Common Criteria Evaluated Configuration Guide for Citrix XenApp 7.15 LTSR Platinum Edition and XenDesktop 7.15 LTSR Platinum Edition

CITRIX

Common Criteria Evaluated Configuration Guide for Citrix XenApp 7.15 LTSR Platinum Edition and XenDesktop 7.15 LTSR Platinum Edition

Document code: 1/26/2018 07:11:28

Table of Contents

Chapter 1 Introduction

This guide, the Common Criteria Evaluated Configuration Guide (CCECG) for Citrix XenApp 7.15 LTSR Platinum Edition and XenDesktop 7.15 LTSR Platinum Edition, describes the requirements and procedures for installing and configuring Citrix XenApp and XenDesktop in accordance with the Common Criteria evaluated deployment.

If your security requirements and policies require you to deploy XenApp or XenDesktop to match the Common Criteria Target of Evaluation configuration exactly, you should follow the procedures in this guide.

Common Criteria Target of Evaluation

This guide details how to configure XenApp or XenDesktop to match the Common Criteria Target of Evaluation (TOE) configuration. The TOE is a XenApp 7.15 LTSR (Platinum Edition license) or XenDesktop 7.15 LTSR (Platinum Edition license) deployment comprising:

- Delivery Controller 7.15.0.15097
- Studio 7.15.0.93
- StoreFront (including StoreFront management console) 3.12.0.17
- Virtual Delivery Agent 7.15.0.15097
- Receiver for Windows 4.9.0.2539 with Online plug-in 14.9.0.2539

Other components for XenApp and XenDesktop included in XenApp and 7.15 LTSR Platinum Edition and XenDesktop 7.15 LTSR Platinum Edition are considered outside of the scope of the TOE.

Further details about the scope of the TOE can be found in Common Criteria Evaluated Deployment Components.

Other Documentation

In addition to this CCECG, refer to the following documents for essential information when deploying XenApp or XenDesktop in the TOE configuration:

- *Common Criteria Security Target for Citrix XenDesktop 7.15 LTSR Platinum Edition and XenApp 7.15 LTSR Platinum Edition* describes the TOE and details assumptions such as the physical environment used and associated roles.
- Administrator and User Operational Guidance for XenApp and XenDesktop describe operational aspects of the XenApp and XenDesktop Common Criteria evaluated deployment. These documents are included as appendices to this CCECG.

Citrix product documentation is provided at https://docs.citrix.com. Common Criteria-specific documentation is provided at https://www.citrix.com/security in the Common Criteria section.

While administrators are expected to use the online product documentation as a whole, the following sections of the online documentation are specifically relevant to the evaluated configuration. To access these sections, go to https://docs.citrix.com and then use the following guidance:

For documentation about	From the left menu on docs.citrix.com, navigate to
Licensing	XenApp and XenDesktop > Licensing > Licensing 11.14
Citrix Receiver for Windows	Citrix Receiver > Receiver for Windows > Citrix Receiver for Windows 4.9 LTSR
StoreFront	XenApp and XenDesktop > StoreFront > StoreFront 3.12
XenApp and XenDesktop Version 7.15 LTSR	XenApp and XenDesktop > XenApp and XenDesktop 7.15 Long Term Service Release

The Citrix-specific Group Policy Security Templates are provided in an annex to this CCECG (Document: CitrixGPOs_201708.pdf).

Secure Delivery of Common Criteria Documentation

You can obtain an electronic copy of the XenApp and XenDesktop CCECG and other Common Criteria documentation from the Citrix website. These documents are available as an HTTPS secure download in order to provide authenticity and data integrity.

To obtain the XenApp and XenDesktop Common Criteria documentation:

1. Navigate to https://www.citrix.com/security using a web browser.
2. Click **Common Criteria**.
3. Click **Common Criteria Documents for XenApp 7.15 LTSR and XenDesktop 7.15 LTSR** to download.

It is your responsibility to verify that the download hyperlink connects to www.citrix.com using HTTPS and that the corresponding website certificate is valid.

Reporting Suspected Vulnerabilities

If you discover suspected vulnerabilities in this the Common Criteria evaluated configuration, Citrix recommends you report these vulnerabilities through this email address: secure@citrix.com.

You can also report suspected vulnerabilities through Citrix support personnel, systems engineers, or resellers.

About XenApp and XenDesktop in This Guide

Features available in XenApp 7.15 LTSR versus XenDesktop 7.15 LTSR are determined by the type of Citrix licenses used. In the evaluated deployment, the features available in XenApp are a subset of the features available in XenDesktop. Specifically, XenDesktop delivers virtual desktops and applications, whereas XenApp delivers only applications.

In this guide, procedures that apply only to XenDesktop are noted as such. In general discussions of the evaluated deployment's features and functionality, assume all references to virtual desktops in this guide refer only to XenDesktop.

Chapter 2 Planning for Citrix XenApp and XenDesktop

This chapter describes the Common Criteria evaluated deployment and explains what you must do before installing and configuring XenApp and XenDesktop. It also outlines the system requirements for the various components.

Common Criteria Evaluated Deployment Components

The Target of Evaluation (TOE) components of XenApp and XenDesktop in the Common Criteria evaluated deployment are:

Delivery Controller. Installed on servers in the data center, the Delivery Controller authenticates users and administrator, manages the assembly of desktop users' virtual desktop environments, and brokers connections between users and their virtual desktops and applications.

Studio. This provides an administration interface to the Delivery Controller, making use of Windows authentication for administrators. It provides administrators with a number of functions to manage the configuration of virtual desktops and applications, manage desktop users' access permissions for virtual desktops and applications, and manage the Endpoint data access control policy. Studio is installed on the same server as the Delivery Controller in the evaluated deployment.

For the evaluated deployment, XenApp and XenDesktop are configured to have no communication channel or interface to the VM Host. This mean Studio cannot create or manage the virtual machines that provide users with virtual desktops and applications. These virtual machines must be explicitly created by an administrator and managed through the VM Host.

Virtual Delivery Agent (VDA). VDAs are installed on the machines inside the data center that host virtual desktops and applications that are available to users. VDAs enable direct ICA connections between a user device and these virtual desktops and applications. There are two types of VDAs: the VDA for Windows Desktop OS is installed on desktop machines and gives users access to virtual desktops; the VDA for Windows Server OS in installed on servers running Microsoft Remotes Desktop Services (RDS) and gives sets access to hosted applications.

Citrix Receiver. Installed on user devices, Citrix Receiver enables direct ICA connections from user devices to published applications running on the server or to virtual desktops. The user device on which Citrix Receiver is installed can be a physical desktop or a virtual desktop. Citrix Receiver installed on a physical desktop are used to connect to published applications or virtual desktops. Citrix Receiver installed on a virtual desktop are used to connect to applications on the second hop of a double-hop connection.

Desktop Lock. Installed on physical desktops, Desktop Lock works with Citrix Receiver to allow users to connect to a virtual desktop while preventing them from accessing the local desktop.

StoreFront. Installed on a server in the data center, StoreFront gives users access to the virtual desktops and applications that they are authorized to use. Users log on to StoreFront through Citrix

Receiver, Desktop Lock, or using Receiver for Web through a web browser. StoreFront retrieves an ICA file containing the information required for user to connect to the VDA for access to an authorized virtual desktop or application. StoreFront also keeps track of user data to ensure they have a consistent experience across multiple user devices.

StoreFront management console. This provides an administration interface to StoreFront, making use of Windows authentication for administrators. It provides administrators with functions to manage the configuration of StoreFront, including setting the user authentication method. This is installed on the StoreFront server.

Databases. The Site database stores the Configdata managed by the administrators with the Studio, including the Endpoint data access control policy, configuration of virtual desktops and applications, desktop users' access permissions for virtual desktops, lists of permitted published applications, and access permissions for administrators, as well as data used by the Delivery Controller to manage virtual desktops, applications, users, and sessions. The Configuration Logging database stores information about Site configuration changes and administrative activities. The Monitoring database stores data used by Director, such as session and connection information. (The use of Director is not included in the evaluated configuration.)

Other Prerequisite Components

In addition to the products included in the TOE, the following components are required to enable XenApp and XenDesktop for evaluation:

VM Host. This is a hypervisor that provides managed server virtualization platform. The VM Host is used to create and manage the virtual machines in the TOE that provide users with virtual desktops and applications.

Microsoft SQL Server. Installed on a Windows server, this provides a comprehensive, integrated data management and analysis tool. It is used to hold the Databases.

Citrix License Server. Installed on a Windows server, this maintains the licenses for Citrix products through an administration interface to license services.

Domain Controller. Installed on a Windows server, this maintains a database of security principal objects in a domain, using the Active Directory services and Domain Name System.

Smart card enrollment station, smart card readers and associated software. This acts as the smart card enrollment station allowing the enrollment agent to create a certificate on behalf of a smart card user and is only required for those environments using smart cards for authentication purposes. (In the evaluation, NIST PIV (Personal Identity Verification) cards were used for smart card authentication.) Additional software such as Cryptographic Service Provider (CSP) software and smart card reader drivers may need to be installed on user devices to support the use of smart cards.

XenApp and XenDesktop Components Explicitly Excluded from the TOE

The Citrix XenServer hypervisor (which is a separately installed component) was used in the environment for testing, but is not part of the TOE and is therefore not part included in this evaluation. (Various other hypervisors are supported; see VM Host for more information.)

The following Citrix components, which are included in XenApp Platinum Edition or XenDesktop Platinum Edition, are out of scope of the TOE:

- **Citrix NetScaler Gateway**. Offers secure remote access, not used in the evaluated configuration. This is a separately installed component; do not install it.
- **Citrix Provisioning Services**. Optimizes provisioning of virtual desktops, not used in the evaluated configuration. This is a separately installed component; do not install it.
- **Citrix Profile Management**. High performance user personalization method, not used in the evaluated configuration. The Citrix User Profile Manager and User Profile Manager WMI Plugin are additional components you can include when installing a VDA. Omit these additional components during the command line VDA installation with the /exclude “Citrix User Profile Manager” “Citrix User Profile Manager WMI Plugin” option.
- **Citrix NetScaler SD-WAN (previously Citrix CloudBridge)**. Accelerator for improved performance on wide area networks, not used in the evaluated configuration. This is a separately installed component; do not install it.**Director**. Provides the help desk with a single console to monitor, troubleshoot and fix virtual desktops, not used in the evaluated configuration. Director is a component you can install when installing a Delivery Controller. Exclude Director from a command-line installation by omitting it from the /components option.
- **XenClient**. High-performance, bare-metal hypervisor that divides the physical resources of a user device and enables multiple operating systems to run side-by-side securely in complete isolation, not used in the evaluated configuration. This is a separately installed component; do not install it.
- **XenMobile**. A comprehensive solution to manage mobile devices, applications and data, and allowing users to access all of their mobile, SaaS and Windows applications from a unified corporate app store, not used in the evaluated configuration. This is a separately installed component; do not install it.
- **AppDNA**. Reduces the time, cost and risk for OS migration and virtualization technology adoptions by automating application compatibility and overall application migration, not used in the evaluated configuration. This is a separately installed component; do not install it.
- **Citrix Federated Authentication Service.** Integrates with Active Directory Certificate Services, dynamically issuing certificates for users, allowing them to log on using SAML authentication to the NetScaler Gateway; not used In the evaluated configuation. This is a separately installed component; do not install it.

