197 and RFC 5289.
- TLS_ECHDE_RSA_WITH_AES_128_GCM_SHA256 supports ECDHE key agreement and 128-bit keys in GCM mode for TLS connections, as defined in FIPS 197 and RFC 5289.
- TLS_ECHDE_RSA_WITH_AES_256_CBC_SHA384 supports ECDHE key agreement and 256-bit keys for TLS connections, as defined in FIPS 197 and RFC 5289.
- TLS_ECHDE_RSA_WITH_AES_128_CBC_SHA256 supports ECDHE key agreement and 128-bit keys for TLS connections, as defined in FIPS 197 and RFC 5289.

Citrix ADC MPX FIPS hardware appliances can be configured to use government-approved cryptography to protect data by using the applicable cipher suites:

- Cipher Name: TLS1-AES-256-CBC-SHA [TLS_RSA_WITH_AES_256_CBC_SHA]
- Cipher Name: TLS1-AES-128-CBC-SHA [TLS_RSA_WITH_AES_128_CBC_SHA]
- Cipher Name: TLS-1.2-ECDHE-RSA-AES-128-SHA256 [TLS_ECHDE_RSA_WITH_AES_128_CBC_SHA256]
- Cipher Name: TLS-1.2-ECDHE-RSA-AES-256-SHA384

[TLS_ECHDE_RSA_WITH_AES_256_CBC_SHA384]

- Cipher Name: TLS-1.2-ECDHE-RSA-AES-128-GCM-SHA256 [TLS_ECHDE_RSA_WITH_AES_128_GCM_SHA256]
- Cipher Name: TLS-1.2-ECDHE-RSA-AES-256-GCM-SHA384 [TLS_ECHDE_RSA_WITH_AES_256_GCM_SHA384]

Components of Citrix Virtual Apps and Desktops, StoreFront, and Citrix ADC may support other cipher suites with government approved cryptography. These are not described in these deployment scenarios.

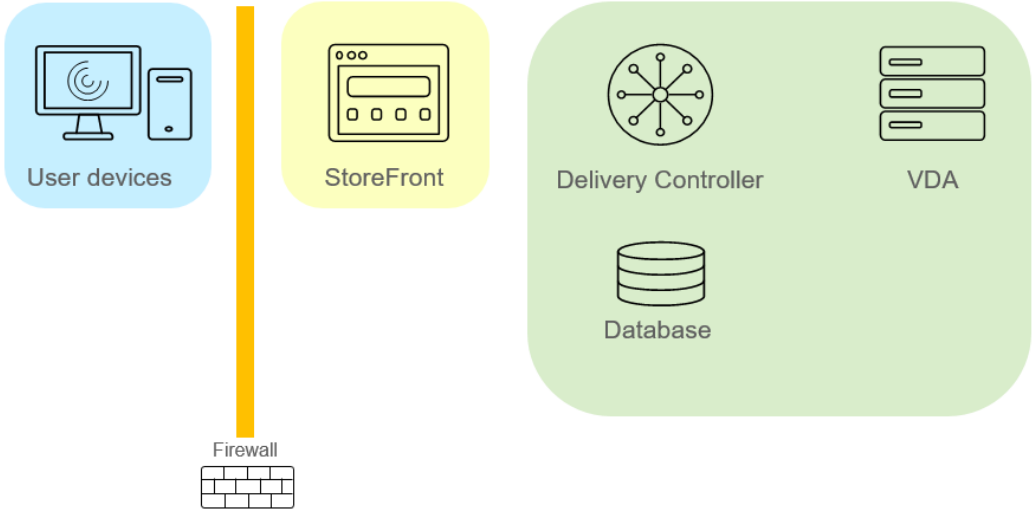
The following features and components are outside the scope of these FIPS 140-2 sample deployments:

- UDP-based features: UDP audio, and Enlightened Data Transport (EDT) including DTLS. (For information on disabling EDT see https://support.citrix.com/article/CTX220732.)
- Linux VDA
- Federated Authentication Service (FAS)
- VMware SSL thumbprint
- Universal Print Server (UPS)

For more information and support regarding these deployment scenarios, including the operating system requirements, contact Technical Support or your Citrix partner.

Citrix Virtual Apps (internal network)

This deployment provides end-to-end TLS encryption between the user device and the applications hosted on Citrix Virtual Apps. The deployment includes Citrix Workspace app, StoreFront, the Delivery Controller and the VDA.



