



# System Hardening Guidance for XenApp and XenDesktop

Version 1.1

Joint white paper from Citrix and Mandiant to understand and implement hardening techniques for app and desktop virtualization

## Table of Contents

Introduction .....	1
Top Application and Desktop Virtualization Risks and Recommendations .....	2
Environment or Application Jailbreaking.....	2
Network Boundary Jumping.....	10
Authentication.....	12
Authorization.....	15
Inconsistent Defensive Measures .....	18
Non-configured or Misconfigured Logging and Alerting.....	20
Summary .....	22
References .....	23
Contributors.....	24

## Introduction

Global organizations including healthcare, government and financial services rely on Citrix XenApp and XenDesktop to provide secure remote access to environments and applications. When properly configured, Citrix XenApp and XenDesktop provide security measures that extend beyond what is natively available in an enterprise operating system by providing additional controls enabled through virtualization. Citrix and Mandiant are working together to enhance the security of virtualized environments. This joint Citrix and Mandiant white paper outlines recommendations and resources for establishing a security baseline for Citrix XenApp and XenDesktop and highlights some of the real world misconfigurations often uncovered by Mandiant security engagements.

This white paper provides summary guidance and resources for hardening against exposures that threaten server based computing and VDI environments, including XenApp and XenDesktop. All changes should be implemented in a test or development environment before modifying the production environment in order to avoid any unexpected side effects. Finally, all efforts should be reinforced and validated through continuous penetration testing against the virtualized environment as a whole. This should provide the greatest level of resiliency against a real-world attack.

*Note: The guidance presented in this white paper is designed to complement existing Citrix security guidance, including product-specific eDocs, KnowledgeBase articles and detailed Common Criteria configurations. References to this information are provided at the end of this white paper.*

## Top Application and Desktop Virtualization Risks and Recommendations

Virtualized environments include risks that must be mitigated at the architectural, configuration and administrative levels. The most common risks along with a short definition are listed below. Understanding the risk is the first step to developing an effective defense.

### Environment or Application Jailbreaking

#### Risks

Mandiant continues to observe that one of the commonly overlooked virtualization security issues is *environment or application jailbreaking*. Jailbreaking is the ability to abuse an application running in the virtualized or physical environment to launch other applications, spawn command shells, execute scripts and perform other unintended actions prohibited by administrators.

Application jailbreaking can provide an attacker with an initial foothold into the environment and domain. Based on Mandiant's investigative experience, it is common for attackers to leverage this initial foothold to gain access to the internal network, escalate privileges, move laterally, and compromise the entire enterprise environment.

An example of a common jailbreak is shown in Figure 1 using a virtualized published instance of Internet Explorer to launch a command shell that is running on the Citrix server farm.

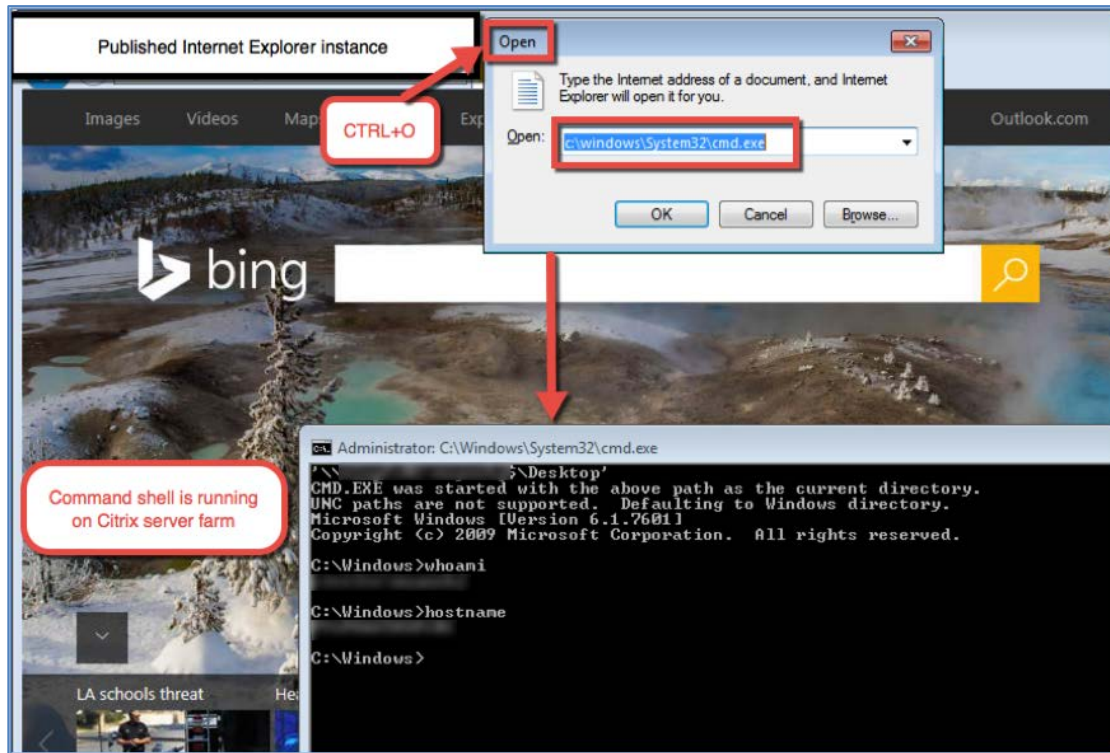


Figure 1: An example of a Citrix application jailbreak using a published instance of Internet Explorer

### Recommendations

Application jailbreaking is the most critical and complex risk associated with virtualized environments; thus, it will require a layered defense as shown in Figure 2.