XenApp and XenDesktop Features Explicitly Excluded from the TOE

In addition to this components listed above, certain features of XenApp and XenDesktop are not included in the scope of the evaluation:

Only one application delivery method is included in the evaluation: XenApp published apps, also known as server-based hosted applications. These are applications hosted from a Windows server to a Windows desktop. All other application deliver methods are excluded from the evaluation.

- Only one desktop delivery method is included in the evaluation: VDI desktops. These are virtual applications each running a Windows desktop operating system, rather than running in a shared, server-based environment. These virtual desktops are delivered to physical Windows desktop machines. All other desktop deliver methods are excluded from the evaluation.
- All desktop Delivery Groups in the evaluation deliver desktops of the *static* type, meaning each user connects to the same desktop each time. Desktops of the *random* type are not included in the evaluation. Furthermore, administrators must pre-assign a user to each desktop, rather than allowing the desktop to be assigned to a user on first use.
- Each user in the evaluated configuration can only use one virtual desktop from one desktop Delivery Group. The capability for users to belong to multiple desktop Delivery Groups is not included in the evaluation; nor is the capability for desktop users to be assigned multiple desktops in a desktop Delivery Group.
- Each user in the evaluated configuration can use only a single application Delivery Group. The capability for users to belong to multiple application Delivery Groups is not included in the evaluation.
- Creation of Application Groups is not Included in the evaluation.
- Creation of virtual machines using Machine Creation Services is not included; only virtual machines of the *existing* type, created explicitly by an administrator, are included in the evaluation.
- Because only virtual machines of the *existing* type are included, power management of virtual machines via the Delivery Controller is not included in the evaluation.
- The Local Host Cache and connection leasing features are not included in the evaluation.
- Only Full Administrators are included in the evaluation; other delegated administrator roles are excluded.
- Streaming applications using App-V is not included in the evaluation.
- Remote PC Access is not included in the evaluation.
- Personal vDisk is not included in the evaluation.
- Managing applications with AppDisks Is not included in the evaluation.
- Multi-zone environments are not included in the evaluation.

- Administrators can enable and disable local peripheral support either as a global control policy or for individual users and groups of users; only the facility for applying a global control policy is included in the evaluation.
- By default, non-brokered sessions are not allowed. Administrators must not enable non-brokered sessions for the evaluated configuration.

Any VM Host used to create and manage the virtual machines on which the VDAs are installed (that is, the machines that host the virtual desktop and applications made available to users) is not included in the scope of the TOE.

TOE Boundaries

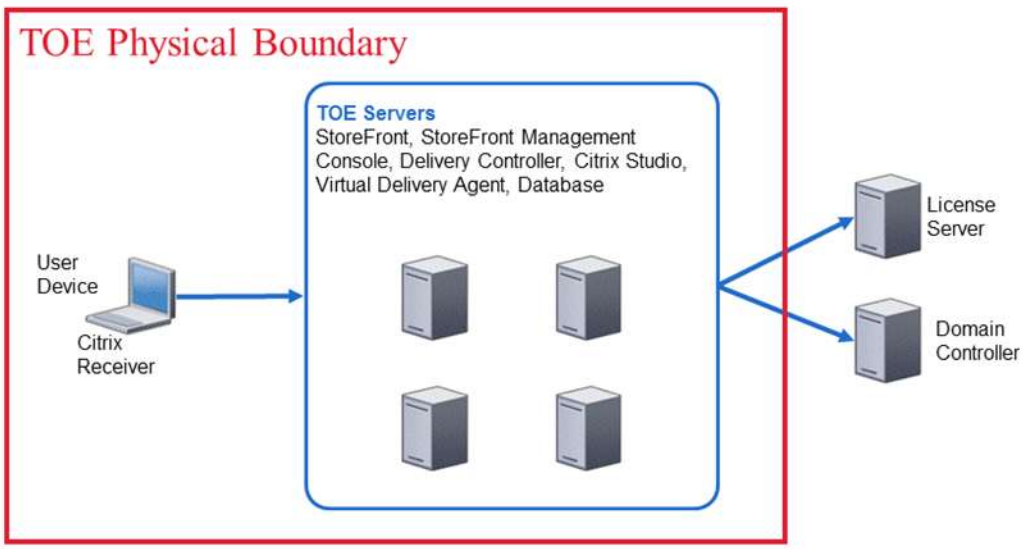

Figure 1 – Physical Boundaries

The physical boundary of the TOE encompasses the TOE server components and the TOE client component, as shown in the figure above.

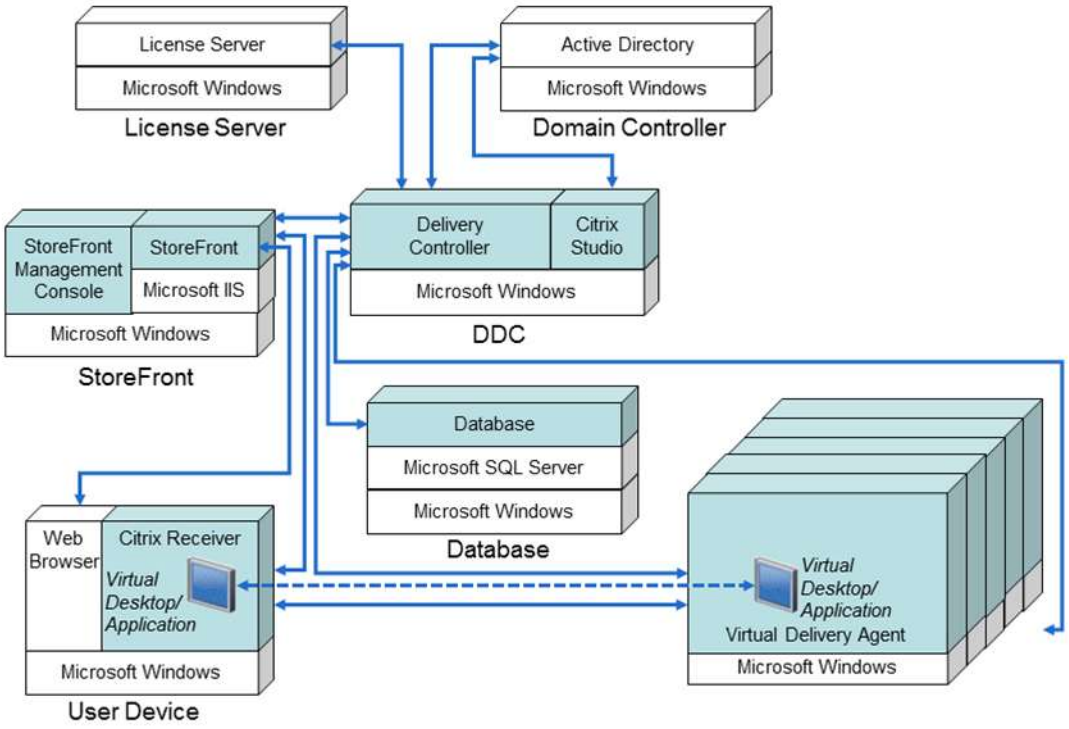

Figure 2 – Logical Boundaries

The figure above depicts the interactions between the components used in the XenApp 7.15 LTSR and XenDesktop 7.15 LTSR Common Criteria evaluated deployment. The shaded items are components of the TOE within the logical boundary.

Domain Configuration

All of the components of the TOE must be installed on machines that belong to the same Active Directory domain, as must all users and administrators.

The domain is a Windows Server 2016 Active Directory domain in native mode. The domain is a single Active Directory with no trust relationship with any other domain.

FIPS 140 Policies and X.509 Certificates

To ensure only FIPS 140 compliant cipher suites and cryptographic modules are used within the deployment, you must apply FIPS 140 compliant group policies. For further details about the deployment of the FIPS 140 compliant group policies, see Active Directory Group Policies.

All of the user devices must have Certificate Authority (CA) root certificates installed that match the

server authentication certificates installed on the VDA machines and on the StoreFront server.

Authentication

StoreFront can be used to configure a variety of authentication methods, including methods that require a username and password for authentication, methods that use smartcards for authentication, and pass-through methods.

These authentication methods are included in the evaluated deployment:

- For user devices connecting to StoreFront using Citrix Receiver or Desktop Lock installed on a user device:
    - User name and password disabled
    - Smart card disabled
    - Domain pass-through enabled
- For user devices connecting to StoreFront using a web browser (Receiver for Web):
    - User name and password enabled
    - Smart card enabled
    - Domain pass-through disabled

Note: Do not configure the Common Criteria evaluated deployment to simultaneously allow users to authenticate using the username and password or smartcard authentication methods; users must have only one of these authentication methods available at a time.

System Requirements

This section describes the minimum system requirements for the various server and client machines in the Common Criteria evaluated deployment of XenApp 7.15 LTSR Platinum Edition and XenDesktop 7.15 LTSR Platinum Edition.

Evaluated Platforms

The operating systems supported by XenApp and XenDesktop components and those actually used in this Common Criteria evaluated deployment are described in the *Common Criteria Security Target for Citrix XenDesktop 7.15 LTSR Platinum Edition and XenApp 7.15 LTSR Platinum Edition*.

You must ensure that the operating systems used in the Common Criteria evaluated deployment are patched with the appropriate updates. After installing the Citrix software, additional updates may be required. So, it is important to rerun Windows Update.

Delivery Controller Server

The minimum system requirements for the Delivery Controller server, on which the Delivery Controller and the Studio are installed, are:

Server Hardware	Server Software
Disk Space Requirements: 175 MB of available space	Microsoft Windows Server 2016, Standard Edition
SVGA video adapter with color monitor	Microsoft .NET Framework 4.6.2
At least 1 NIC	

StoreFront Server

The minimum system requirements for the StoreFront server, on which the StoreFront (including the StoreFront management console) is installed, are:

Server Hardware	Server Software
Disk Space Requirements: 2 GB of available space	Microsoft Windows Server 2016, Standard Edition
SVGA video adapter with color monitor	Microsoft Internet Information Services (IIS) Version 8.0 and ASP .NET 4.5
At least 1 NIC	Microsoft .NET Framework 4.6.2

Virtual Delivery Agents

The minimum system requirements for the VDA for Windows Server OS, which gives users access to published applications, are:

Server Hardware	Server Software
At least 1 NIC	Microsoft Windows Server 2016, Standard Edition

The minimum system requirements for the VDA for Windows Desktop OS, which gives users access to virtual desktops are:

Device Hardware	Device Software
At least 1 NIC	Microsoft Windows 10 Enterprise, 64-bit

User Devices

Microsoft Windows 10 Enterprise, 64-bit is the only supported operating systems for user devices.

Microsoft operating systems chosen for this Common Criteria evaluated deployment have received FIPS accreditation. The minimum system requirements for the client user devices, on which the Citrix Receiver and Desktop Lock are installed, are:

Device Hardware	Device Software
Refer to Microsoft documentation for the hardware requirements for each Operating System	Windows 10 Enterprise, 64-bit
At least 1 NIC	Microsoft Internet Explorer 11
	Smart Card*: Smart card software including PC/SC software, Cryptographic Service Provider (CSP) software, and smart card reader drivers. See your smart card vendor-specific information for details.