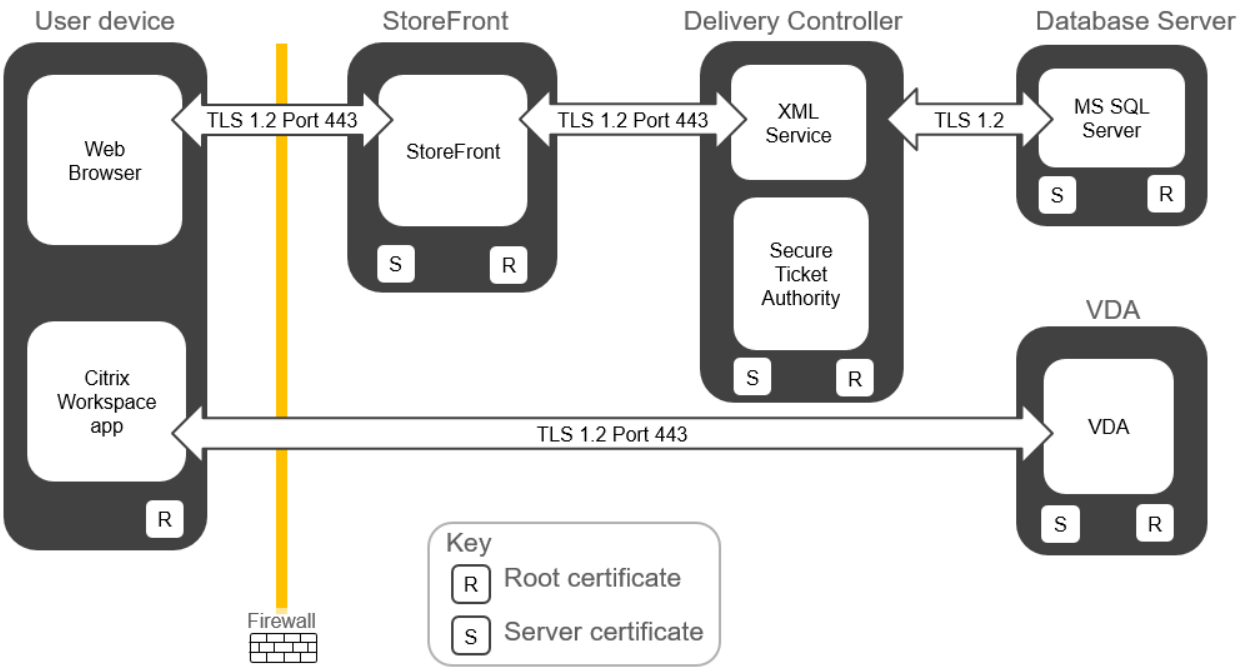
The following table lists the components of the deployment and the operating systems required for the servers and user devices.

	Product/Components	Operating System
Citrix Virtual Apps	Delivery Controller (Secure Ticket Authority is part of the Delivery Controller) Citrix Virtual Apps VDA	Windows Server 2019 Windows Server 2019
StoreFront	StoreFront 1912	Windows Server 2019
User Devices	Citrix Workspace app for Windows 1911 TLS-enabled web browser	Windows 10 x64 version 17763.805

How the components interact

Traffic between the web browser on the user device and StoreFront is secured using HTTPS. Traffic between the VDA machines and the delivery controllers, between some of the services on the delivery controllers, and between consoles and the delivery controller is encrypted using WCF message level encryption based on Kerberos. All other traffic is secured using TLS.

The diagram below shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.

