Securing Your Virtual Desktop Environment
# Table of Contents

Overview .................................................................................................................................................. 3  
Endpoint Security .................................................................................................................................... 5  
Access Security ........................................................................................................................................ 7  
Authentication Security .......................................................................................................................... 10  
Session Security ...................................................................................................................................... 13  
Virtual Desktop Security .......................................................................................................................... 14  
Infrastructure Security ............................................................................................................................ 16  
Security Levels ........................................................................................................................................ 20
Overview

This white paper provides an overview of the technologies and procedures that are available to help secure a Citrix based virtual desktop environment. Furthermore, recommendations for low and high security environments are provided. While many areas are covered, this document is not intended to be a comprehensive planning and configuration guide, or as a training guide. Furthermore, it is recommended that all changes are fully tested within a dedicated test environment before being implemented into production.

For further technical guidance Citrix Consulting recommends the following web resources:

- How to Set Up FIPS 140 on XenApp 6.0 and 6.5 on Windows 2008 R2
- Securing Server Farms (XenApp only)
- XenApp 6.5 Security Standards and Deployment Scenarios
- Security Planning for XenDesktop
- Operations Guide - Support and Maintenance Citrix Desktop and Datacenter (for organizational security)
- Citrix Security and Compliance Information
- Communication Ports Used By Citrix Technologies

This white paper is split into the following sections:

- **Endpoint Security:** Focuses on endpoint devices used to access a Citrix environment.
- **Access Security:** Focuses on techniques for securing the Web Interface / Storefront network communications.
- **Authentication Security:** Available authentication techniques are described in detail within this section.
- **Session Security:** Focuses on techniques for securing the virtual desktop network communications.
- **Virtual Desktop Security:** Outlines how virtual desktops can be secured.
- **Infrastructure Security:** Techniques for securing the network communications between infrastructure components as well as security related monitoring and networking is described. In addition important items about organizational security are outlined.

The following diagram depicts how the aforementioned topics integrate within a common XenDesktop / XenApp infrastructure:
Endpoint Security

The first line of defense of every IT infrastructure, and certainly one of the most important, is the user. Because users have all the information required to access an organization’s data (in order to do their jobs), it makes them a valuable target for hackers. The techniques of “attacking” users are typically subsumed under the term “Social Engineering”, which refers to the art of manipulating people into performing actions or divulging confidential information. Typical countermeasures are limited to user training and increasing awareness. Further information can be found here: http://en.wikipedia.org/wiki/Social_engineering_(security)

The second line of defense is the actual endpoint device (i.e. Windows workstation or thin client), which is the main focus of this section. Common security measures for endpoints include implementing antivirus / antimalware software (incl. regular pattern updates), regular patching of the operating system as well as applications / agents and strict rules for the personal firewall. In order to help organizations secure their environment, Citrix provides the following:

- Monthly testing of Microsoft Security Patches
- Guidelines for Antivirus software configuration

In addition, the following techniques can be used in order to increase endpoint security and the respective level of trust.

- **Securing the Clients by means of Microsoft Security Baselines.** Microsoft provides the Security Compliance Manager (SCM), which contains a large variety of recommendations (security baselines) for securing Windows systems. Furthermore this tool enables administrators to export the defined security settings and to apply them to managed computers by means of Group Policies, System Center or other enterprise tools. Citrix Receiver is compatible with and functions in environments where the Microsoft Specialized Security - Limited Functionality (SSLF) desktop security templates (SCM severities Critical and Important) are used. These settings track closely with the security level historically represented in the NSA guidelines. Further information about Security Compliance Manager and the Windows 7 Baselines can be found here: http://technet.microsoft.com/en-us/library/ee712767.aspx.