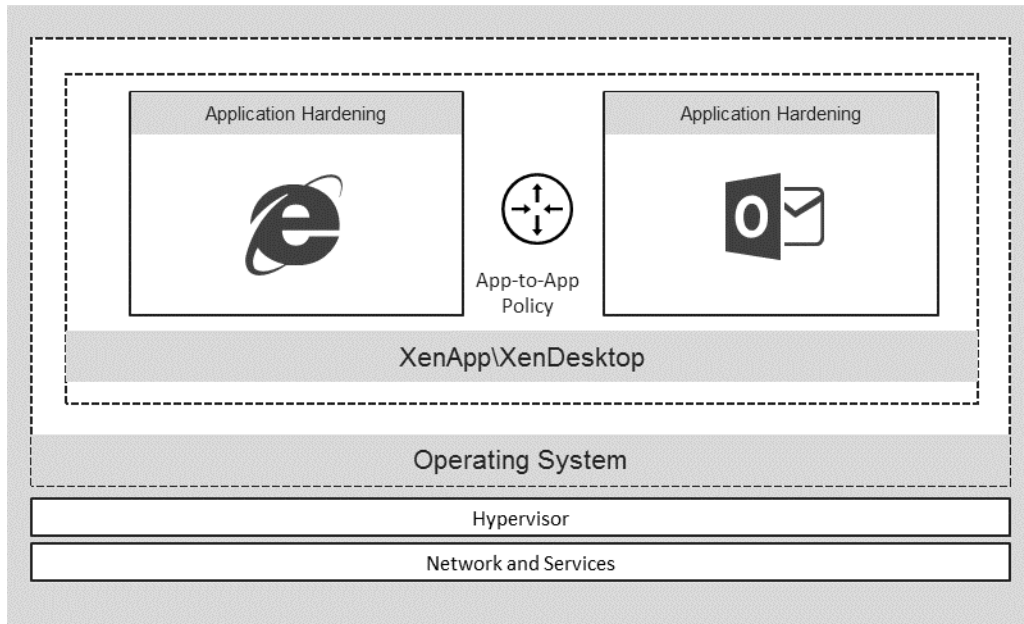


Figure 2: Many layers of defense required for a hardened environment

Defense against jailbreaking can be divided into categories:

- Preventing jailbreak attacks
- Minimizing the impact of attacks

Naturally, defenders want to prevent the jailbreak itself. This effort focuses on preventing an attacker from gaining access to unintended functionality. This can mean access to native administrative tools or third party attacker tools, usually with the end goal of command prompt access. Some of the best methods of prevention are listed below.

**Remove all undesired Windows and Citrix functionality** – Even if there appears to be no direct security threat, it is important to minimize the attack surface by removing unnecessary functionality. This includes removing:

- All shortcuts and help keys
- Access to all unused ICA channels
- Unused Windows functionality such as pre-installed applications
- Access to printers or devices that are not absolutely required
  - Especially since this often leads to file system access via “Print to File”
- Drivers that provide access to devices and services not required
  - E.g. floppy disk drives and music search

**Application Hardening** – Review policies and hardening guides for all applications that are published on a specific server. Apply the recommended hardening configuration; for example disable context menus, printing (if not required) or diagnostic tools. Be especially careful with applications that provide a development environment, such as Visual Basic for Applications language.

**Restrict access to internal tools** – Prevent access to all tools and utilities that can provide an attacker with access to the underlying operating system and/or other applications hosted on the same server. Defenders often think about Task Manager, Remote Desktop, and command shell, but most forget about PowerShell and PowerShell ISE. Restrict access to any other system utilities that are not needed for normal users (for example, many executables under the System32 folder). Access can be prevented using standard methods (Software Restrictions, AppLocker), using various 3<sup>rd</sup> party tools, or using NTFS permissions.

**Restrict access to external tools** – Restrict local network and Internet access to only approved domains and sites via a web proxy. Block all possible methods where software could be transferred to the local system. For highly-secured environments, consider running a separate XenApp farm to host secure virtual browsers.

**Restrict access to file system dialog** – The goal here is to prevent access to the file system where an attacker may have unintended access to launch executables, data-mine files, or write malware. This does not only mean Windows Explorer, but also any other methods that access the file system. A good example mentioned before is the Windows print functionality that allows a user to “Print to File” or use “Save As” dialogs. This recommendation is closely related to the previous recommendation about restricting access to the internal tools, as some system utilities can display the local file system as well (e.g. FTP.exe). Hiding local drives is another common method – either using Group Policy (hide & prevent access) or Group Policy Preferences (hide, but do not prevent access).