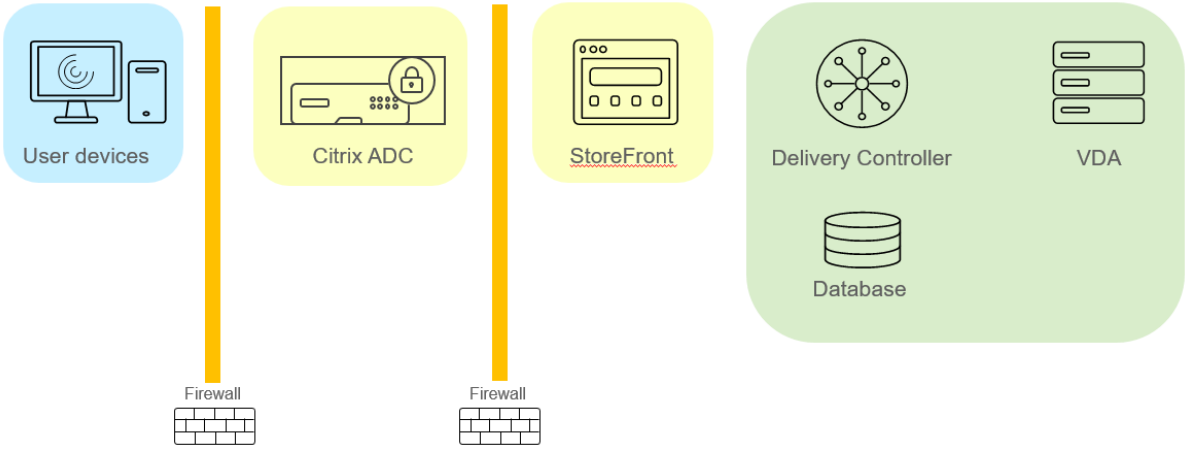


The MS SQL database must be hosted on a dedicated server, and the connection between the database and Delivery Controller must be secured. For details regarding securing this

link, see http://support.citrix.com/article/CTX137556.

Citrix Virtual Apps using Citrix ADC MPX FIPS hardware appliance (external access)

The deployment includes Citrix Workspace app, Citrix ADC MPX FIPS hardware appliance, StoreFront, the Delivery Controller, and the VDA. The Citrix ADC MPX FIPS hardware appliance terminates the TLS/HTTPS connections from the user device (browser and Citrix Workspace app). Traffic from the Citrix ADC MPX FIPS hardware appliance through StoreFront, the Delivery Controller, and the VDA is secured using TLS.



The following table lists the components of the deployment and the operating systems required for the servers and client devices.

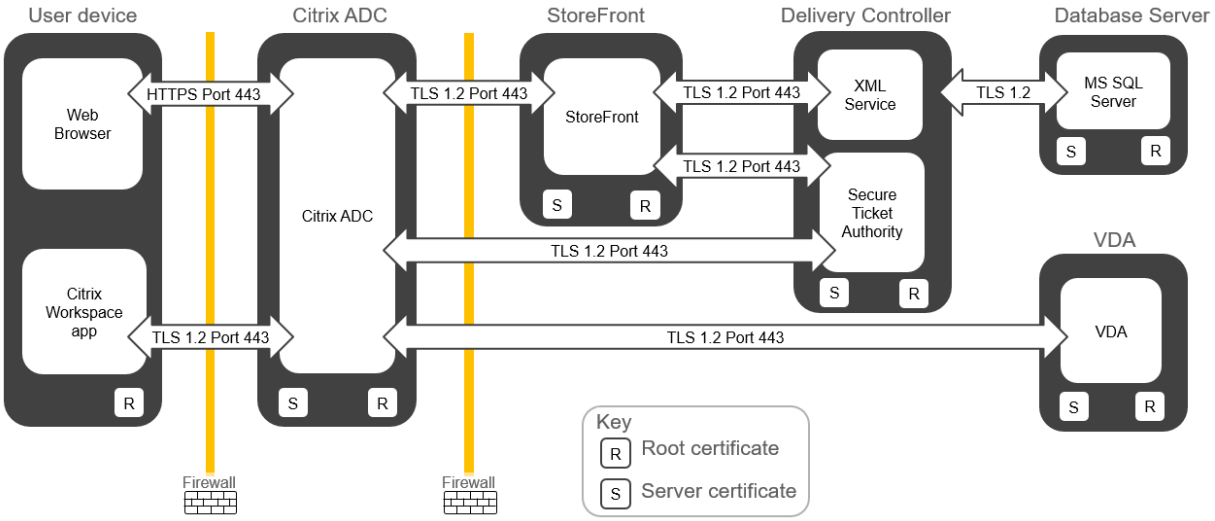
	Product/Components	Operating System
Citrix Virtual Apps	Delivery Controller (Secure Ticket Authority is part of the Desktop Controller) Citrix Virtual Apps VDA	Windows Server 2019 Windows Server 2019
Citrix ADC	Citrix ADC 12.1 MPX 14060 FIPS appliance	
StoreFront	StoreFront 1912	Windows Server 2019
User Devices	Citrix Workspace app for Windows 1911 TLS-enabled web browser	Windows 10 x64 version 17763.805

How the components interact

Traffic between the web browser on the user device and Citrix ADC is secured using HTTPS. All other traffic is secured using TLS.