- **Trusted Server Configuration.** Trusted server configuration is designed to identify and enforce trust relations involved in Receiver connections. When this feature is enabled, admins can specify the requirements for trust and determine whether or not they trust a connection to a server. When trusted server configuration is enabled, connections can be established to XenApp servers, virtual desktops or Access Gateways, which reside in a Windows Trusted Sites zone (i.e. Trusted Sites or Local Intranet). Further information can be found here within eDocs – Enforcing Trust Relations.
• **ICA File Signing.** The ICA File Signing feature helps protect users from unauthorized application or desktop launches and can help prevent Man-in-the-Middle attacks. When enabled, Citrix Receiver verifies that a trusted source generated the application or desktop launch request by checking the signature hash inside the ICA file. This feature requires:

  - Server Certificate, which is trusted on the client
  - Windows Receiver 3.x or higher
  - Client Side configuration as outlined in eDocs – [ICA File Signing](#).

• **Endpoint Encryption.** A key benefit of centrally delivering applications or desktops with Citrix technologies is that policies can be used to ensure data remains securely located within the datacenter. However if data is permitted to be located on the client device via client drive mapping, clipboard redirection or other feature, then the security of the data at rest also needs to be considered. Various technologies are available that offer full disk encryption for the endpoint including those from Microsoft (Bitlocker) and third parties (Symantec PGP, Becrypt). Citrix XenClient if used to manage endpoint devices can also be configured to provide full disk encryption.
Access Security

A comprehensive security plan must include the protection of the data at all points in the resource delivery process. This section describes techniques for securing the Web Interface / Storefront network communication.

User Device / Web Interface or Storefront Communication

Communication between Citrix clients and the Web Interface / Storefront server consists of passing several different types of data. As users identify themselves, browse their resources, and select a resource to access, the Web browser/Receiver and Web server pass user credentials, resource sets, and session initialization files. Specifically, this network traffic includes:

- **HTML form data.** Web Interface / Storefront sites use a standard HTML form to transmit user credentials from the Web browser to the Web server when users log on. The Web Interface form passes user names and credentials in clear text.

- **HTML pages and session cookies.** After users enter their credentials on the Logon screen, the credentials are stored on the Web server and protected by a session cookie. The HTML pages sent from the Web server to the browser contain resource sets. These pages list the resources available to the user.

- **ICA files.** When a user selects a resource, the Web server sends an .ica file for that resource to the Citrix client (in some cases using the Web browser as an intermediary). The .ica file contains a ticket that can be used to log on to the server. ICA files do not include a ticket for pass-through or smart card authentication. The ICA File Signing feature allows users to verify that they are launching applications or desktops from a trusted Web server. For more information, please refer to section “Endpoint Security”.

Because the user device to web server communication is typically routed over networks outside the data center boundaries or on completely untrusted connections (such as the Internet), Citrix strongly recommends encrypting this traffic by means of SSL.

Web Interface or Storefront / Citrix Server Communication

Communication between the Web Interface / Storefront and the server running XenApp or XenDesktop involves passing user credentials and resource set information between the Web Interface and the Citrix XML Service in the server farm.

In a typical session, the Web Interface server passes credentials to the Citrix XML Service for user authentication and the Citrix XML Service returns resource set information. The server and farm use a TCP/IP connection and the Citrix XML protocol to pass the information. The Web Interface XML protocol uses clear text to exchange all data, with the exception of passwords, which are transmitted using obfuscation.
For Citrix environments with high security requirements it is recommended to encrypt the web server to XenApp / XenDesktop communication. There are two options to achieve this.

- **Using IPSEC.** The implementation is described within TechNet – [Creating and Using IPSEC Policies](#).

- **Using Citrix mechanisms.** The implementation is described in eDocs – [Use the SSL Relay](#) (XenApp only) and CTX130213 - [How to Configure SSL on XenDesktop 5 Controller to Secure XML Traffic](#) (XenDesktop only).

**Server / Appliance Placement**

In scenarios where users are located on untrusted networks (e.g. the Internet) or use untrusted devices (i.e. BYO) and access the Citrix environment, it is recommended to deploy XenApp/XenDesktop and the Web Interface / Storefront server within the internal network for security reasons. In addition an Access Gateway appliance is deployed in the demilitarized zone (DMZ), as depicted below:

![DMZ Diagram](#)

A DMZ is a subnet that lies between the secure internal network and the Internet (or any external network). When Access Gateway is deployed in the DMZ, it acts as a reverse proxy, which relays connections from the untrusted network to the internal servers.