The final layer of defense addresses the situation where the attacker has been able to jailbreak from the application successfully. In this scenario we want to minimize the impact of the jailbreak by limiting what an attacker can do once the jailbreak is achieved. This will hopefully create some indicators and

warnings for the network defenders as the attacker attempts to escalate or laterally move within the network.

**Limit sensitive information on local and remote drives** – One of the easiest methods an attacker uses to escalate privileges is by finding a clear-text file with credentials. This could either be on the local computer or remote shares that do not require authentication. It is common for attackers to find credentials hard coded in scripts that execute without a human supplying a username and password.

One of the core principles when designing a Citrix environment is the proper segmentation of applications and deciding whether to build a few delivery groups with multiple servers, or separate the servers into multiple groups. When making the decision on server groupings, security isolation should be an important consideration. There are two primary options described below: separate applications on different servers or isolate applications on the same server.

**Separate applications on different servers** - In this scenario, very critical applications should be hosted on a dedicated set of servers, with few other applications installed on the same server. Additionally, this server should be isolated from other servers at the network level. Isolating applications on a specific set of servers allows the implementation of different network level restrictions. For example, network administrators can now provide network level access to backend databases only from servers where the application is hosted. This configuration is shown below in Figure 3.

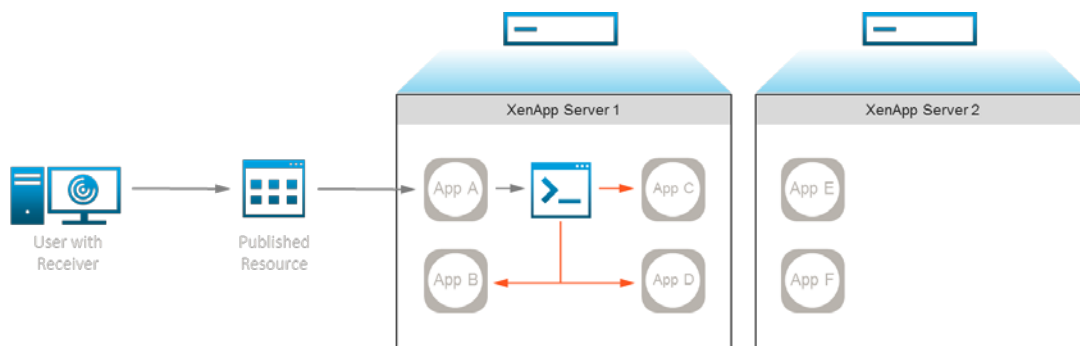


Figure 3: Isolating applications on different servers



**Isolate applications on the same server** – There are numerous methods to separate applications that are running on the same server. Common methods include usage of native Windows features such as Software Restriction Policies or AppLocker, but also include third-party tools. Separating applications by NTFS permissions is one of the oldest, but most reliable methods available.

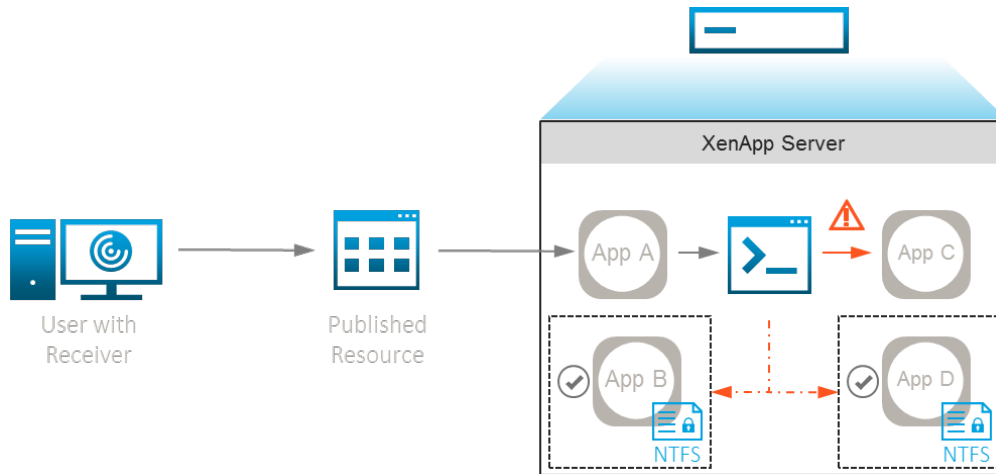


Figure 4: Isolating applications using NTFS permissions

### Group Policy Policies

Here are some examples of policies that administrators can implement to lock down desktops and server based environments, documented by Carl Stalhood: <http://www.carlstalhood.com/group-policy-objects-vda-user-settings/#lockdown>.