This diagram shows a detailed view of the deployment including the components and

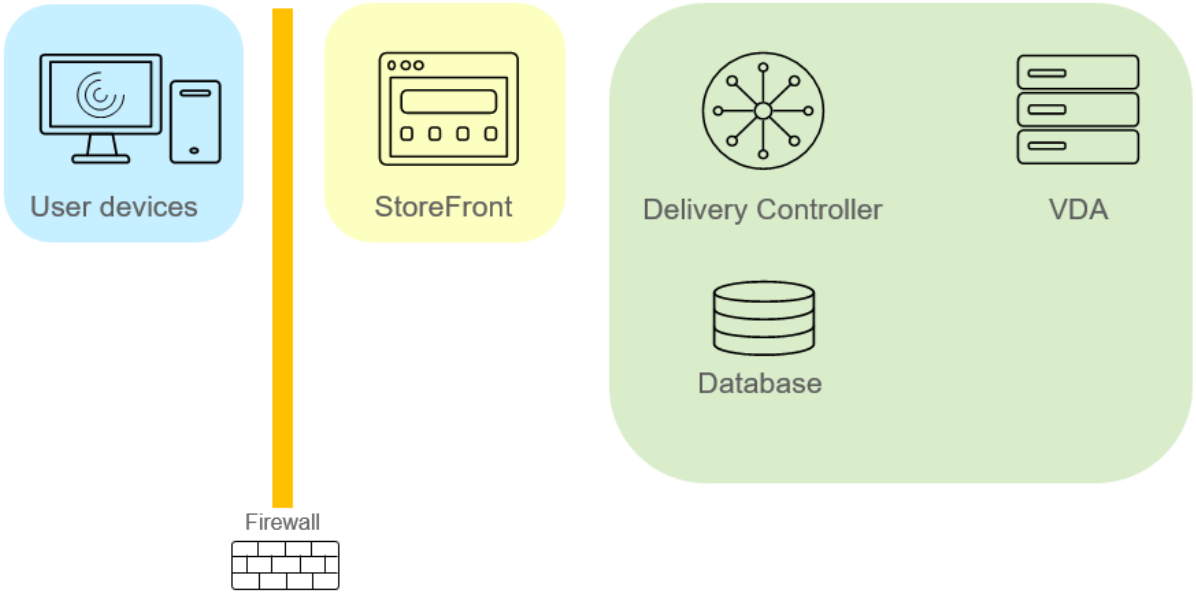
certificates on each server, plus the communication and port settings.



The MS SQL database must be hosted on a dedicated server, and the connection between the database and Delivery Controller must be secured. For details regarding securing this link, see http://support.citrix.com/article/CTX137556.

Citrix Virtual Desktops (internal network)

This deployment provides end-to-end TLS encryption between the user device and the resources hosted on Citrix Virtual Desktops. The deployment includes Citrix Workspace app, StoreFront, the Delivery Controller, and the VDA.