* Only required if smart card authentication is used.

Additional information about the system requirements for user devices can be found in the Citrix Receiver for Windows 4.9 product documentation.

Database Server

The minimum system requirements for the Database server, on which the site database is located, are:

Server Hardware	Server Software
At least 1 NIC	Microsoft Windows Server 2016, Standard Edition
	Microsoft SQL Server 2016 SP1

License Server

The minimum system requirements for the License server, on which the Citrix License Server is installed, are:

Server Hardware	Server Software
At least 1 NIC	Microsoft Windows Server 2016, Standard Edition

Domain Controller

The domain controller is installed on a Windows server and configured with Active Directory. See the Microsoft Windows documentation for system requirements for the domain controller.

VM Host

The evaluated deployment requires the use of a hypervisor for creating and managing the virtual machines that provide users with virtual desktops and applications. For the evaluated deployment, XenApp and XenDesktop are configured to have no communication channel or interface to the VM Host. Therefore, XenApp and XenDesktop cannot be used to create or manage these machines.

VM Host software must be securely configured. The VM Host must be a hypervisor certified against a security target that includes the separation of virtual machines (including virtual memory, virtual disk and networking).

A list of hypervisor versions supported for XenApp 7.15 LTSR and XenDesktop 7.15 LTSR is included in the *System requirements* article in the XenApp and XenDesktop 7.15 LTSR product documentation. The following host platforms are supported:

- XenServer
- VMware vSphere
- System Center Virtual Machine Manager, including Hyper-V
- Nutanix Acropolis
- Microsoft Azure Resource Manager
- Microsoft Azure Classic

Windows Firewall Settings

The Windows firewall must be turned on for each machine in the Common Criteria environment. Some machines will also require specific exceptions for services or ports, as described in Specific Windows Firewall Settings.

Third Party Components

The Common Criteria evaluated deployment includes various third party components such as web browsers, virus protection software, and smart cards. These requirements are outlined below.

Note: For detailed configuration details, see the relevant manufacturer's documentation.

Web Browsers

A web browser is required on each user device. The web browser supported by the Common Criteria evaluated deployment is Microsoft Internet Explorer, Version 11.

Virus Protection Software

Good practice dictates that an environment should be suitably protected by anti-virus and anti-spyware software.

The precise choice of anti-virus software may be dependent on your company's security policy.

Smart Cards

The types of smart cards supported for XenApp and XenDesktop are included in the *Smart cards* articles in the XenApp and XenDesktop 7.15 LTSR product documentation. NIST PIV (Personal Identity Verification) cards were used for smart card authentication.

Installation and configuration of the environment to support smart cards is dependent on the vendor used. Further details should be obtained from your vendor or any associated documentation.

Prerequisite Infrastructure Components and Set-up

This section provides a short summary of the tasks required to set up the infrastructure for the XenApp and XenDesktop Common Criteria evaluated deployment. Complete these tasks before securing the environment, installing Citrix components, and performing subsequent tasks described in this guide.

- Install and securely configure the VM Host according to the instructions provided by its manufacturer and the requirements stated in the Common Criteria Security Target for XenDesktop 7.15 LTSR Platinum Edition and XenApp 7.15 LTSR Platinum Edition document.
- Configure Active Directory on a domain controller using the following guidelines:
    - Create an Active Directory domain for the environment. The evaluated configuration has a single forest containing both user and VDA/Controller machine accounts. Multiple-forest configurations (for example, where user accounts exist in a different domain forest than the VDA/Controller machine accounts), are out of scope of the evaluation.
    - Configure Active Directory to include a DNS server, which must be configured to have both forward and reverse look-up zones.
    - Specify a DHCP scope with an address range that excludes the static IP addresses used for the infrastructure components. This enables DHCP to dynamically assign IP addresses to the virtual desktops while protecting the static IP addresses of the infrastructure components.
    - Install Active Directory Certificate Services on the domain controller and configure an

Enterprise Certificate Authority.

- Create and install a TLS server certificate on the StoreFront server.
- Install and configure the Microsoft SQL Server:
    - Install Microsoft SQL Server on the Database server.
    - Create and install a TLS server certificate on the Database server.
    - Enable TLS on the Database server by setting the Force Encryption flag to Yes.
    - Set local and remote connections to use TCP/IP only.

Note: Since XenApp 7.15 LTSR and XenDesktop 7.15 LTSR do not support Mixed Mode Authentication, it is essential to ensure Windows Authentication Mode is the chosen authentication method during the SQL Server installation. An 'sa' account will be created as a result of the setup process but will be disabled by default.

See the Microsoft SQL Server 2016 documentation for installation and configuration instructions.

- Install the Citrix License Server on the License server. See the Citrix Licensing 11.14 product documentation.

Environment Assumptions

This Common Criteria evaluated deployment assumes:

- That all computers within the physical boundaries of the TOE, as well as the License server and domain controller, are installed within a physically secure location that can only be accessed by authorized administrators.
- Keys and other secret data generated and stored outside of the TOE must be managed in accordance with the level of risk.
- Configuration data stored outside the TOE, such as in the SQL database, is accessible only by administrators.
- VM Host software is operating correctly and securely.
- User device operating systems are securely configured with appropriate access permissions.
- User devices must have only trusted third party software installed. This software must be configured securely according to the risks in the operational environment.
- If required, disable endpoint functionality such as screen capture and screen print, so that users cannot bypass controls on data movement between published desktops/applications and their local endpoint.

For further details concerning this and other Common Criteria environment assumptions, refer to the *Common Criteria Security Target for XenDesktop 7.15 LTSR Platinum Edition and XenApp 7.15 LTSR Platinum Edition* document.

Chapter 3 Securing the Environment

This chapter contains information necessary to secure the XenApp and XenDesktop Common Criteria evaluated environment. It is intended to enable you to plan these activities in detail. The activities discussed are not necessarily intended to be performed in the order shown here.

In general, actions for securing the environment should be performed in this order:

1. While configuring the prerequisite components, install certificates, configure firewall settings, and set any other security-related parameters required for those components.
2. Install the Delivery Controller, StoreFront, the VDAs, and Citrix Receiver and Desktop Lock, following all security-related instructions, in the order given in this guide.
3. Apply Active Directory group policies to the Active Directory organizational objects in the evaluated deployment, as described in this chapter, and add machine and user accounts.
4. Create machine catalogs and Delivery Groups for the evaluated deployment, following all security-related instructions.
5. Follow the applicable security recommendations in this chapter while operating the evaluated deployment as described in Appendix A: Operational Guidance for XenDesktop Administrators.

It is important to securely configure the hypervisor in your XenApp and XenDesktop deployment. Obtain guidance from your hypervisor vendor. For example, if you are using XenServer as your hypervisor, you could consider implementing the recommendations in chapter 2 of the document https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/security-recommendations-when-deploying-citrix-xenserver.pdf.

Note: The configuration information and other guidance provided in this section takes precedence over any alternative configuration information and guidance presented in the supporting documents.

Specific Windows Firewall Settings

The specific Windows firewall settings for machines in the Common Criteria environment are summarized below.

Delivery Controller Server

Lock down traffic to allow the following connections only:

- Core Networking Group: Enabled
- XML SSL Port: Enabled (TCP port 443 incoming)
- VDA Registration Port: Enabled (TCP port 8888 incoming)

StoreFront Server

Lock down traffic to allow the following connections only:

- Core Networking Group: Enabled
- World Wide Web Services (HTTPS Traffic-In): Enabled (TCP port 443 incoming)

VDA Machines

Lock down traffic to allow the following connections only:

- Core Networking Group: Enabled
- Citrix ICA SSL Service: Enabled (TCP port 443 incoming)
- Citrix Desktop Service: Enabled (TCP port 8888 incoming)

User devices

Lock down traffic to allow the following connections only:

- Core Networking Group: Enabled

SSL/TLS Configuration

In order to configure the evaluated deployment to use the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) security protocol, you must complete configuration tasks on multiple components of XenApp and XenDesktop, as well as on the Microsoft SQL database. These SSL/TLS configuration tasks can be completed as the components are installed and configured.

For details, see the *Transport Layer Security (TLS)* article in the XenApp and XenDesktop 7.15 LTSR product documentation.

For the Microsoft SQL database, install and configure as described in Prerequisite Infrastructure Components and Set-up.

For the Delivery Controller:

- Obtain, install, and register a server certificate on the Delivery Controller server.
- Configure the SSL port with the TLS certificate.
- Change the default VDA registration port.

For StoreFront:

- Ensure a TLS server certificate is installed on the StoreFront server.
- When installing, accept the default transport type of HTTPS and default port of 443.

For each VDA:

- Install TLS certificates on the VDA machines.
- Configure TLS on the VDA machines.
- Change the default VDA registration port.

For each Delivery Group:

Configure TLS in the Delivery Groups containing VDAs by running a set of PowerShell cmdlets in Studio.Active Directory Group Policies

In the Common Criteria evaluated deployment, it is necessary to set various Active Directory group policies to ensure XenApp 7.15 LTSR and XenDesktop 7.15 LTSR components meet the security requirements.

Microsoft Security Baselines

Use the Microsoft Security Compliance Manager (SCM) 4.0 to configure Microsoft security baselines. To obtain the SCM and find information about using it, go to this Microsoft web page: https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx.

Using the SCM, download and import the following Microsoft security baselines to your domain controller:

- Win10-1607 Domain Security Compliance 1.0
- IE11 Computer Security Compliance 1.0
- Win10-1607 Computer Security Compliance 1.0
- WS2016 Member Server Security Compliance 1.0
- IE11 User Security Compliance 1.0
- Win10-1607 User Security Compliance 1.0

Citrix-specific Group Policy Security Templates

Citrix provides group policies security templates specific to the Common Criteria evaluated environment for XenApp and XenDesktop.

To use these group policies security templates:

1. Locate the XenApp and XenDesktop Common Criteria group policies templates included with the XenApp and XenDesktop Common Criteria documentation. The group policies templates are in a file named Ref_XD2017CC_GPOs – 081617.zip, within the zip file containing the Common Criteria documentation.
2. Extract the contents of Ref_ XD2017CC_GPOs – 081617.zip to a folder on your domain controller.

3. Import the group policies objects to your domain controller using the Group Policies Management Console.
4. Edit the policies with the Group Policy Management tool to customize them for your environment, as described in Customize the Citrix-provided group policy objects.
5. Apply the group policies objects to the Active Directory organizational object in the evaluated deployment.

How to Use Microsoft and Citrix-provided Group Policies

You apply the group policy objects in the Microsoft security baselines and Citrix-provided security templates to Active Directory organizational objects in the domain of your Common Criteria evaluated deployment.

Active Directory OU hierarchy

The group policy objects must be applied to Active Directory organizational unit (OU) structure similar to the one described here.

The Common Criteria evaluated deployment domain, containing these OUs:

- *CC TOE Computers* — An OU for all computers within the physical boundaries of the TOE, containing these OUs:
    - *Desktops* — An OU for all machines accessed by users of the evaluated deployment, containing these OUs:
        - *User Devices* — An OU for physical user devices access by users of the evaluated deployment.
        - *VDA* — An OU for all machines in the evaluated deployment on which the VDAs are installed, containing these OUs:
            - *Desktop VDA* — An OU for all machines in the evaluated deployment on which the VDA for Windows Desktop OS is installed.
            - *Server VDA* — An OU for all machines in the evaluated deployment on which the VDA for Windows Server OS is installed.
    - *Servers* — An OU for the servers within the physical boundaries for the TOE (Delivery Controller server, Citrix License server, and SQL Server), containing this OU:
        - *StoreFront* — An OU for the StoreFront server.
- *CC Users* — An OU for all users of the Common Criteria evaluated deployment (this OU does not include administrators for the evaluated deployment).