### Control Panel GPO Settings

- User Configuration | Policies | Administrative Templates | Control Panel
  - **Always open All Control Panel Items when opening Control Panel** = enabled
  - **Show only specified Control Panel items** = enabled, canonical names =
    - **Microsoft.RegionAndLanguage**
    - **Microsoft.NotificationAreaIcons**
    - **MLCFG32.CPL**
    - **Microsoft.Personalization**
    - **Microsoft.Mouse**
    - **Microsoft.DevicesAndPrinters**
    - **Microsoft.System** (lets users see the computer name)

- User Configuration | Policies | Administrative Templates | Control Panel | Add or Remove Programs
  - **Remove Add or Remove Programs** = enabled
- User Configuration | Policies | Administrative Templates | Control Panel | Programs
  - **Hide the Programs Control Panel** = enabled

### ***Desktop GPO Settings***

- User Configuration | Policies | Administrative Templates | Desktop
  - **Hide Network Locations icon on desktop** = enabled
  - **Prohibit user from manually redirecting Profile Folders** = enabled
  - **Remove Properties from the Computer icon context menu** = enabled
  - **Remove Properties from the Recycle Bin icon context menu** = enabled

### ***Start Menu & Taskbar GPO Settings***

- User Configuration | Policies | Administrative Templates | Start Menu & Taskbar
  - **Clear the recent programs list for new users** = enabled
  - **Do not allow pinning Store app to the taskbar** = enabled
  - **Remove and prevent access to Shut Down, Restart, Sleep, and Hibernate commands** = enabled
  - **Remove common program groups from Start Menu** = enabled (only if you have some other means for putting shortcuts back on the user's Start Menu/Desktop. Also, enabling this setting [might prevent Outlook 2013 desktop alerts](#). Microsoft [3014833](#))
  - **Remove Help menu from Start menu** = enabled
  - **Remove links and access to Windows Update** = enabled
  - **Remove Network Connections from Start menu** = enabled
  - **Remove Network icon from Start menu** = enabled
  - **Remove Run menu from Start menu** = enabled
  - **Remove the Action Center icon** = enabled (not in Windows 10)
  - **Remove the networking icon** = enabled
  - **Remove the Security and Maintenance icon** = enabled (Windows 10)
  - **Remove user folder link from Start menu** = enabled

### ***System GPO Settings***

- User Configuration | Policies | Administrative Templates | System
  - **Prevent access to registry editing tools** = enabled, disable regedit from running silently = **No**
  - **Prevent access to the command prompt** = enabled, disable command prompt script processing = **No**

Disabling registry editing tools also disables **reg.exe**. This is true even if *silently* is set to **No**.

### Explorer GPO Settings

- User Configuration | Policies | Administrative Templates | Windows Components | File Explorer (Windows 8+) or Windows Explorer (Windows 7)
  - **Hide these specified drives in My Computer** = enabled, **Restrict A, B, C, and D drives only**
  - **Hides the Manage item on the File Explorer context menu** = enabled
  - **Prevent access to drives from My Computer** = enabled, **Restrict A, B, C, and D drives only**. If this setting is enabled, you can't use Start Menu's search to find programs.
  - **Prevent users from adding files to the root of their Users Files folder** = enabled
  - **Remove "Map Network Drive" and "Disconnect Network Drive"** = enabled
  - **Remove Hardware tab** = enabled
  - **Remove Security Tab** = enabled

Note: A detailed version of policies and registration settings is available at <http://www.citrix.com/about/legal/security-compliance/common-criteria.html>.

### Hiding Disk Drives

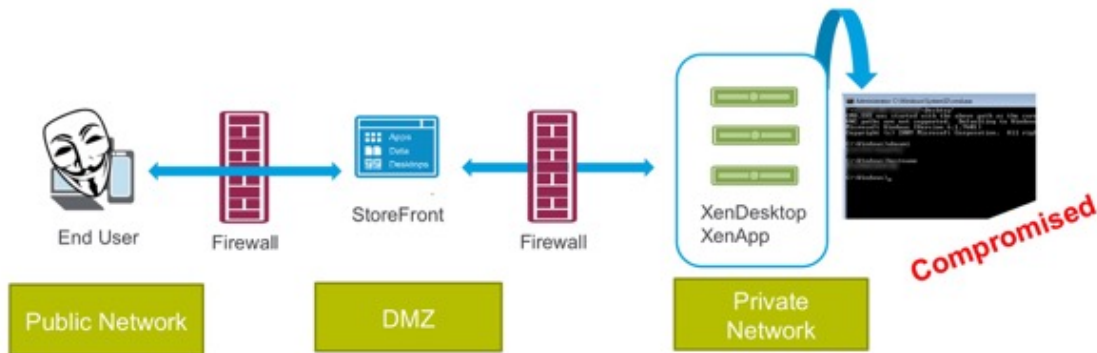
#### To hide specific drive letters:

1. User Configuration → Preferences → Windows Settings → Drive Maps → New Mapped Drive
2. Choose Action Update → Drive Letter Existing C → Hide this drive
3. Common Tab: Run in logged-on users Security

## Network Boundary Jumping

### Risks

Network boundary jumping unintentionally allows an attacker to move across trust levels. For Internet-available virtualized environments this often means bypassing the DMZ altogether. In other words, when a jailbreak occurs on an Internet-facing Citrix or Microsoft Remote Desktop instance, the shell obtained is often on the internal network and not contained within a DMZ. An example of boundary jumping is shown in Figure 5.