With Access Gateway, users log on to a realm, logon point, or virtual server to gain access to their resources. To make resources available to users a realm, logon point, or virtual server is configured to forward a user to a Web Interface / Storefront site after successful authentication (incl. credential pass-through).

Access Gateway provides several methods for integrating Web Interface / Storefront sites, including:

- A Web Interface / Storefront site configured as the default home page for a realm, logon point, or virtual server. Once logged on, users are presented with the web site.

- A Web Interface / Storefront site embedded within the Access Interface. When the Access Interface is selected as the default home page, a Web Interface / Storefront site appears
Securing Secure Ticket Authority (STA) communication

The Secure Ticket Authority (STA) is a vital component when accessing a Citrix infrastructure by means of Access Gateway as ICA Proxy. The STA is an XML Web service that exchanges XenApp server / XenDesktop virtual desktop information for randomly generated session tickets in response to connection requests for published resources on XenApp or XenDesktop. These session tickets form the basis of authentication and authorization for access to published resources. Every XenApp or XenDesktop Controller can perform STA tasks. In order to secure Web Interface ➔ STA and Access Gateway ➔ STA network communication, it is required to implement a server certificate on the XenApp / XenDesktop controller, which is leveraged as the STA. For more information about implementing a server certificate, please refer to eDocs – Use the SSL Relay (XenApp only) and CTX130213 - How to Configure SSL on XenDesktop 5 Controller to Secure XML Traffic (XenDesktop only).
Authentication Security

Authentication is the initial step, which takes place when a user logs on to a local client or accesses central resources (such as published applications, content, and virtual desktops). The general Citrix recommendation is to implement a strong authentication mechanism for the initial logon and use transparent mechanisms (i.e. pass-through) for any subsequent authentication.

Citrix supports the following authentication mechanisms:

- **Anonymous.** Anonymous authentication is the simplest authentication method available. Anonymous users can log on without supplying a user name and password, and access resources, which have been specifically published for anonymous users. Anonymous sessions are always launched using one of several anonymous user accounts that are set up during installation. Anonymous authentication is supported by Web Interface and XenApp only.

- **Explicit.** Explicit authentication is the default method of authentication. Users are required to log on by supplying a user name (UPN or Domain\Username) and password. Web Interface / Storefront validates the credentials with one or more XenApp server farms / XenDesktop sites before displaying the available resources. In addition Storefront will validate the credentials with an available domain controller directly, in order to be able to display the subscriptions of the user. At launch time, Web Interface / Storefront inserts a logon ticket into the ICA file that is returned to the client. This allows the Citrix Receiver to authenticate to the XenApp - Worker / XenDesktop – Virtual Desktop.

- **Pass-through.** Users can authenticate using the credentials they provided when they logged on to their physical Windows desktop. Users do not need to reenter their credentials and their resource set appears automatically. Pass-through to Web Interface / Storefront is initiated by IIS using Integrated Windows Authentication. Web browsers that support integrated authentication recognize the authentication challenge from IIS and respond automatically with the user’s Windows identity information. Web Interface / Storefront obtains this identity information from IIS in the form of a list of security identifiers (SIDs) and passes the list to the XML service. The XenApp / XenDesktop Controller then uses the SIDs to calculate the list of applications and/or desktops that the user can access. Pass-through authentication from the client to the XenApp - Worker / XenDesktop – Virtual Desktop can be achieved in two ways: with captured credentials or with Kerberos (more secure). Please note that Citrix Receiver must be installed with administrative permissions and single sign-on explicitly specified, in order to activate pass-through authentication.

**Note:** Pass-through authentication is typically used for integrating published resources into existing fat client architectures (majority of applications reside locally) or in Session-in-Session scenarios.
- **Smart card.** When the Web Interface is configured for smart card authentication, users accessing the login page are prompted to insert their card into the card reader and type in their PIN. Certificate authentication is automatically performed using IIS mechanisms. If authentication succeeds, Web Interface obtains the SIDs for the user and passes them to the XenApp Farm / XenDesktop Site, in order to determine what applications the user can see. Smart card authentication from the client to the XenApp - Worker / XenDesktop – Virtual Desktop is only available when using the Windows or Linux version of Receiver. At application launch time, the system hosting the resulting ICA session will detect the smartcard and prompt the user to re-enter their PIN.