Where to apply each group policy object

Apply the group policies to the Active Directory organizational object as described here.

As you apply these group policy objects ensure that, for each Active Directory organizational object, the group policy objects in the Citrix-provided templates have higher link order than the Microsoft security baselines.

To the Common Criteria evaluated deployment domain:

- Win10-1607 Domain Security Compliance 1.0
- Default Domain Policy

To the CC TOE Computers OU:

- XD2017 CC - Computer - SSL Ciphersuite Order

To the *Desktops* OU:

- XD2017 CC – Computer - Shell and Start Menu Restrictions
- XD2017 CC – Computer – App Launch Restrictions
- XD2017 CC - Computer - Control Panel Restrictions
- XD2017 CC – Computer – System settings
- XD2017 CC – Computer – Network Settings
- XD7 CC – Computer – HDX Single Sign-On Enabled
- XD2017 CC – Computer – Security Settings
- XD2017 CC – Computer – Printing Restrictions
- XD7 CC – Computer – Internet Explorer Customizations
- XD2017 CC – Computer – Installation Restrictions
- XD2017 CC – Computer – Internet Explorer Restrictions
- IE11 Computer Security Compliance 1.0
- Win10-1607 Computer Security Compliance 1.0

To the User Devices OU:

- XD2017 CC – Computer – Disable Print Screen

To the *VDA* OU:

- XD2017 CC – Computer – Microsoft Win10 Security Compliance Fixes

To the *Server VDA* OU:

- XD2017 CC – Computer – Endpoint client drive redirection
- XD2017 CC - Computer - Prevent RDS Disconnected Sessions

- XD2017 CC – Computer – Server VDA Security Settings
- XD2017 CC – Computer – Server VDA AppLocker

To the *Servers* OU:

- XD2017 CC – Computer – Allow CC Admin Logon
- WS2016 Member Server Security Compliance 1.0

To the *CC Users* OU:

- XD2017 CC – User – App Launch Restrictions
- XD2017 CC – User – Internet Explorer Restrictions
- XD7 CC – User – Internet Explorer Customizations
- XD2017 CC – User – System settings
- XD2017 CC – User – Shell and Start Menu Restrictions
- XD2017 CC – User – Control Panel Restrictions
- XD2017 CC – User – Installation Restrictions
- Win10-1607 User Security Compliance 1.0
- IE11 User Security Compliance 1.0

Customize the Citrix-provided group policy objects

Some settings in the group policy objects provided in the Citrix templates must be customized with information specific to your deployment, such as infrastructure server names, administrator usernames, and published applications.

Use the Group Policies Management Editor to customize these group policy objects, as described below.

XD7 CC – Computer – HDX Single Sign-On Enabled

Navigate to	Edit this policy setting	Change required
Computer Configuration > Policies > Administrative Templates > Citrix Components/Citrix Receiver/StoreFront	StoreFront Accounts List	Change **Enter the StoreFront account details here** to reflect the FQDN of your StoreFront server.

XD7 CC – Computer – Internet Explorer Customizations

Navigate to	Edit this policy setting	Change required

Computer Configuration > Policies > Windows Components/Internet Explorer/Internet Control Panel/Security Page	Site to Zone Assignment List	Change the value to URL of the StoreFront server.

XD2017 CC – Computer – Allow CC Admin Login

Navigate to	Edit these policy settings	Change required
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies/User Rights Assignment	• Allow log on locally • Shut down the system	Change both settings to the global security group name containing the XenApp or XenDesktop administrators.

XD7 CC – User – Internet Explorer Customizations

Navigate to	Edit this policy setting	Change required
Computer Configuration > Policies > Administrative Templates > Windows Components/Internet Explorer	Disable changing home page settings	Change **Home Page** to the URL of your Receiver for Web site.

XD2017 CC – Computer – Server AppLocker

Navigate to	Edit this setting	Change required
Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > Executable Rules	Enforce rules of this type	• Configure a path rule for each published application in your deployment. For each of these rules, allow access to Everyone and specify no exceptions. • Delete existing path rules for any published application not in your deployment. • Delete rules allowing access to JonasAgentSystray.exe and powershell.exe. • Edit the rule allowing the domain administrator to log onto the server. Change the username of the domain administrator in this rule to the name of the domain administrator of your deployment.

Active Directory Users and Security Groups

When creating Delivery Groups, an Active Directory object picker is used to select the users to add to each group. Users should be added to Delivery Groups using user account names only.

When Security groups are used to assign users to a Delivery Group, any new user added to that security group will, by default, gain access to the desktops and applications in that group. This contravenes the security requirements of the Common Criteria evaluated deployment, which demand that a new user has no desktop or application access by default.

To avoid this, new users must be added to a Delivery Group using their user account to remove the possibility of them having access to a Delivery Group by default. Active Directory administrators must be made aware of this to ensure that they do not create security groups to be used by Citrix administrators for Delivery Group assignment.

Chapter 4 Installing and Configuring the XenApp and XenDesktop Components

This section describes the tasks that must be performed to install and configure XenApp and XenDesktop in the Common Criteria evaluated deployment.

Note: The configuration information and other guidance provided in this chapter takes precedence over any alternative configuration information and guidance presented in the supporting documents.

Before You Begin

Before beginning to install and configure XenApp and XenDesktop components, ensure that all prerequisite infrastructure set-up and environment security tasks described in the previous sections have been completed.

You will download the XenApp and XenDesktop software from https://www.citrix.com. If you have not yet registered for a Citrix account, go to https://www.citrix.com, click **Sign in**, and create an account.

Download and Verify the Installation Media

To download the Citrix Receiver for the XenApp and XenDesktop Common Criteria evaluated deployment:

1. Go to https://www.citrix.com.
2. Click **Downloads**.
3. From the **Select a product** drop-down, choose **Citrix Receiver**.
4. On the Citrix Receiver screen, in the Receiver for Windows category, click **Receiver 4.9 for Windows**. (Do not click Download Receiver 4.7 for Windows at the top of the page.)
5. Verify that the URL in the browser begins with "https".
6. On the Receiver 4.9 for Windows screen, note the checksum.
7. Click **Download Receiver for Windows** and save the file.
8. To ensure the integrity and authenticity of the download, verify the source file against the hash using the Windows PowerShell command `certutil –hashfile sha256`
9. Save the verified download to media, in an empty directory.

To download the Desktop Lock software used with the XenApp and XenDesktop Common Criteria evaluated deployment:

1. Go to https://www.citrix.com.
2. Click **Downloads**.
3. From the **Select a product** drop-down, choose **Citrix Receiver**.

4. On the Citrix Receiver screen, select **Additional Client Software** and then **Other Receiver Plug-ins**.
5. Click Receiver 4.9 Desktop Lock.
6. Verify that the URL in the browser begins with "https".
7. On the Receiver 4.9 Desktop Lock screen, note the checksum.
8. Download and save the file.
9. To ensure the integrity and authenticity of the download, verify the source file against the hash using the Windows PowerShell command `certutil -hashfile sha256`.
10. Save the verified download to media, in an empty directory.

To download the Delivery Controller, Studio, StoreFront (including StoreFront management console), and VDA software for the XenApp and XenDesktop Common Criteria evaluated deployment:

1. Go to https://www.citrix.com.
2. Click **Downloads**.
3. In the Select a product drop-down, select **XenApp & XenDesktop**.
4. Click **XenApp 7.15 LTSR / XenDesktop 7.15 LTSR**. (If there is also an entry for XenApp 7.15x LTSR / XenDesktop 7.15x LTSR, do not click that entry, even though the names are similar.)
5. Click **Sign in to access restricted downloads**. When prompted for credentials, enter your Citrix account name and password, and then click **Sign in.**
6. On the XenApp & XenDesktop page, click **Product Software** and click **XenApp 7.15 LTSR / XenDesktop 7.15 LTSR, All Editions.**
7. On the XenApp 7.15 LTSR / XenDesktop 7.15 LTSR, All Editions screen:
    a. Click **Product ISO**.
    b. Note the checksum.
    c. Click **Download File**.
8. Accept the download agreement. When the download starts, close the Download Agreement window.
9. Save the file.
10. To ensure the integrity and authenticity of the download, verify the source file against the hash using the Windows PowerShell command `certutil -hashfile sha256`.
11. Burn the downloaded .iso file to a DVD for use in any procedures in this guide that require you to load the XenApp and XenDesktop 7.15 LTSR DVD or .iso file.

Citrix will, from time to time, issue product updates which may correct flaws in the underlying software. Administrators should check with Citrix on a regular basis for these updates. Administrators may also opt to subscribe to proactive email alerts about product security vulnerabilities and their associated fixes. These alerts are sent out on a regular basis whenever new fixes are available. Administrators may contact and work with Citrix Support directly if they require additional support in obtaining and deploying any fix. More information about the email alerts system can be found at: http://support.citrix.com. Alerts are available in your profile.

Administrative Permissions

In order to install the XenApp and XenDesktop components described here, you must use a domain user account that has Administrative rights on each of the machines on which these components are installed.

To perform the additional configuration tasks described here, such as configuring SSL/TLS for a Delivery Group, you must use an account that has the XenApp and XenDesktop delegated administration role of Full Administrator. The user who creates the site, as part of the installing and configuring Delivery Controller procedure described here, is automatically made a Full Administrator.

After you perform the required installation task, you should remove the domain administrator account from the list of Full Administrators and add a different domain account, which is not a member of the Enterprise Admins or Domain Admins group, or any other group that has SQL server database or Active Directory scheme administration privileges, to the list of Full Administrators. This prevents the same account from having Full Administrator of the XenApp or XenDesktop site and administrator rights to the domain and the SQL database. The Common Criteria evaluated deployment does not include any account that is both and a XenApp or XenDesktop Full Administrator and has SQL server database or Active Directory scheme administration privileges while the deployment is operating.

Task 1: Installing and Configuring the Delivery Controller and Studio

In the Common Criteria evaluated deployment, installing the Delivery Controller software on the Delivery Controller server involves creating a site, connecting to the Database server to create the Database, and connecting to the Citrix License Server.

Before installing the Deliver Controller and Studio:

- Ensure that Microsoft SQL Server is installed on the Database server and Citrix License Server is installed on the License server. (See Prerequisite Infrastructure Components and Set-up.)
- Install the prerequisites on the Delivery Controller server:
    - Microsoft .NET Framework 4.6.2

To install the Delivery Controller and Studio

1. Log on to the Delivery Controller server with a domain account that has Domain Administrator

rights and is a database administrator on the SQL Server.