**Figure 5: An insecure architecture can allow an Internet-based attacker to obtain a foothold in the internal network after initial compromise**

As shown in Figure 5, the StoreFront end or Citrix NetScaler Gateway (positioned in the DMZ) is merely pass-through authentication for the backend Citrix resources. The applications and environments reside on the Citrix server farm, potentially providing an attacker a shell in this private network when compromised, as shown in Figure 5. Thus, it is important to understand the architecture and possible consequences of a Citrix jailbreak should it occur. The question should be asked: “If a jailbreak were to occur, would the attacker have a foothold into the internal network?”

### Recommendations

Direct external access to internal resources from the Internet must be disallowed as an architectural principle. More specifically, each trust boundary must enforce user access to trusted enclaves through layers of security that provide proper user restrictions and monitoring. In the case of Citrix virtualization, it may be tempting to place only the web front-end within the DMZ, but the position of the Citrix resource zone is also critical to security.

Network boundary jumping bypasses all traditional guidance of maintaining separate zones based on the risk and sensitivity of the network and resources within. Mandiant recommends the following architecture to prevent attackers from being able to boundary jump directly into the internal or otherwise critical environment:

- ✓ Architect Citrix sites requiring different trust levels into their own DMZ environment.
- ✓ Enforce strong multi-factor authentication access utilizing TLS for all sensitive resources – internal and external. Consider the use of FIPS-validated algorithms, where appropriate.
- ✓ Implement a double-hop DMZ architecture utilizing NetScaler.
- ✓ Consider advanced ecosystem integrations with XenApp and XenDesktop, including: DLP, IRM, whitelisting, watermarking, tokenization, and redaction.

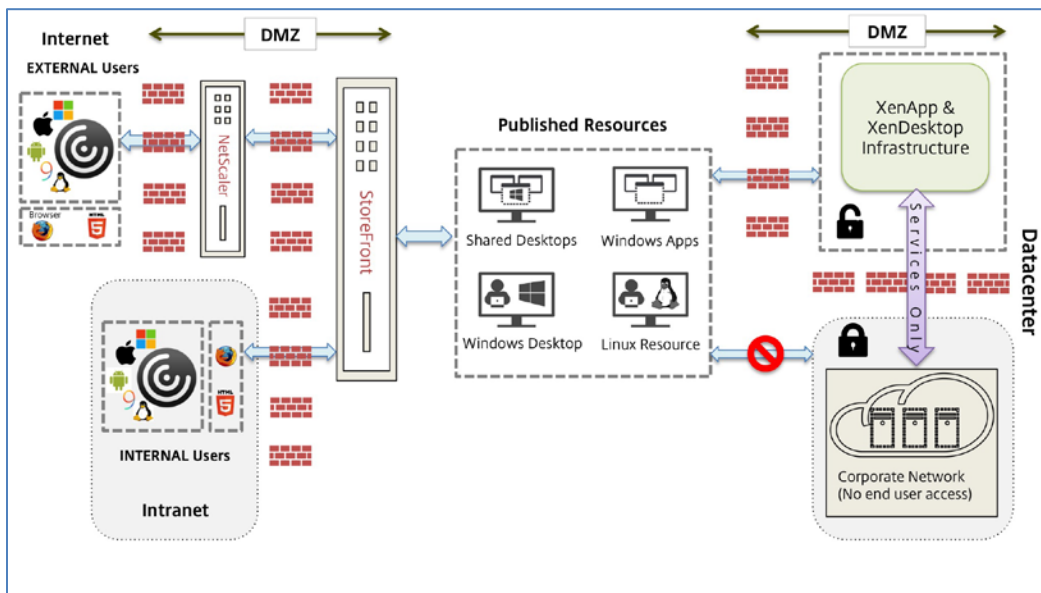


Figure 6: Sample architecture to segment the XenApp Site into a DMZ

## Authentication

### Risks

Mandiant's proactive engagements and incident response investigations typically reveal a large number of virtualized environment misconfigurations. One of the most common categories deals with authentication issues. The following recommendations will pay dividends toward securing a virtual environment:

- ✓ Citrix StoreFront supports a number of different authentication methods including NetScaler Gateway pass-through, Domain pass-through and Smartcard. NetScaler Gateway supports LDAP, RADIUS (token) and Client certificates. The specific option chosen will depend on the sensitivity of the environment and enterprise policy.
- ✓ In addition to strong credentials, the authentication policy should be set as LDAP + Token, LDAP + Smartcard or Token + Smartcard for increased security. Using only an LDAP user name and password is not recommended for production environments. The following article contains instructions and further resources for configuring multi-factor authentication on a NetScaler Gateway:  
<http://support.citrix.com/article/CTX125364>
- ✓ Increase the strength of credential validation as data sensitivity increases, using application-specific policy and multiple credential sources.
- ✓ Enable SSO (Single Sign-on) for access to internal, partner, cloud and SaaS resources, brokering passwords through NetScaler so that user credentials are always presented via strong authentication.
- ✓ Disallow the use of login scripts that contain credentials, service accounts, and default passwords.
- ✓ Monitor privileged accounts for brute force attacks and other signs of abuse.
- ✓ Require successive strong authentication for security-sensitive operations such as password changes, certificate and private key updates and those that require a higher level of non-repudiation.