**Note:** Smart card authentication is not supported by Storefront (at the date of this paper).

- **Pass-through with smart card.** Pass-through authentication with smart card allows users to access the Web Interface and their applications without having to enter their PIN, provided they have logged in to Windows using a smart card. Users are automatically authenticated to the Web Interface by IIS by using Integrated Windows Authentication.

**Note:** Because of the security enhancements introduced in Windows Vista, smart card users running Windows Vista or Windows 7 who leverage the default Cryptographic Service Providers (CSP) are required to provide their PINs when they access a published application or desktop, even if pass-through with smart card authentication has been enabled. In order to achieve full pass-through 3rd party CSPs have to be implemented, which offer the "Global PIN Cache" feature.

**Note:** Pass-through, pass-through with smart card, and smart card authentication are not available with Web Interface for Java Application Servers.

- **Two-Factor.** Two-factor authentication is a standard way of improving the security of explicit authentication. In order to successfully authenticate to a two-factor system, a user must provide information from something they know (typically a password and/or PIN) and something they have (typically a number from a personalized token). Web Interface provides built-in support for Secure Computing SafeWord and RSA SecurID two-factor authentication systems. Storefront integrates with Access Gateway in order to support multi-factor authentication. Please refer toCTX131908 – Configuring Pass-Through Authentication with Access Gateway and Storefront for further information. In scenarios where the authentication happens at the Web Interface, two-factor authentication requires agent software being installed on the Web Interface server. This adds a passcode field to the Web Interface login page, into which users type the passcode from their token. Web Interface then passes the username and passcode to the agent software for authentication. If authentication is successful with the agent software, Web Interface will proceed to carry out explicit authentication with the XenApp farm / XenDesktop site. Web Interface is also capable of being extended to support other authenticators.
Note: Two-Factor authentication is a very strong authentication mechanism, which is strongly recommended for remote access scenarios.

Authentication for disconnected user sessions

When an ICA session gets disconnected unexpectedly, Citrix Receiver tries to reconnect to the session automatically. This feature is called Auto Client Reconnect. Auto Client Reconnect incorporates an authentication mechanism based on encrypted user credentials. When a user initially logs on to a server farm, XenApp / XenDesktop VDA encrypts and stores the user credentials in memory, and creates and sends a cookie containing the encryption key to the Receiver. The Receiver submits the key to the XenApp server / XenDesktop VDA for reconnection. The system decrypts the credentials and submits them to Windows logon for authentication.

When cookies expire, users must re-authenticate to reconnect to sessions. Cookies are not used if the “Auto Client reconnect authentication” Citrix policy has been configured to “Require authentication”. Selecting this option displays a dialog box to users requesting credentials when Receiver attempts to reconnect automatically. Enabling this configuration is recommended for high security environments.

In addition XenApp and XenDesktop can be configured to log automatic reconnection events. When logging is enabled, the server’s System log captures information about successful and failed automatic reconnection events. This can be beneficial for environments with above normal security needs.

Web Interface / Storefront user session inactivity

By default, user sessions on Web Interface / Storefront Receiver for Web sites time out after 20 minutes of inactivity, for security reasons. When a session times out, users can continue to use any desktops or applications that are already running, but must log on again to access Web Interface / Receiver for Web site functions such as subscribing to desktops and applications. As an additional security measure for high security environments, this time out may be reduced to ensure malicious users cannot start applications on endpoints left unattended. Additional information can be found in eDocs – Configuring Session Durations.
Session Security

The communication between users’ devices and a XenApp Worker / XenDesktop virtual desktop consists of passing several different types of session data, including initialization requests and session data.

- **Initialization requests.** The first step in establishing a session, called initialization, requires the Citrix client to request a session and produce a list of session configuration parameters. These parameters control various aspects of the session, such as which user to log on, the size of the window to draw, and the program to execute in the session.