2. Insert the XenApp 7.15 LTSR or XenDesktop 7.15 LTSR DVD into the machine's DVD drive. I From the \x64\XenDesktop Setup directory on the media, run the following command. (If the installer's graphical interface launches automatically, cancel it.

```
XenDesktopServerStartup.exe /components "CONTROLLER,DESKTOPSTUDIO"
/disableexperiencemetrics /exclude "Smart Tools Agent" /nosql
/quiet /verboselog /noreboot
```

/components "CONTROLLER,DESKTOP STUDIO"	The components to install. (If this is omitted, all core components are installed on this server.)
/disableexperiencemetrics	Prevents automatic upload of installation experience metrics that are collected locally during installation.
/exclude "Smart Tools Agent"	Prevents installation of the Citrix Smart Tools agent.
/nosql	Prevents installation of SQL Server Express for use as the site database.
/quiet	No user interface appears during the installation.
/verboselog	
/noreboot	Prevents an automatic restart after the installation completes.

3. Launch Studio.
4. On the Studio Welcome screen, click **Deliver applications and desktops to your users**.
5. On the Introduction screen:
    a. For the type of Site you want to create, select **An empty, unconfigured Site**.
    b. In the Site name field, type the name of name of the Common Criteria evaluated deployment site you are creating.
    c. Click **Next**.
6. On the Databases screen:
    a. Accept the default selection to create and set up databases from Studio.
    b. Enter the locations of the database servers.

c. Enter names of the databases or accept the default names.

d. Click **Next**. Connection tests to the databases launch automatically. If the connection test passes, Studio creates the database. If the connection test fails, ensure the address is specified correctly.

7. On the Licensing screen:

a. Type the name and port of the License Server and click **Connect**.

b. When Studio connects to the License Server, select the license to use. To use a license that provides access to all features supported in the evaluated deployment, select **Citrix XenDesktop Platinum** or **Citrix XenApp Platinum**.

c. Click **Next**.

8. On the Connection screen, select **No machine management** and click **Next**.

9. On the Additional Features screen, uncheck all features and click **Next**.

10. On the Summary screen, click **Finish**.

11. Confirm that the version number of the Delivery Controller and Studio is 7.15.0.15097:

a. Go to the Control Panel of the Deliver Controller server and view the list of installed programs.

b. Select the program **Citrix XenDesktop 7.15 LTSR** or **Citrix XenApp 7.15 LTSR** and view the product version number that appears near the bottom of the window.

12. End participation in the Citrix Customer Experience Improvement Program (CEIP.

a. Launch Studio.

b. Select **Configuration** in the left navigation pane.

c. Select the **Support** tab.

d. Follow the guidance to end participation in CEIP.

To configure SSL/TLS on the Delivery Controller

To install a TLS server certificate on the Delivery Controller and to configure a port with the TLS certificate:

1. Log on to the Delivery Controller server with a domain account that has Administrator rights.

2. Obtain a TLS server certificate and install it on the Delivery Controller using the guidance in http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspx. For information on the certreq tool, see http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx.

3. Configure the Delivery Controller with the certificate; see http://msdn.microsoft.com/en-us/library/ms733791%28v=vs.110%29.aspx. When you configure the port:

- For `ipport`, use the IP address of the Delivery Controller server and port 443.
- For `certhash`, use the thumbprint of the certificate.
- For `appid`, use the GUID of the Citrix Broker Service on the Delivery Controller server.

To change the default VDA registration port:

1. Log on to the Delivery Controller server with a domain account that has Administrator rights.
2. Open the command prompt window and type these commands:

   ```
   %SystemDrive%
   Cd %ProgramFiles%\Citrix\Broker\Service
   BrokerSerivce.exe –VDAport 8888
   ```
3. Launch Server Manager from the Start menu.
4. In the Server Manager, go to the Local Server properties window and edit the Window Firewall setting. Click **Advanced Settings**.
5. Click **Inbound Rules**.
6. Create a new inbound rule with the following settings:
   a. In the Rule type screen, click **Port**. Click **Next**.
   b. In the protocol and Ports screen, select **Specific local ports** and type **8888**. Click **Next**.
   a. In the Action screen, accept the default value **Allow the connection** and click **Next**.
   b. In the Profile screen, accept the default values and click **Next**.
   c. In the Name screen, type a name for the rule (example: **Citrix VDA Registration Port**) and click **Finish**.

To disable Local Host Cache and connection leasing, and enable trust requests

When you install the Delivery Controller, connection leasing is disabled by default and Local Host Cache is enabled. Connection leasing and Local Host Cache are not included in the evaluated deployment, so you must ensure both are disabled, using PowerShell. Additionally, enable trust requests sent to the XML Service port.

1. Log on to the Delivery Controller server with a domain account that has Administrator rights.
2. Open the PowerShell command window, running PowerShell as administrator.
3. In the PowerShell console, run `asnp Citrix.*` to load the Citrix product cmdlets.
4. Run `Set-BrokerSite –LocalHostCacheEnabled $false –ConnectionLeasingEnabled $false –TrustRequestsSentToTheXmlServicePort $true`.

Task 2: Installing and Configuring StoreFront

As you install and configure StoreFront, you create a StoreFront deployment, which is known as a store. Users access virtual applications and desktops through the store.

Before installing StoreFront:

- Ensure that a TLS server certificate is installed on the StoreFront server. (See Prerequisite Infrastructure Components and Set-up.)
- Install the prerequisites on the StoreFront server:
    - Microsoft Internet Information Services (IIS) Version 8.0 and ASP .NET 4.5
    - Microsoft .NET Framework 4.6.2
- Prevent the automatic upload of collected installation analytics, run the PowerShell command: New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name SendExperienceMetrics -PropertyType DWORD -Value 0

For more information about StoreFront, see the StoreFront 3.12 product documentation.

To install and configure StoreFront

1. Log on to the StoreFront server with a domain account that has Administrator rights.
2. Insert the XenApp and XenDesktop 7.15 LTSR DVD into the machine's DVD drive. From the \x64\XenDesktop Setup directory on the media, run the following command. (If the installer's graphical interface launches automatically, cancel it.

```
Citrix StoreFront-x64.exe –silent
```

`Silent`	`No user interface appears during the installation.`

3. End automatic participation in the Citrix Customer Experience Improvement Program (CEIP). Run the PowerShell command: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0`
4. Launch the StoreFront management console.
5. On the StoreFront Welcome screen, click **Create a new deployment**.
6. On the Create a New Deployment screen, ensure the default base URL begins with **https:**, and then click **Next**.
7. On the Getting Started screen, click **Next**.
8. On the Store Name screen, type the name of the store you are creating. Accept the default

settings for unauthenticated users and Receiver for Web site settings. Click **Next**.

9. On the Delivery Controllers screen:
    a) Click **Add**.
    b) In the Add Delivery Controller window, click **Add** and type the fully qualified domain name of the Delivery Controller server. Click **OK**.
    c) Accept all other default values in the Add Delivery Controller window. Ensure that the transport type is set to **HTTPS** and the port is set to **443**. Click **OK**.
    d) Click **Next**.
10. On the Remote Access screen, ensure that Enable Remote Access is not selected and click **Next**
11. On the Authentication Methods screen, check **User name and password**, **Domain pass-through**, and **Smart card**. Ensure that no other methods are selected. Click **Next**.

By default, the authentication methods you selected here are enabled. However, the evaluated deployment does not include simultaneously allowing users to authenticate using the username and password or smartcard authentication methods. Before you begin allow users to access you site, you must disable one of these methods. See Setting Authentication Methods.

12. On the Password Vallidation screen, click **Next**.
13. On the XenApp Services URL screen, uncheck **Enable XenApp Services URL** and click **Create**.
14. On the Summary screen, click **Finish**.
15. Select the Stores node in the left pane of the Citrix StoreFront management console and ensure the store in selected in the center pane.
16. In the Actions pane, click **Configure Store Settings.** On the User Subscription page, select **Disable User Subscriptions (Mandatory Store)** and then click **OK**.
17. Confirm that the version number of StoreFront is 3.12.0.17:
    a) Go to the Control Panel of the StoreFront server and view the list of installed programs.
    b) Select the program **Citrix StoreFront** and view the product version number that appears near the bottom of the window.

To modify the web.config file and default.ica file

The files that are created on the StoreFront server when StoreFront is installed (web.config and default.ica) must be modified to configure the evaluated deployment. You modify these files by manually editing them in a text editor.

To modify the web.config file:

1. Log on to the StoreFront server with a domain account that has Administrator rights, if you are not already logged on.
2. Locate the web.config file on the StoreFront server at C:\inetpub\wwwroot*Citrix**CCWeb*\web.config, where *Citrix**CCWeb* is the URL of the Receiver for Web site.
3. Open the web.config file in a text editor, such as Notepad.
4. Locate the `userInterface` element within the file and edit it to have these values:

```
- <userInterface autoLaunchDesktop="false" multiClickTimeout="3"
enableAppsFolderView="true">
  <workspaceControl enabled="false" autoReconnectAtLogon="false"
logoffAction="disconnect" showReconnectButton="false"
showDisconnectButton="false" />
  <receiverConfiguration enabled="false"
downloadURL="ServiceRecord/GetDocument/receiverconfig.cr" />
  <uiViews showDesktopsView="true" showAppsView="true"
defaultView="desktops" />
  <appShortcuts enabled="false" allowSessionReconnect="false" />
  </userInterface>
```

To do this, you change the values of these elements:

- Change autoLaunchDesktop to false
- Change workspaceControl enabled to false
- Change autoReconnectAtLogon to false
- Change logoffAction to disconnect
- Change showReconnectButton to false
- Change showDisconnectButton to false
- Change receiverConfiguration enabled to false

5. Save and close the web.config file.

To modify the default.ica file:

1. Locate the default.ica file on the StoreFront server at C:\inetpub\wwwroot*Citrix**Store*\App_Data\default.ica.
2. Open the default.ica file in a text editor, such as Notepad.
3. In the default.ica file, locate the `[WFClient]` section and add the following key/value pair: `DisableDrives=ABC`.
4. Save and close the default.ica file.

Adding this key/value pair prevents Desktop Lock user from accessing the local system drive (assuming

it is installed as the C drive).

Task 3: Installing the Virtual Delivery Agents

Install the VDAs on virtual machines that users will connect to in order to access virtual desktops and published applications.

Install the VDA for Windows Servers OS on virtual machines running Microsoft Windows Server 2016, Standard Edition. When the VDA for Windows Server OS is installed, the Remote Desktop Session Host is enabled.

Install the VDA for Windows Desktops OS on virtual machines running Microsoft Windows 10 Enterprise, 64-bit.

Before installing the VDAs:

- Install Microsoft .NET Framework 4.6.2
- Enable Remote Desktop Server (RDS) role (Server VDA only)

For details about command-line options, see the *Install using the command line* article in the XenApp and XenDesktop 7.15 LTSR product documentation.