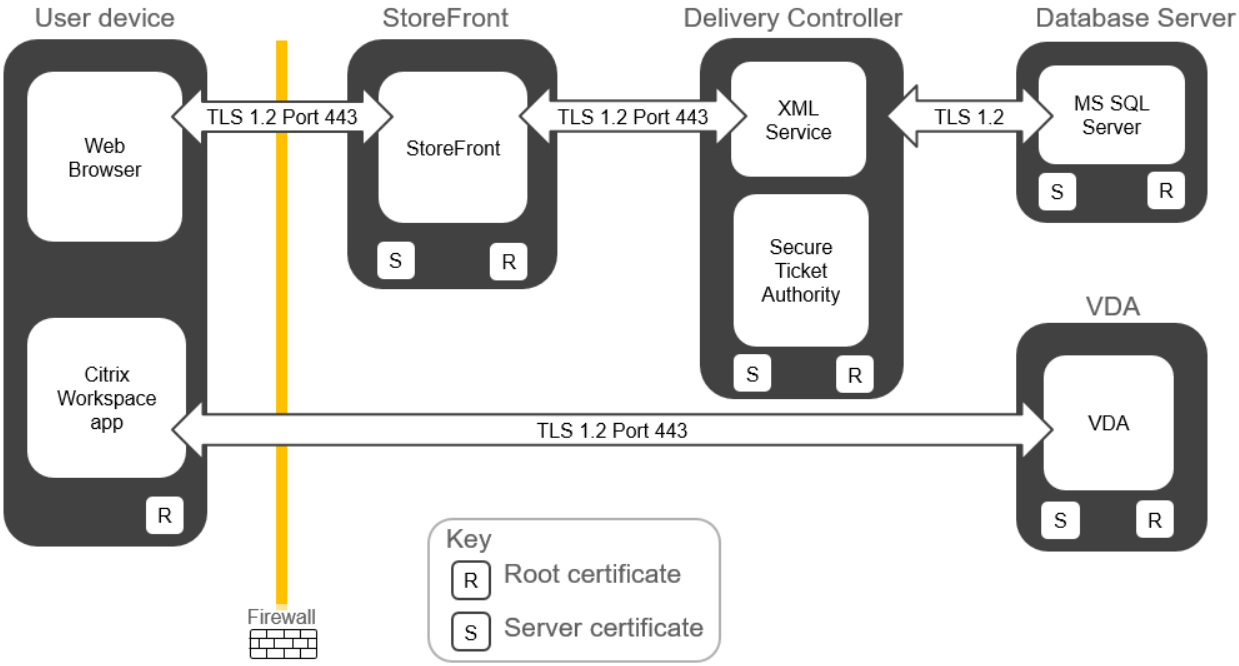
The following table lists the components of the deployment and the operating systems required for the servers and client devices.

	Product/Components	Operating System
Citrix Virtual Desktops	Delivery Controller (Secure Ticket Authority is part of the Desktop Controller) Citrix Virtual Desktops VDA	Windows Server 2019 Windows 10 x64 version 17763.805
StoreFront	StoreFront 3.12	Windows Server 2019
User Devices	Citrix Workspace app for Windows 1911 TLS-enabled web browser	Windows 10 x64 version 17763.805

How the components interact

Traffic between the web browser on the user device and StoreFront is secured using HTTPS. Traffic between the VDA machines and the delivery controllers, between some of the services on the delivery controllers, and between consoles and the delivery controller is encrypted using WCF message level encryption based on Kerberos. All other traffic is secured using TLS.

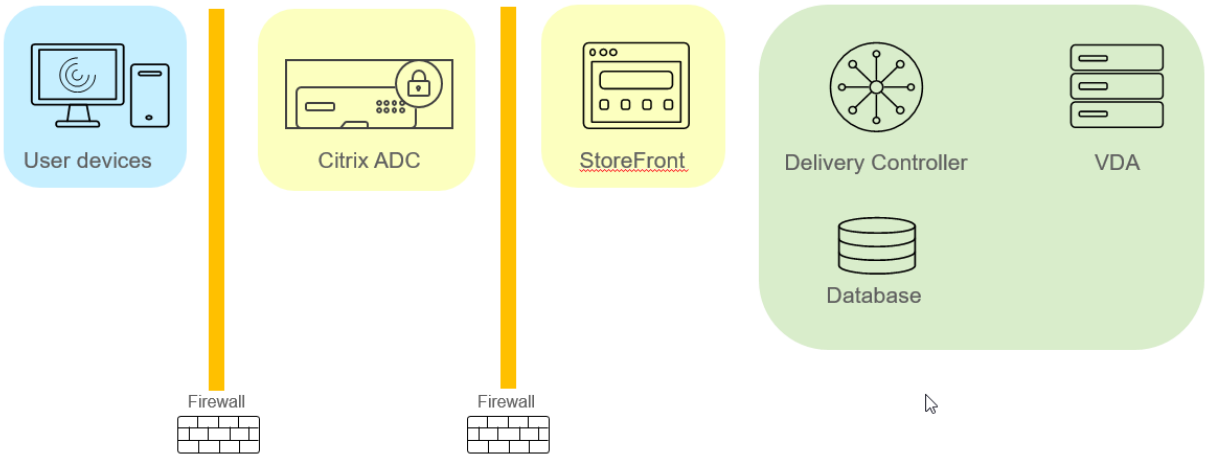
The following diagram shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.