- **Session data.** After session initialization, data is passed between the Citrix client and server / virtual desktop through a number of virtual channels; for example, mouse input (from client to server) and graphical updates (from server to client).

XenDesktop as well as XenApp enables administrators to obfuscate all communications to and from published applications or virtual desktops using the SecureICA feature. SecureICA uses a RC5 algorithm in order to encrypt the ICA protocol. This algorithm has a negligible impact on performance on modern computer systems (even with 128-Bit encryption) and should therefore be enabled in all environments.

In scenarios where user sessions traverse public networks, Citrix does not recommend SecureICA as the only method of encryption. This is because SecureICA does not provide authentication of the server. Therefore information could be intercepted as it crosses a public network and then be rerouted to a counterfeit server. Also, SecureICA does not check data integrity.

For such scenarios Citrix recommends adding another layer of encryption by deploying Citrix Access Gateway. As discussed earlier within this document Access Gateway is the only Citrix component located within the DMZ. It acts as a reverse proxy, which relays connections from the untrusted network to the internal servers. All traffic handled by Access Gateway is encapsulated into an SSL data stream.

In high security environments Access Gateway can be deployed in a double-hop architecture. This means that one appliance is located within the DMZ and an additional appliance is located close to the XenApp servers / virtual desktop (i.e. Top-of-Rack or collocated within the same blade chassis as virtual appliance). This ensures SSL encryption from the endpoint to the Access Gateway. However, the final leg between the Access Gateway and the XenApp server / virtual desktop remains unencrypted (almost end-to-end SSL encryption).
Virtual Desktop Security

By far, the most complex task when securing a virtual desktop environment is developing a security strategy for the actual virtual desktop. This involves a large variety of technologies and techniques, whose specific configuration is highly dependent on an organization’s security requirements. Various organizations such as Microsoft, the US-based National Security Agency (NSA) or the German Bundesamt für Sicherheit in der Informationstechnik (BSI) provide guidelines for securing the operating systems. These should be reviewed before developing a security strategy.

The task of securing a virtual desktop can be divided into the following sub-tasks.

Securing the Operating System

Since the Windows operating system is the foundational layer for every virtual desktop or published application, security measures have to start here. The specific security configuration depends on the requirements of an organization as well as their risk of exposure. For detailed guidance on securing the OS layer as well as low/medium and high security configuration samples, please refer to CTX134081 - Planning Guide - Citrix XenApp and XenDesktop Policies. In addition the following items are valid for all Citrix infrastructures.

- **Deploy all security hotfixes.** In general all security hotfixes for the operating systems (as well as the installed applications) should be tested and deployed immediately after public release. Microsoft offers a notifications service for security bulleting and security advisories. Administrators should subscribe to this service in order to remain up-to-date. To simplify the deployment process for our customers, Citrix tests all relevant Microsoft Windows hotfixes (Monthly testing of Microsoft Security Patches). This testing can provide an initial indication of issues, but does not make individual testing redundant.

- **Implement anti-virus scanners.** AV scanners should be implemented at all components of a virtual desktop infrastructure (i.e. file servers, proxy servers, XenApp Workers, etc.). Virus pattern updates should be tested (to prevent false positives) and rolled out to all systems immediately after becoming available. In addition organizations should consider CTX127030 - Citrix Guidelines for Antivirus Software Configuration.

- **System placement.** XenApp Servers and virtual desktops should not be exposed to untrusted networks. In scenarios where users access the infrastructure via an untrusted network, such as the Internet, a Citrix Access Gateway solution should be implemented.

- **Anonymous user accounts (XenApp only).** During installation XenApp creates server local users accounts, which are used for anonymous user access. If all users have a user account and anonymous access is not required, these local accounts should be disabled or deleted.