To install the VDA for Windows Server OS

1. Log on to the virtual machine on which you want to install the VDA with a domain account that has Administrator rights.
2. Insert the XenApp and XenDesktop 7.15 LTSR DVD into the machine's DVD drive. From the \x64\XenDesktop Setup directory on the media, run the following command. (If the installer's graphical interface launches automatically, cancel it.)

```
XenDesktopVDASetup.exe /verboselog /optimize /portnumber 8888
/components "VDA" /enable_hdx_ports /noreboot  /exclude "Citrix
Universal Print Client","Personal vDisk","Citrix Personalization for
App-V - VDA" /disableexperiencemetrics /nodesktopexperience
```

/components "VDA"	The component to install. (If this is omitted, the installation includes the Citrix Receiver from the media, which might be an earlier version.)
/disableexperiencemetrics	Prevents automatic upload of installation experiencee metrics that are collected locally during installation.
/exclude "Citrix Universal Print Client","Personal vDisk","Citrix Personalization for App-V - VDA","Citrix	Excludes installation of the Citrix Universal Print Client, Personal vDisk, App-V, User

User Profile Manager","Citrix User Profile Manager WMI Plugin"	Profile Manager, and User Profile Manager WMI Plugin components.
/noreboot	Prevents an automatic restart after the installation completes.
/optimize	Optimizes VDAs running on a VM.
/portnumber 8888	Port number the VDA uses to communicate with the Delivery Controller.
/quiet	No user interface appears during the installation.
/verboselog	

3. Confirm that the version number of the VDA is 7.15.0.15097:
    a. Go to the Control Panel of the virtual machine on which you installed the VDA and view the list of installed programs.
    b. Select the program **Citrix Virtual Delivery Agent 7.15 LTSR** and view the product version number that appears near the bottom of the window.
4. End automatic participation in the Citrix Customer Experience Improvement Program (CEIP) by running the PowerShell command:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -
Name Enabled -PropertyType DWORD -Value 0
```

To install the VDA for Desktop OS

Note: This procedure is for XenDesktop installations only.

1. Log on to the virtual machine on which you want to install the VDA with a domain account that has Administrator rights.
2. Insert the XenApp and XenDesktop 7.15 LTSR DVD into the machine's DVD drive. From the \x64\XenDesktop Setup directory on the media, run the following command. (If the installer's graphical interface launches automatically, cancel it.

```
XenDesktopVDASetup.exe /verboselog /optimize /portnumber 8888
/components "VDA" /enable_hdx_ports /noreboot  /exclude "Citrix
Universal Print Client","Personal vDisk","Citrix Personalization for
App-V - VDA" /disableexperiencemetrics /nodesktopexperience
```

/components "VDA"	The component to install. (If this is

	omitted, the installation includes the Citrix Receiver from the media, which might be an earlier version.)
/disableexperiencemetrics	Prevents automatic upload of installation experiencee metrics that are collected locally during installation.
/exclude "Citrix Universal Print Client","Personal vDisk","Citrix Personalization for App-V - VDA"","Citrix User Profile Manager","Citrix User Profile Manager WMI Plugin"	Excludes installation of the Citrix Universal Print Client, Personal vDisk, App-V, User Profile Manager, and User Profile Manager WMI Plugin components.
/noreboot	Prevents an automatic restart after the installation completes.
/optimize	Optimizes VDAs running on a VM.
/portnumber 8888	Port number the VDA uses to communicate with the Delivery Controller.
/quiet	No user interface appears during the installation.
/verboselog	

3. Confirm that the version number of the VDA is 7.15.0.15097:
    a. Go to the Control Panel of the virtual machine on which you installed the VDA and view the list of installed programs.
    b. Select the program **Citrix Virtual Delivery Agent 7.15 LTSR** and view the product version number that appears near the bottom of the window.

5. End automatic participation in the Citrix Customer Experience Improvement Program (CEIP) by running the PowerShell command:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
Enabled -PropertyType DWORD -Value 0Change the default VDA
registration port
```

1. Go to the Control Panel of the VDA machine and click **Uninstall a Program**.
2. In the list of installed programs, right-click **Citrix Virtual Delivery Agent 7.15 LTSR** and select **Change**.
3. In the XenApp 7.15 LTSR or XenDesktop 7.15 LTSR window that appears, click **Customize**

Virtual Delivery Agent Settings and click **Next**.

4. On the Delivery Controller screen, select **Do it later (Advanced)**. When prompted to confirm your selection, answer **Yes**.
5. On the Protocol and Port screen, change the TCP/IP port the VDA uses to register with the Delivery Controller to **8888**. Ensure that the **Automatically open ports in Windows Firewall if it is detected (even if It is not runing)** check box is selected. Click **Next**.
6. On the Summary screen, click **Reconfigure**.
7. On the Smart Tools screen, select I do not want to participate in Call Home. Click Next.
8. On the Finish Reconfiguration screen, click **Finish**.

To configure SSL/TLS on VDA machines

For each VDA machine in the evaluated deployment, install and configure a TLS server certificate and change the default VDA registration port.

Note: This procedure assumes only one certificate is installed on the VDA machine. If more than one certificate is installed, use thumbprints to identify the certificate.

To install and configure a TLS server certificate:

1. Log on to the VDA machine with a domain account that has Administrator rights.
2. Install a TLS server certificate on the VDA machine.
3. Find Enable-VdaSSL.ps1 PowerShell script on the XenApp and XenDesktop 7.15 LTSR DVD in Support > Tools > SslSupport folder and save it to the VDA machine's desktop.
4. Open the PowerShell command window, running PowerShell as administrator.
5. Run Enable-VdaSSL.ps1 –Enable –CertificateThumbPrint "<*thumbprint*>". The thumbprint identifies which certificate to use.
6. When prompted to confirm this ACL configuration and firewall configuration, type Y each time.

Task 4: Installing and Configuring Citrix Receiver and Desktop Lock

The Common Criteria evaluated deployment includes these configurations of Citrix Receiver and Desktop Lock:

- Citrix Receiver (without Desktop Lock) enables users to connect to virtual desktops and applications while still having access to their physical desktops. If Citrix Receiver is installed on a virtual desktop, it enables users connected to this desktop to then connect to a published application (this is a double-hop scenario).
- Desktop Lock is a component installed in addition to Citrix Receiver that enables users to connect to a virtual desktop. When Desktop Lock is used, the virtual desktop appears in place

of the physical desktop and the user does not have access to the physical desktop.

Install Citrix Receiver with or without Desktop Lock on every user device in your Common Criteria evaluated deployment.

After you install Citrix Receiver, ensure that the user device is configured to prevent users from modifying the Citrix Receiver software. This can be accomplished using operating system permissions and controls such as denying local administrator rights.

To install and configure Citrix Receiver without Desktop Lock

1. Log on to a user device with a domain account that has local administrator rights.
2. Insert the media containing the Citrix Receiver installation file (CitrixReceiver.exe) into the machine's drive.
3. Open the command prompt window, running it as an administrator.
4. In the elevated command prompt window, go to the location of CitrixReceiver.exe and type:

```
CitrixReceiver.exe /includeSSON ENABLE_SSON=Yes SELFSERVICEMODE=FALSE
```

Note: When Citrix Receiver is installed with SELFSERVICEMODE=FALSE, the users have no access to the self-service Receiver interface. Instead, users access an administrator-defined set of virtual desktops and applications though the Start menu.

5. The Citrix Receiver installation wizard appears. Click **Next** through the wizard whenever prompted.
6. Click **Finish** in the installation wizard.
7. Confirm that the version number of Citrix Receiver is 4.9.0.2539 and the version number of the Online plug-in is 14.9.0.2539:
    a. In the notification area of the user device on which you installed Citrix Receiver, right-click the Citrix Receiver icon and select **Advanced Preferences**.
    b. In the About section of the Advanced Preferences window, observe that the version number is 4.2.0.10.
    c. Click **Support Info**. A text file named SupportInfo appears.
    d. In the SupportInfo text file, observe that the text between the "<Version>" tags is "14.9.0.2539".
8. Log off the user device.

To install and configure Desktop Lock

Note: This procedure is for XenDesktop installations only.

To install Desktop Lock, first install Citrix Receiver for use with Desktop Lock:

1. Log on to a user device with a domain account that has local administrator rights.
2. Insert the media containing the Citrix Receiver installation file (CitrixReceiver.exe) into the machine's drive.
3. Open the command prompt window, running it as an administrator.
4. In the elevated command prompt window, go to the location of CitrixReceiver.exe and type:

```
CitrixReceiver.exe /includeSSON ENABLE_SSON=Yes
```

5. The Citrix Receiver installation wizard appears. Click **Next** through the wizard whenever prompted.
6. Click **Finish** in the installation wizard.
7. In the Citrix Receiver Advanced Properties, confirm that the version number of Citrix Receiver is 4.9.0.2539 and the version number of the Online plug-in is 14.9.0.2539:
    a. In the notification area of the user device on which you installed Citrix Receiver, right-click the Citrix Receiver icon and select **Advanced Preferences**.
    b. In the About section of the Advanced Preferences window, observe that the version number is 4.9.0.2539.
    c. Click **Support Info**. A text file named SupportInfo appears.
    d. In the SupportInfo text file, observe that the text between the "<Version>" tags is "14.9.0.2539".

Then add the administrate template required by Desktop Lock to the user device's local computer policy:

1. On the user device, open the Local Group Policy Editor.
2. Right-click on Local Computer Policy > Computer Configuration > Administrative Templates and select **Add/Remove Templates**.
3. In the Add/Remove Templates window, click **Add**.
4. Add the icaclient.adm template for the ICA Client\Configuration subfolder in the Citrix Receiver installation directory.
5. Expand Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User authentication.
6. Right-click the **Local user name password** setting and select **Edit**.
7. Select **Enabled**.
8. Select Enable pass-through authentication and Allow pass-through authentication for all ICA connections.
9. Click **OK**.

10. Right-click the **Smart card authentication** setting and select **Edit**.
11. Select **Enabled**.
12. Select **Allow smart card authentication** and **Use pass-through authentication for PIN**.
13. Click **OK**.
14. Expand Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > StoreFront.
15. Right-click the **StoreFront Accounts List** setting and select **Edit**.
16. Select **Enabled**.
17. Click **Show** then enter into the Value field:

`Store;https://cc-sf-1.cc.local/Citrix/Store/Discovery;on;Store`
where *cc-sf-1.cc.local* is the FQDN of the StoreFront server

18. Close the Local Group Policy Editor and reboot the user device.

To install Desktop Lock:

1. Log on to a user device with a domain account that has local administrator rights.
2. Insert the media containing the Desktop Lock installation file (CitrixReceiverDesktopLock.msi) into the machine's drive.
3. Open the command prompt window, running it as an administrator.
4. In the elevated command prompt window, go to the location of the installer and type:

`msiexec /i CitrixReceiverDesktopLock.msi.`

5. When the Desktop Lock wizard appears, accept the license agreement and click **Install**.
6. Confirm that the version number of Desktop Lock is 14.9.0.2539:
    a. Go to the Control Panel of the user device on which you installed Desktop Lock and view the list of installed programs.
    b. Select the program **Citrix Desktop Lock** and view the product version number that appears near the bottom of the window.
7. Reboot the user device when prompted.

To configure automatic redirection of USB devices

Perform this procedure on any user device on which you want to enable automatic redirection for specific types of USB devices.

USB devices are automatically redirected if USB support is enabled by a Citrix administrator and the USB user preference settings are set to automatically connect USB devices. Depending on your security policies, some or all USB devices might be set by default for automatic redirection. For more

information, see the article *How to Configure Automatic Redirection of USB Devices* at http://support.citrix.com/article/CTX123015/.

Caution! This procedure requires you to edit the registry. Using Registry Editor incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Back up the registry before you edit it.