More details on access and authentication best practices can also be found in the [XenDesktop handbook](#).

## Recommendations

Authentication for virtualized environments can pose significant risk if not properly configured. Virtual environments are very flexible in deployment, allowing administrators to publish anything from a simple time sheet to a full remote desktop. Thus, they may not always be recognized as a type of VPN access and afforded the same protections, such as multi-factor authentication. It is commonly understood that traditional VPN concentrators require multi-factor authentication, but web-based apps are often overlooked.

In environments where single-factor authentication is used for Citrix solutions, Mandiant commonly observes attackers using it to maintain access to the victim's environment post-compromise. Organizations often integrate Citrix authentication with Active Directory. If an attacker is able to dump username and password hashes from Active Directory, the attacker may use those credentials to log into the Internet-facing Citrix environment. Many attackers prefer Citrix/VPN access to traditional backdoors for the following reasons:

- They can access the victim's network using a full-featured virtualized desktop as if the attacker were on the internal network.
- Citrix network traffic may be encrypted, which makes it more difficult for the traffic to be inspected by network monitoring tools.
- It can be very difficult to identify malicious use of legitimate credentials.
- Backdoors, remote access tools, and other types of malware are noisier and easier to detect from a host and network-based perspective.
- Although passwords typically expire after 90 days, the attacker can re-dump passwords from the domain controllers or use another set of credentials to re-access the victim's environment.

For these reasons, we strongly recommend multi-factor authentication for remote access to any Citrix instances.

An example of single-factor and multi-factor authentication screens are shown in Figure 7 and Figure 8.

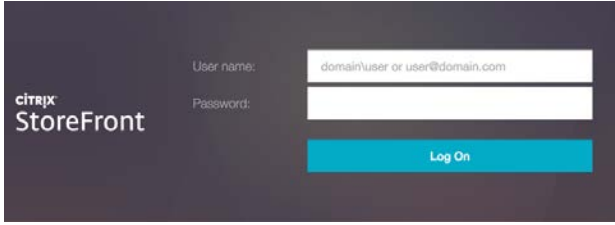


Figure 7: Single factor authentication

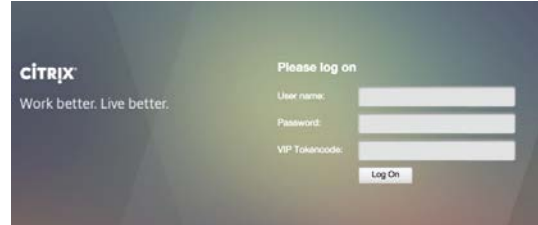


Figure 8: Multi-factor authentication



## Authorization

### Risks

Without multi-factor authentication, passwords are the primary access defense. Industry standard best practices should be followed to ensure strong passwords. This should include, at a very minimum: eight characters or more, at least one uppercase letter, at least one lowercase letter, and at least one special character or number. Additionally, every virtualized environment that is Internet accessible or sensitive in nature must require multi-factor authentication for all users.

Unrestricted disk, file share, or host access is common in enterprise environments; however, it is also a direct path to data loss and compromise. Any time the attacker can access disk, a file share, or other hosts, they may be able to jailbreak, propagate, or steal and corrupt data. The example shown in Figure 9 illustrates how an attacker can use file system access to use creative methods to launch command shells. Note that this file system access was provided via the native Windows “Print to File” functionality.