- **Securing the virtual desktops by means of Microsoft Security Baselines.** Please refer to chapter “Endpoint Security” within this document.
Securing the User layer

The second aspect, which needs to be considered when securing a virtual desktop environment, is the user layer. Similar to what has been stated earlier, the level of security restriction depends on the specific requirements of an organization. For detailed guidance on securing the user layer as well as low/medium and high security configuration samples, please refer to CTX134081 - Planning Guide - Citrix XenApp and XenDesktop Policies. The following items are valid for all Citrix infrastructures.

- **User Permissions.** Users should be granted default user permissions only, in order to ensure users cannot modify system critical configurations or interfere with other users working on the same system. In case an application requires elevated user rights it should be evaluated if this application can be sandboxed by means of Citrix Application Streaming or Microsoft App-V or if the application can be completely isolated on dedicated systems.

- **Application control.** In environments with above average security requirements, administrators should tightly control which applications users can execute. By ensuring only trusted executables or scripts can be used, the risk-exposure can be minimized. This can be achieved by means of Software Restriction Policies, which are part of Windows Group Policies. 3rd party software, such as AppSense Application Manager, Tricerat Application Security Solutions or RES Workspace Manager all allow more fine-grained control.

**Smart Auditor (XenApp only)**

SmartAuditor captures and archives screen updates, including mouse activity and the visible output of keystrokes in secured video recordings to provide a record of activity for specific users, applications, and servers. Organizations that use SmartAuditor have a better chance of proving criminal intent, where it exists, by using video evidence combined with traditional text-based eDiscovery tools.

SmartAuditor allows organizations to record on-screen user activity for applications that deal with sensitive information. This is especially critical in regulated industries such as health care and finance, where compliance with personal information security rules is paramount.

SmartAuditor playback protection should always be enabled in order to automatically encrypt recorded files before they are downloaded for viewing in the SmartAuditor Player. Playback protection prevents recorded files from being copied and viewed by anyone other than the user who downloaded the file.

The security of SmartAuditor can be further enhanced by assigning digital signatures to session recording.
Infrastructure Security

Securing the infrastructure components as well as the related network communication is the final piece of the virtual desktop security puzzle. For simplicity, this section will focus on infrastructure components only, which are directly adjacent to a Citrix environment and which exist within most organizations. Since the vast majority of organizations consider the data center as a trusted zone, the majority of the security measures outlined within this section will apply to high security environments only.

- **Securing Active Directory traffic (SSL).** The LDAP (Lightweight Directory Access Protocol) communication, which is used to read from and write to Active Directory, is transmitted unsecured by default. In order to make LDAP traffic confidential and secure, Secure Sockets Layer (SSL) / Transport Layer Security (TLS) technology can be implemented. To enable LDAP over SSL (LDAPS) a server certificate issued by a trusted certification authority (CA) must be installed on every domain controller. Further information about LDAPS can be found in KB321051 - How to enable LDAP over SSL.

- **Securing IMA data traffic (XA only).** The Independent Management Architecture (IMA) is the underlying architecture used in XenApp for configuring, monitoring, and operating all XenApp functions. The IMA data store stores all XenApp configurations. By default the configuration data is encrypted by means of a Citrix proprietary algorithm. The IMA encryption feature provides a more robust AES encryption algorithm to protect sensitive data in the data store. In order to use this feature identical encryption keys must be loaded on all XenApp servers within a farm. Enabling IMA encryption also provides an additional layer of security for the data preserved by the Configuration Logging feature. Further information can be found in eDocs - Planning for IMA Encryption.

- **Configuration Logging (XA only).** The Configuration Logging feature enables administrators to keep track of administrative changes made to a XenApp server farm environment. By generating the reports that this feature makes available, admins can determine what changes were made to the XenApp farm, when they were made, and which administrators made them. This is especially useful when multiple administrators are modifying the configuration of a server farm. Configuration Logging also facilitates the identification and, if necessary, reversion of administrative changes that may be causing problems for the server farm. When this feature is enabled for a licensed server farm, administrative changes initiated from the Citrix AppCenter, CLI utilities and custom tools using the SDK lead to the creation of log entries in a central Configuration Logging database. For environments with increased security needs, it is recommended to disable “Allow changes to the farm when logging database is disconnected” and to enable “Require administrators to enter database credentials before clearing the log”.