1. Log on to a user device with a domain account that has local administrator rights.
2. Open Registry Editor (**Run > regedit**).
3. Expand the tree: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB\Devices.
4. Double-click any of these settings and set their **Value data** entry to **1** to enable USB automatic redirection for that type of device:
    - AutoRedirectAudio
    - AutoRedirectPrinters
    - AutoRedirectStorage
    - AutoRedirectVideo

Task 5: Change the XenApp or XenDesktop Site Administrator

When the Delivery Controller was installed, the domain administrator was automatically made a Full Administrator of the XenApp or XenDesktop site being created. Before you continue, you must make a different account in your domain a Full Administrator of the site and remove the domain administrator from the list of XenApp or XenDesktop site administrators.

Any account you make a XenApp or XenDesktop site administrator must be a domain user account that is not a member of the Domain Admins or Enterprise Admins groups, or any other group that has SQL Server database or Active Directory schema administration privileges.

To do this, you will use the domain administrator account to make another domain account in the XenApp or XenDesktop site and then use this other account to delete the domain administrator from the list of site administrators.

Note: Only XenApp or XenDesktop Full Administrators for all scopes are included in the evaluation; other delegated administration scopes and roles are not.

To change the site administrator

1. Log on to the Delivery Controller server with the domain administrator account used to install the Delivery Controller, if you are not already logged on.
2. If Studio it is not already running, start it by clicking **Citrix Studio** on the Start menu.

3. Click **Administrators** in the left pane of Studio.
4. In the Action pane on the right, click **Create Administrator**.
5. Using the wizard that appears, choose a domain account other than a domain administrator and make this account an administrator. Use the wizard to give this administrator rights to all scopes and all roles.
6. Confirm that the site administrator account you created in step 5 now appears in the center pane of Studio as Full Administrator.
7. Log off the Delivery Controller server.
8. Log on to the Delivery Controller server with the domain account made a site administrator in step 5.
9. Click **Administrators** in the left pane of Studio.
10. In the center, select the site administrator associated with the domain administrator account.
11. In the Action pane on the right, click **Delete Administrator**.

Perform the subsequent tasks described in the chapter using the account associated with the XenApp or XenDesktop site administrator created in this procedure.

Task 6: Configuring Citrix Policy Settings

Use Studio to configure Citrix policy settings that define aspects the behavior of ICA connections in the evaluated deployment.

To configure Citrix policies

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio it is not already running, start it by clicking **Citrix Studio** on the Start menu.
3. Click **Policies** in the left pane of Studio.
4. Begin creating policies. This is the procedure for a creating policy:
    a. In the Actions pane on the right, click **Create Policy**. The Create Policies window appears.
    b. On the Settings screen, select the settings you want to include in your policies. Click **OK** after editing or accepting the default values for each. After selecting all the settings you want to include in the policies, click **Next**.
    c. In the Users and Machines screen, select the objects in the Site you want to apply this policy to. For the initial configuration of these policies, select **All objects in Site**. Click **Next**.
    d. In the Summary screen, type a name (and, optionally, a description) for the policy.

e. To enable the policy immediately after creating it, ensure **Enable policy** is checked and. If you don't want to the policy to be enabled by default, uncheck **Enable policy**.

f. Click **Finish**

5. Repeat the steps for creating a policy until you have created each of the following policies, each of which is applied to all objects in the Site:

Priority	Policy name	Settings	Enable or Disable
1	Disable Client Reconnection	• Auto client reconnect: Prohibited • Multi-Stream computer setting: Disabled • Session reliability connections: Prohibited • Disconnected session timer: Enabled • Disconnected session timer interval: 0	Enabled
2	Disable Windows Media Redirection	• Multimedia conferencing: Prohibited • Windows Media redirection: Prohibited	Enabled
3	Disable Audio over UDP	• Audio over UDP: Prohibited	Enabled
4	Disable Flash Redirection	• Flash backwards compatibility: Disabled • Flash default behavior: Disable Flash acceleration	Enabled
5	Enable USB Device Redirection	• Client USB device redirection: Allowed	Disabled
6	Disable Client Drive Redirection	• Allow file transfer between desktop and client: Prohibited • Auto connect client drives: Disabled • Client drive redirection: Prohibited • Client fixed drives: Prohibited • Client floppy drives: Prohibited • Client network drives: Prohibited • Client optical drives: Prohibited • Client removable drives: Prohibited • Download file from desktop: Prohibited	Enabled

Priority	Policy name	Settings	Enable or Disable
		• Upload file to desktop: Prohibited	
7	Disable Clipboard Redirection	• Client clipboard redirection: Prohibited	Enabled
8	Disable Audio Redirection	• Audio over UDP real-time transport: Disabled • Audio Plug N Play: Prohibited • Client audio redirection: Prohibited • Client microphone redirection: Prohibited	Enabled
9	Disable Printer Redirection	• Auto-create client printers: Do not auto-create client printers • Auto-create generic universal printer: Disabled • Automatic installation of in-box printer drivers: Disabled • Client printer redirection: Prohibited • Direct connections to print servers: Disabled • Universal Print Server enabled: Disabled	Enabled
10	Disable Multimedia Redirection	• Multimedia conferencing: Prohibited • Windows Media redirection: Prohibited	Enabled
11	Disable Plug and Play USB Redirection	• Client USB Plug and Play device redirection: Prohibited	Enabled
12	Disable TWAIN Device Redirection	• Client TWAIN device redirection: Prohibited	Enabled

Task 7: Apply Active Directory Group Policy and Add Computer and User Accounts

Before continuing to the tasks that complete your XenApp or XenDesktop site installation, complete these tasks on the Common Criteria domain:

- Apply the required Active Directory group policies to the organizational objects in the Common Criteria domain, as described in Active Directory Group Policies.

- Add domain computer accounts for the VDA machines that will host virtual desktops and applications in the site.
- Add domain user accounts for the users who will access these virtual desktops and applications.

Task 8: Creating Machine Catalogs and Delivery Groups

XenApp and XenDesktop provide users with virtual desktops and applications using machine catalogs and Delivery Groups. Machine catalogs are collections of machines that host the virtual desktops and applications that you provide to the users of the evaluated deployment. Delivery Groups are collections of users given access to a specified set of virtual desktops (one desktop per user in the evaluated configuration) or applications.

To complete the tasks in this section, you must be a XenApp and XenDesktop Full Administrator.

Machine Catalogs

When you create a machine catalog, you specify the provisioning method for the machines in the catalog, specify the type of machines in the catalog, and add machines to the catalog. For the evaluated deployment, you also assign users to an individual desktop machine in the catalog.

In the evaluated deployment:

- Machines in the machine catalogs are manually provisioned on the VM Host before being assigned to machine catalogs.
- Windows Server OS machine catalogs deliver applications only, not server-based desktops.
- Windows Desktop OS machine catalogs can contain only *static* virtual desktops.
- Machines in Windows Desktop OS machine catalogs are pre-assigned to users by the administrator when the machine catalog is created (or edited).

Before you begin creating a machine catalog:

- Ensure that virtual machines with domain computer accounts are available to be added to the machine catalog you are creating.
- Ensure that domain user accounts are available to be assigned to virtual desktops in the machine catalog you are creating.
- Ensure each virtual machine has a VDA installed.
- Ensure that these virtual machines have any applications you want to provide to users installed, including Citrix Receiver if applicable.
- Note that each machine in a machine catalog must have the same operating system, VDA, and applications installed.

To create a Windows Server OS machine catalog

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio is not already running, start it by click **Citrix Studio** on the Start menu.
3. If this is the first catalog being created in this Site, Studio guides you to the correct selection. After selecting it, continue with step 6.
4. If this is not the first catalog being created in this Site, click **Machine Catalogs** in the left pane of Studio.
5. In the Actions pane on the right, click **Create Machine Catalog**.
6. Click **Next** at the Introduction screen if it appears.
7. In the Operating System screen, select **Server OS** and click **Next**.
8. In the Machine Management screen, select **Machines that are powered managed** for the types of machines in the catalog, and **Another service or technology** for how machines are deployed. Click **Next**.
9. In the Machines screen, click **Add computers** and add one or more computers to the machine catalogs. Click **Next**.
10. In the Summary screen, type a name and, optionally, a description for the machine catalog. Click **Finish**.

To create a Windows Desktop OS machine catalog

Note: This procedure is for XenDesktop installations only.

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio is not already running, start it by clicking **Citrix Studio** on the Start menu.
3. If this is the first catalog being created in this Site, Studio guides you to the correct selection. After selecting it, continue with step 6.
4. If this is not the first catalog being created in this Site, click **Machine Catalogs** in the left panel of Studio.
5. In the Actions pane on the right, click **Create Machine Catalog**.
6. Click **Next** at the introduction screen if It appears.
7. In the Operating System screen, select **Desktop OS** and click **Next**.
8. In the Machine Management screen, select **Machines that are powered managed** for the types of machines in the catalog, and **Anotherr service or technology** for how machines are deployed. Click **Next**.
9. In the Desktop Experience screen, select I want users to connect to the same (static) desktop each time they log on. Click Next.

10. In the Machines and Users screen:
    a. Click **Add computers** and add one or more machines.
    b. In the User names column, assign one user to each machine. Click Next. Note: When assigning users to machines, make note of the users you assign. You will need to add these users to the Delivery Group containing the machines to which the users are assigned.
11. In the Summary screen, type a name and optionally, a description for the machine catalog. Click **Finish**.

Delivery Groups

When you create a Delivery Group, you choose a machine catalog to provide applications or desktops for the Delivery Group, specify which desktops or applications are available to the Delivery Group, and add users to the Delivery Group.

In the evaluated deployment:

- Only domain users can be added to Delivery Groups.
- Each user can belong to one desktop Delivery Group and one application Delivery Group.
- Delivery Groups deliver virtual desktops or applications; no Delivery Group delivers virtual desktops and applications.
- After each Delivery Group is created, it must be configured for SSL/TLS.

Before you begin creating Delivery Groups:

- Ensure machines in machine catalogs are available to be added to the Delivery Groups.
- Ensure that domain user accounts are available to be added to the Delivery Groups.
- For desktop Delivery Groups, because you assigned users to machines when you created a Desktop OS machine catalog, ensure you know which users you assigned. As you create a Delivery Group, you will add the users that are assigned to the machines that you add.

To create an application Delivery Group

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio is not already running, start it by clicking **Citrix Studio** on the Start menu.
3. If this is the first Delivery Group being created in this Site, Studio guides you to the correct selection. After selecting It, continue with step 6.
4. If this is not the first Delivery Group being created, click **Delivery Groups** in the left panel of Studio.
5. In the Actions pane on the right, click **Create Delivery Group**.

6. Click **Next** at the Introduction screen, if it appears.
7. In the Machines screen, select a Server OS machine catalog. Click **Next**.
8. In the Users screen, select **Restrict use of this Delivery Group to the following users**. Then click **Add** and add one or more users. Click **Next**.
9. In the Applications screen:
    a. From the **Add** drop-down, select **From start menu**.
    b. In the list of discovered applications, select those you want to add, and then click **OK**.
    c. Click **Next**.
10. In the Desktops screen, click **Next**.
11. In the Summary screen, type a name and optionally, a description for the Delivery Group. Click **Finish**.

To create a desktop Delivery Group

Note: This procedure is for XenDesktop installations only.