The MS SQL database must be hosted on a dedicated server and the connection between the database and Delivery Controller must be secured. For details regarding securing this link, see http://support.citrix.com/article/CTX137556.

Citrix Virtual Desktops using Citrix ADC MPX FIPS (external access)

The deployment includes Citrix Workspace app, Citrix ADC MPX FIPS hardware appliance, StoreFront, the Delivery Controller, and the VDA. Citrix ADC terminates the TLS/HTTPS connections from the user device (browser and Citrix Workspace app). Traffic from Citrix ADC through StoreFront, the Delivery Controller, and the VDA is secured using TLS.



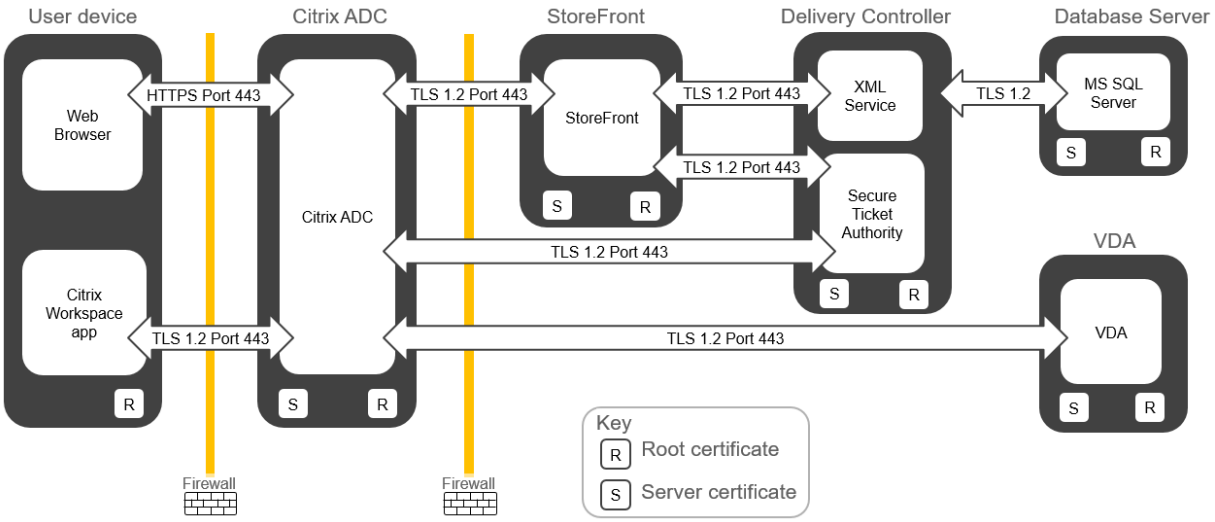
The following table lists the components of the deployment and the operating systems required for the servers and user devices.

	Product/Components	Operating System
Citrix Virtual Desktops	Delivery Controller (Secure Ticket Authority is part of the Desktop Controller) Citrix Virtual Desktops VDA	Windows Server 2019 Windows 10 x64 version 17763.805
Citrix ADC	Citrix ADC 12.1 MPX 14060 FIPS appliance	
StoreFront	StoreFront 1912	Windows Server 2019
User Devices	Citrix Workspace app for Windows 1911 TLS-enabled web browser	Windows 10 x64 version 17763.805

How the components interact

Traffic between the web browser on the user device and Citrix ADC is secured using HTTPS. All other traffic is secured using TLS.

This diagram shows a detailed view of the deployment including where the components and certificates on each server, plus the communication and port settings.



The MS SQL database must be hosted on a dedicated server, and the connection between the database and Delivery Controller must be secured. For details regarding securing this link, see http://support.citrix.com/article/CTX137556.

Finding more information

For more information regarding the products, requirements, and specific procedures, please see:

- Product-specific content at the Citrix product documentation site (https://docs.citrix.com/).
- For more information about secure Citrix ADC deployments, see http://support.citrix.com/article/CTX129514.
- For more information regarding the Citrix Virtual Apps and Desktops 7 1912 LTSR FIPS support and features, see http://blogs.citrix.com/2014/10/16/xenapp-and-xendesktop-7-6-security-fips-140-2-and-ssl-to-vda/.
- For additional guidance regarding certificate management, see http://blogs.citrix.com/2014/12/11/how-to-secure-ica-connections-in-xenapp-and-xendesktop-7-6- using-ssl/ .

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States