- **Securing Citrix License Server Traffic (SSL).** When accessing the admin console of the Citrix License Server, all data (incl. username / password) traverses the network unencrypted by default. In order to secure console communication HTTPS (Hypertext Transfer Protocol Secure / aka SSL) can be used to create a secure channel. A valid server certificate issued from a trusted certificate authority (CA) needs to be installed on the license server. Further information can be found within the Help section of the License Server Console.

- **Securing the Host Connection traffic (XenDesktop only).** XenDesktop can integrate with the virtualization platform (XenServer, Hyper-V, vSphere) in order to automate creating virtual desktops or to orchestrate start/stop/suspend/resume cycles of the VMs. This network communication consists of administrative commands, VM status messages as well as an initial authentication, during which username and password of the service account are sent over the wire. In order to make hosting traffic confidential and secure, Secure Sockets Layer (SSL) technology should be implemented for XenServer and vSphere based environments. If Hyper-V is used, XenDesktop leverages the Windows Communication Foundation (WCF) protocol by default in order to secure the network communication. For more information please refer to eDocs – Using XenDesktop with XenServer or eDocs - Using XenDesktop with vSphere.

- **Securing the user profile share.** Since user profiles can contain sensitive data, unauthorized access should be prevented by means of tight share permissions and/or NTFS permissions. The permissions recommended by Citrix, which ensure a high level of security, can be found in eDocs – Securing a profile manager deployment.

- **Separating infrastructure components using vLANs.** Virtual networks (vLANs) can be used to ensure that there is a high level of security at critical boundaries between the various infrastructure / management components and the Citrix environment. Dividing the network into smaller entities allows a fine-grained control over which servers / ports can be accessed and will minimize the capabilities of malicious users of pivoting onto more privileged systems. A sample vLAN segmentation is provided below:
  
  - **User vLANs:** In traditional client server infrastructures administrators could secure the data center by placing firewalls at the perimeter of the data center (internally and externally). For modern virtual desktop scenarios the network security paradigm needs to be changed, since user desktops are now hosted inside the data center and a compromised desktop could access / infect backend server systems. Therefore systems directly accessed by users should be separated in a specialized vLAN. For service provider scenarios an additional segmentation (as outlined below) might be required:
    
    - **Multi-Tenant vLAN:** Houses all the XenApp servers / virtual desktops directly accessed by many customers.
• **Tenant vLAN.** Houses only the XenApp servers / virtual desktops directly accessed by a specific customer.

  o **Provisioning vLAN.** Contains the Provisioning Servers, which provide the central image management functionality for the infrastructure.

  o **Authentication vLAN.** The authentication vLAN contains the Microsoft Active Directory Forest and Domains within a secured network. Only specific secured access to Active Directory capabilities are enabled in this vLAN for specific users, administrators and machines from the other networks.

  o **Management vLAN.** The management vLAN contains many of the foundational network services necessary in a hosted environment such as Domain Name Services, NTP and SNMP as well as other services provided by the CSP. In some cases an out-of-band management vLAN is implemented, which provides access for monitoring (i.e. SNMP) and remote administrative access to servers and other components. In such scenario the Authentication vLAN will provide the foundational network services.

  o **Application vLAN.** This vLAN contains the back-office applications that enable web, mail, collaboration and line of business application backend services. Leverage these vLANs and services across tenants or dedicate them to a specific tenant, as determined by the CSP and subscriber service level agreements.

• **Delegated Administration.** Within large IT organizations, administrative tasks are typically performed by specialized teams (i.e. support level 1 – 3), who may need to access the same administrative consoles. In order to prevent unauthorized changes, a delegated admin model should be developed, which defines the admin rights per team/level fine-grained. More information, including sample delegated admin models for Citrix environments, can be found in CTX133786 - [Operations Guide - Support and Maintenance Citrix Desktop and Datacenter](#)
• **Specialized User Accounts.** It is a recommended security practice to create user accounts specialized for a single purpose. By separating accounts and limiting the permissions assigned to each account, the opportunity for a malicious user or process to compromise the environment, can be reduced. The following list provides a sample for specialized user accounts:

  o **User Account.** Every user within an organization should get a personalized user account. This account has default user permissions, is used for day-to-day work and its password is changed on a regular schedule.