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio is not already running, start it by clicking **Citrix Studio** on the Start menu.
3. If this is the first Delivery Group being created in this Site, Studio guides you to the correct selection. After selecting It, continue with step 6.
4. If this is not the first Delivery Group being created, click **Delivery Groups** in the left panel of Studio.
5. In the Actions pane on the right, click **Create Delivery Group**.
6. Click **Next** at the Introduction screen, if it appears.
7. In the Machines screen, select a Desktop OS machine catalog. Click **Next**.
8. In the Delivery Type screen, select **Desktops**. Click **Next**.
9. In the Users screen, select **Restrict use of this Delivery Group to the following users**. Then click **Add** and add one or more users. Click **Next**.
10. In the Desktop Assignment Rules screen, click **Add**.
11. In the Add Desktop Assignment Rule dialog box:
    a. Type a display name and description that will appear in Citrix Receiver.
    b. Select Allow everyone with access to this Delivery Group to have a desktop assigned.
    c. Ensure that the **Enable desktop assignment rule** check box is selected.
    d. Click **OK**.

12. Click **Next**.
13. In the Summary screen, type a name and optionally, a description for the Delivery Group. Click **Finish**.

To configure SSL/TLS on Delivery Groups

Complete this procedure for each Delivery Group you create:

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio is not already running, start it by clicking **Citrix Studio** on the Start menu.
3. From Studio, open the PowerShell console, running PowerShell as an administrator.
4. In the PowerShell console, run `asnp Citrix.*` to load the Citrix product cmdlets.
5. Run these PowerShell commands:

```
Get-BrokerAccessPolicyRule –DesktopGroupName "<delivery-group-name>" |
Set-BrokerAccessPolicyRule –HdxSslEnabled $true
```

where <*delivery-group-name*> is the name of the Delivery Group

```
Set-BrokerSite –DnsResolutionEnabled $true
```

Chapter 5 Testing a User Connection

After you complete the installation and configuration of the deployment, you need to test that your deployment works by confirming that users can log in and connect to virtual desktops and applications. This section describes how to log on and test the system.

Logging on to the System

You can log on to the system a user in one of two ways:

- With username and password
- With a smart card

To log on using username and password pass-through

1. Log on to the user device (without Desktop Lock).
2. From the **Start** menu, choose a virtual desktop or application.
3. Verify that you are able to connect to the desktop or application.

To log on using a smart card pass-through

1. Before you log on to the user device (without Desktop Lock), insert your smart card. A dialog box appears prompting you to enter your smart card PIN.
2. Enter your smart card PIN and click **OK**. The virtual desktop session appears.
3. From the **Start** menu, choose a virtual desktop or application.
4. Verify that you are able to connect to the desktop or application.

To log on using a smart card explicit

1. Log on to the user device (without Desktop Lock).
2. Launch the Internet Explorer web browser; it will navigate to the Receiver for Web site automatically (as it is set as the user's home page).
3. Type in the Smartcard PIN when prompted. If the smart card contains more than one certificate, you must select the correct one:
    a. For NIST PIV cards, in the Select a certificate dialog box, click **More Choices**.
    b. Select a certificate. To verify it Is the correct certificate, select **Click here to view certificiate properties**.
    c. Ensure that the Details tab includes the Field **Enhanced Key Usage** set to **Smart Card Log-on**, and then click **OK**.

d. If the certificate you chose is not the correct one, select another certificate and repeat the verification process.

4. Verify that you are able to connect to the desktop or application.

To log on using a username and password explicit

1. Log on to the user device (without Desktop Lock).
2. Launch the Internet Explorer web browser; it will navigate to the Receiver for Web site automatically (as it is set as the user's home page).
3. Type in the username and password when prompted.
4. Verify that you are able to connect to the desktop or application.

Appendix A: Operational Guidance for XenApp and XenDesktop Administrators

The following operational guidance is provided to assist administrators of XenApp 7.15 LTSR and XenDesktop 7.15 LTSR in its evaluated configuration. This guidance is not designed to be comprehensive but instead focuses on those areas that are most pertinent to the security of the system in this configuration.

Administrators should ensure that they understand the significance of changes they make to the configuration of the system to ensure that they do not inadvertently do anything that may compromise the secure operation of the system in its evaluated configuration.

Where necessary, reference should be made to the XenApp 7.15 LTSR and XenDesktop 7.15 LTSR product documentation (see Other Documentation), as well as the guidance provided here.

Setting Authentication Methods

For the combinations of authentication methods included in the evaluated deployment, see Authentication. Follow the procedures below to test the included authentication methods.

To enable and disable authentication methods for Citrix Receiver and Desktop Lock

For Citrix Receiver and Desktop Lock, enable two authentication methods at any one time:

- Domain pass-through and User name and password, or
- Domain pass-through and Smart card.

These authentication methods can be configured as follows:

1. Launch the StoreFront management console if it is not already open.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console.
3. In the center pane, select the store.
4. In the Action pane, click Manage Authentication Methods.
5. Select the authentication methods you want to use. Unselect all other methods. Click **OK**.

To enable and disable authentication methods for Receiver for Web

For Receiver for Web, enable one authentication method and any one time: User name and password or Smart card. Do not enable Domain pass-through.

1. Launch the StoreFront management console if it is not already open.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console.
3. In the center pane, select the store.

4. In the Action pane, click Manage Receiver for Web Sites.
5. Click Configure.
6. In the Edit Receiver for Web site screen, select Authentication Methods in the left pane.
7. Select the authentication methods you want to use. Unselect all other methods. Click **OK**.
8. Click **Close**.

Changing Client Redirection Policies

The evaluated deployment includes enabling and disabling some Citrix policy settings that control how users can intact with their user devices while connected to virtual desktops and applications. This is done by changing the settings of these Citrix policies (these polices were created and applied in Task 6: Configuring Citrix Policy Settings):

- **Enable USB Device Redirection**. Allows redirection of USB devices to and from the user device. When Citrix policies were initially configured for the site, this policy was disabled, meaning users are prevented from using USB devices.
- **Disable Client Drive Redirection**. Prevent file redirection to and from drives on the user device. When Citrix policies were initially configured for the site, this policy was enabled, meaning file redirection to and from the user device is prevented.
- **Disable Clipboard Redirection**. Prevents the clipboard on the user device being mapped to the clipboard on the server. When Citrix policies were initially configured for the site, this policy was enabled, meaning users are prevented from cutting and pasting between the clipboard on the user device and the clipboard on the virtual desktop.

Policy settings changes go into effect the next time users establish a connection. Existing connections remain unchanged.

USB storage devices can be redirected via either client drive redirection or USB device redirection. To fully disable access to USB storage devices the administrator should ensure that the Enable USB Device Redirection policy is disabled and the Disable Client Drive Redirection policy is enabled.

For more information on working with policies, see the *Policies* articles in the XenApp and XenDesktop 7.15 LTSR product documentation.

To enable and disable support for USB device functionality

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio it is not already running, start it by clicking **Citrix Studio** on the Start menu.
3. Click **Policies** in the left pane of Studio.
4. In the center pane, select Enable USB Device Redirection.
5. In the Action pane on the right:

a. Click **Enable** to allow the use of USB devices from being used while connected to virtual desktops.

b. Click **Disable** to prevent the use of USB devices from being used while connected to virtual desktops.

To enable and disable client drive mapping functionality

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio it is not already running, start it by clicking **Citrix Studio** on the Start menu.
3. Click **Policies** in the left pane of Studio.
4. In the center pane, select Disable Client Drive Redirection.
5. In the Action pane on the right:
    a. Click **Disable** to allow file redirection to and from drives on the user device.
    b. Click **Enable** to prevent file redirection to and from drives on the user device.

To enable and disable clipboard mapping functionality

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio it is not already running, start it by clicking **Citrix Studio** on the Start menu.
3. Click **Policies** in the left pane of Studio.
4. In the center pane, select Disable Clipboard Redirection.
5. In the Action pane on the right:
    a. Click **Disable** to allow the clipboard on the user device to be mapped to the clipboard on the server.
    b. Click **Enable** to prevent the clipboard on the user device from being mapped to the clipboard on the server.

Editing Machine Catalogs and Delivery Groups

This section presents procedures for some machine catalogs and Delivery group actions. For information about the types of machine catalog and Delivery groups included in the evaluated deployment and how to create them, see Task 8: Creating Machine Catalogs and Delivery Groups.

To edit a machine catalog

For additional details, see the *Manage Machine Catalogs* article in the XenApp and XenDesktop 7.15 LTSR product documentation.

After a machine catalog has been created, you can edit it:

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio it is not already running, start it by clicking **Citrix Studio** on the Start menu.
3. Click **Machine Catalogs** in the left pane of Studio.
4. Select a machine catalog in the center pane.
5. In the Actions pane on the right, click the task you want to do (for example, add or remove machines in the catalog, manage Active Directory accounts, update or upgrade the catalog).
6. After you select an action, provide the Information requested.

To edit a Delivery Group

For additional details, see the *Manage Delivery Groups* article in the XenApp and XenDesktop 7.15 LTSR product documentation.

After a Delivery Group has been created, you can edit it:

1. Log on to the Delivery Controller server if you are not already logged on.
2. If Studio it is not already running, start it by click **Citrix Studio** on the Start menu.
3. Click **Delivery Groups** in the left pane of Studio.
4. In the Actions pane on the right, click **Edit Delivery Groups**.
5. A display comprising multiple pages appears. Select the page containing the information you want to change. Provide the information requested. When you are done with a page, click **Apply** to apply any changes you made and keep the window open, or click **OK** to apply changes and close the window.

Appendix B: Operational Guidance for XenApp and XenDesktop Users

Note: The following operational guidance is provided to assist users of XenApp 7.15 LTSR and XenDesktop 7.15 LTSR in its evaluated configuration. Any functionality available to users which is not explicitly covered here is considered outside the scope of this document. Administrators should ensure that adequate support is provided to users to supplement the guidance provided here.

Virtual desktops can be used in the same way as an ordinary desktop and published applications can be used the same way as applications installed on ordinary desktops, subject to the policies set by the Citrix administrator.

At the Windows logon screen enter the domain username and password credentials, or if the system is configured to use smart cards, insert the smart card into the card reader and enter the PIN when requested. For Windows 10 or Windows Server 2016 machines, click the smart card key Icon and then enter the PIN.

Your experience depends how your user device is configured to connect to a virtual desktop or to virtual applications.

If your user device has Desktop Lock installed, the Windows logon screen of your user device logs you directly on to a virtual desktop. The screen of the virtual desktop appears to be the screen of your user device.

If your user device does not have Desktop Lock installed, you can access virtual applications from the Start menu, just as you do for applications installed on your user device. If you have a virtual desktop assigned to you, you can access that from the Start menu as well. Without Desktop Lock, the virtual desktop screen appears in a window which you can move and resize, rather than appears as your desktop screen.

You might also be able to access a virtual desktop, or applications, or both, by launching a web browser on your user device and logging in to a web site set up by your Citrix Administrator.

If you are assigned a virtual desktop, you might be able to access virtual applications from the Start menu or the web site, just as you would on your user device, while using your virtual desktop.

When you access virtual applications from the Start menu, you can save data from those applications to a virtual disk drive just as if you were saving to a drive on your user device. When you access virtual applications from a web browser, you can save data from those applications to a virtual disk drive after responding to a prompt that make you aware that you are saving data to a virtual drive.