  o **Admin Account.** Every admin user of an organization gets a personalized admin account in addition to the normal user account. The admin account holds all administrative permission required. This account should not be used for normal day-to-day work (just for admin tasks) and its password is changed on a regular schedule.

  o **Service Account.** These accounts are created for services, which require a domain logon for normal operations. This account gets only the permissions required by the respective service and its password is static. Since the password is not changed regularly it should be of high complexity (min. 16 alpha numeric and special characters).

Further information about separating networks in service provider scenarios can be found within the [Service Provider Reference Architecture](#) document (requires MyCitrix logon). A listing of TCP ports used by Citrix technologies can be found in CTX101810 – [Ports used by Citrix Technologies](#).
Security Levels

The following table outlines recommended configurations for low and high security environments.

<table>
<thead>
<tr>
<th>Security Measure</th>
<th>Low - Security (Baseline)</th>
<th>High - Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Engineering awareness training</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Common security measures (Firewall, patches, AV)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Implementing the Microsoft Specialized Security - Limited Functionality (SSLF) desktop security templates</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Trusted Server Configuration</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>ICA File Signing</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Access Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypting User Device / Web Interface or Storefront Communication</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Encrypting Web Interface or Storefront / Citrix Server Communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hosting the Citrix components on the internal network / implementing a reverse-proxy appliance (i.e. Access Gateway) for Remote Access scenarios</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Securing the Secure Ticket Authority communication</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Authentication Security (depending on requirements and existing infrastructure)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anonymous Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Explicit Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pass-Through Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Card Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Require authentication on reconnect and log reconnect attempts</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Reduce Web Interface / Storefront time out</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Session Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabling SecureICA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Double-Hop Access Gateway with Top-of-Rack SSL termination</td>
<td>128 Bit</td>
<td>128 Bit</td>
</tr>
<tr>
<td><strong>Virtual Desktop Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Auditor</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Common security measures (patches, AV)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Enabling Windows Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable / Remove anonymous user accounts (XenApp only)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Implementing the Microsoft Specialized Security - Limited Functionality (SSLF) desktop security templates</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Implementing application control</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For more information please refer to CTX134081 - [Planning Guide - Citrix XenApp and XenDesktop Policies](#).
<table>
<thead>
<tr>
<th><strong>Infrastructure Security</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure LDAP</td>
<td>X</td>
</tr>
<tr>
<td>IMA encryption</td>
<td>X</td>
</tr>
<tr>
<td>Configuration Logging</td>
<td>X</td>
</tr>
<tr>
<td>Securing License Server Traffic (SSL)</td>
<td>X</td>
</tr>
<tr>
<td>Securing host connection traffic</td>
<td>X</td>
</tr>
<tr>
<td>Securing user profile share</td>
<td>X</td>
</tr>
<tr>
<td>Separating infrastructure components using vLANs</td>
<td>X</td>
</tr>
<tr>
<td>(separating virtual desktops)</td>
<td></td>
</tr>
<tr>
<td>Develop a delegated administration model</td>
<td>X</td>
</tr>
<tr>
<td>Implement specialized user accounts</td>
<td>X</td>
</tr>
</tbody>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Change Description</th>
<th>Updated By</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Document</td>
<td>Thomas Berger – Architect</td>
<td>August 24, 2012</td>
</tr>
</tbody>
</table>

With feedback / input from:
- Daniel Feller – Lead Architect
- Andy Baker – Architect
- Rich Meesters – Architect
- Simon Jackson – Architect
- Martin Zugec – Principal Consultant
- Eric Beiers – Principal Consultant

---

### About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2011 was $2.20 billion.

©2012 Citrix Systems, Inc. All rights reserved. Citrix®, Access Gateway™, Branch Repeater™, Citrix Repeater™, HDX™, XenServer™, XenApp™, XenDesktop™ and Citrix Delivery Center™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.