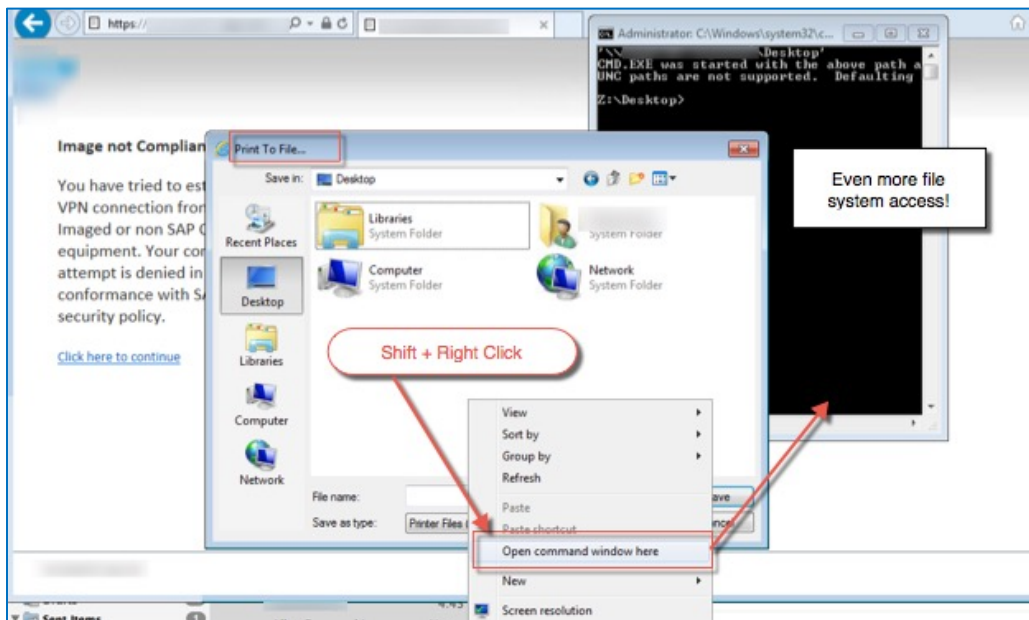


Figure 9: Unrestricted file system access used to jailbreak the system

### High-level solution:

Virtualization can completely remove disk access from remote users. Or if disk access is required, virtualization can be used to prevent access to the root of

the operating system. All file shares, sensitive hosts, and services should be scanned and evaluated to ensure proper authorization controls are applied.

*See the Recommendations and Guidance section for more details.*

## Recommendations

Proper authorization can be complex in any environment. Some issues are shared between both virtualized and non-virtualized environments; however, there are some that can be unique to virtualized environments. The following recommendations will help build a necessary layered defense:

- ✓ Configure accounts and services with the lowest level of rights and privileges required to perform role-specific tasks.
- ✓ Ensure execution of only trusted executables or scripts. This can be achieved by means of Software Restriction Policies, which are part of Windows Group Policies or by using Windows AppLocker to create rules to allow or deny applications from running. Information about AppLocker can be found here: <https://technet.microsoft.com/en-us/library/dd759117.aspx>.
- ✓ Disable disk access for those applications, users and services that do not specifically require it. Enforce read-only access where warranted. This includes client drive mappings. More information can be found here: <http://support.citrix.com/article/CTX133565>.
- ✓ Disable USB access for those applications, users and services that do not specifically require it. Utilize specific USB policies to enable USB with read, write and per device features where required. These can be easily achieved via access control policies. More information can be found here: <http://support.citrix.com/article/CTX133565>.
- ✓ Disable additional unused features, enabling only where required.
- ✓ Configure cryptographic services to only allow defined and approved certificate authorities, cryptographic algorithms and hash functions.
- ✓ Limit data remanence by keeping sensitive data off the endpoint and securely erasing temporary files.
- ✓ To gauge endpoint risk, perform endpoint inspection with the SmartControl and SmartAccess feature of NetScaler Gateway and XenApp, use the results in access policy determination.
  - SmartAccess configuration: <http://docs.citrix.com/en-us/netscaler-gateway/10-1/ng-xa-xd-integration-edocs-landing/ng-integrate-web-interface-apps-wrapper/ng->

[smartaccess-wrapper-con/ng-smartaccess-how-it-works-con.html](#)

- SmartControl configuration: <http://docs.citrix.com/en-us/netscaler-gateway/11/integrate-web-interface-apps/smart-control.html>

In addition, pay special attention to privileged access. Domain administrators, root users, network administrators and services with administrative access to crypto services, keys and certificates must be especially protected, as attackers target them heavily.

Consider certificate-based mutual authentication for privileged users, including domain admins, those with access to keys/certificates, those who manage cryptographic keys and certificates, and other security sensitive use cases.

## Inconsistent Defensive Measures

### Risks

Inconsistent defensive measures may permit activity within the Citrix environment that would otherwise be disallowed in other areas of the enterprise. For example, Mandiant has observed Citrix deployments in which the virtualized instances were not configured to require web traffic to traverse the enterprise web proxies, even though strong content filtering was in place for the rest of the organization.

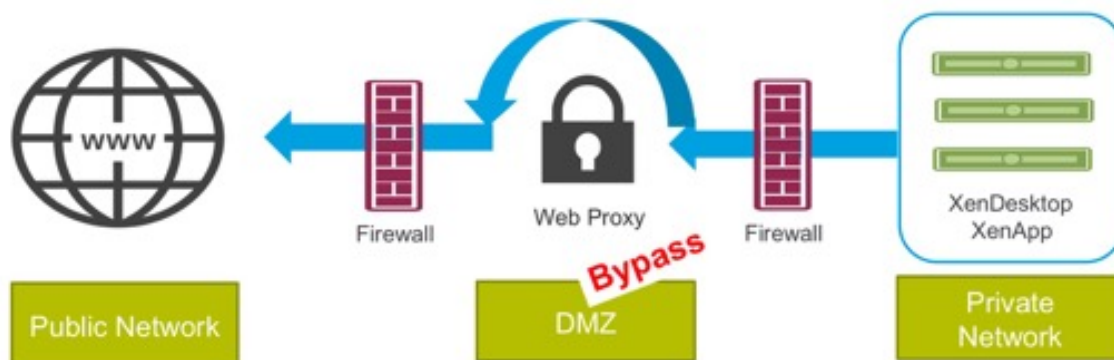


Figure 10: One example of an inconsistent defensive measure

### Recommendations

The same defensive measures afforded to non-virtualized environments should also be applied to a virtualized environment. However, this is often not the case, so here are some recommendations to serve as a reminder:

- ✓ Ensure the virtualized environment uses the same security stack as the non-virtualized environment. This includes IDS, IPS, multi-factor authentication, web proxies and advanced threat detection appliances.
- ✓ Host harden all components by using a Gold disk image when possible and enable cryptographic checksum and hashes on Gold disks and OS.
- ✓ Patch all involved components in a timely manner to include the infrastructure and hosts themselves.
- ✓ Automate the provisioning and de-provisioning processes with Citrix provisioning services or machine creation services.
- ✓ Automate Citrix site creation process via Citrix Life Cycle Management to bring consistency between development, test and production

environment. More information at

<https://www.citrix.com/products/workspace-cloud/tech-info.html>

- ✓ Maintain a consistent development, test and production environment that can be used to test security policies successfully.
- ✓ Enable Secure ICA connections in XenApp and XenDesktop for end-to-end TLS encryption of traffic including traffic inside the data center.  
<https://www.citrix.com/blogs/2014/12/11/how-to-secure-ica-connections-in-xenapp-and-xendesktop-7-6-using-ssl/>
- ✓ Lock down Citrix Database access to authorized administrators only.
- ✓ 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.

## Non-configured or Misconfigured Logging and Alerting

### Risks

Logs play an important role in detecting malicious activity and responding to incidents. If the incident occurred within a virtualized environment, logs will be critical to determining attacker activities such as jailbreaking, escalation, and data theft. Unfortunately, robust logging is often lacking in most environments – especially virtualized environments.

### Recommendations

Enable logging of important system, application, and security events. Ensure all logs are centrally collected and monitored by an appropriately selected security information and event management (SIEM) product.

Activities within a virtualized environment must be logged, monitored, and alerted upon the same as any other environment. Mandiant and Citrix recommend configuring logging, reporting and auditing to highlight anomalies and detect breaches.

- ✓ Configure logging, alerting and reporting on a per application basis to allow application-specific usage auditing.
- ✓ Send logging and alerting to a SIEM to detect access anomalies and data breaches.
- ✓ Configure auditors and audit processes as privileged users, writing their data into immutable storage enclaves.
- ✓ Citrix applications audit records for use and activity that when coupled with the audit capabilities of the Windows operating system provides unparalleled audit records that enhance an organization's ability to know and report on activity generated by a user that includes the following: connecting username, device name, IP of connecting workstation (inside and outside the corporate network), application used, duration, as well as capture of all errors/notifications (such as invalid password or unauthorized access attempts) that the application generates. This information is particularly valuable in investigating potential breaches or unauthorized access. The following link provides more details on monitoring with Citrix Director and EdgeSight  
[https://www.citrix.com/content/dam/citrix/en\\_us/documents/products-solutions/comprehensive-management-and-monitoring-with-citrix-director-and-edgesight.pdf](https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/comprehensive-management-and-monitoring-with-citrix-director-and-edgesight.pdf)

- ✓ In addition to user logging, Citrix XenApp and XenDesktop also provide configuration logging for administrative activities. The following link provides more details on configuration logging.  
<http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-5/cds-configlog-wrapper.html>.
- ✓ Smart Auditor features of XenApp and XenDesktop 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. Details can be found here:  
<http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-6/xad-monitor-article/xad-session-recording.html>.
- ✓ Administrators should take advantage of the NetScaler logging interfaces that can be used in various situations to meet the needs of a variety of customers and under different traffic conditions. These logging interfaces include: Syslog, Audit server, NetScaler web logging, and Historical reporting.

## Summary

Virtualization environments are relied upon to provide flexible access and advanced security, but they must be specifically hardened to required levels. By following the guidance in this paper, environment jailbreaking, network boundary jumping and others risks are better understood and prevented.

Citrix and Mandiant are working together to provide continued insights into threats against virtualization environments and actionable guidance for configuring against these threats.



## References

Strategic Content:

<http://www.citrix.com/secure>

Technical Content:

<https://www.citrix.com/products/xenapp-xendesktop/resources.html#topic=iso-security>

NetScaler Security Best Practices: Secure Deployment Guide for NetScaler MPX, VPX, and SDX Appliances

<http://support.citrix.com/article/CTX129514>

Payment Card Industry (PCI) and Citrix XenApp and XenDesktop Deployment Scenarios

[http://www.citrix.com/content/dam/citrix/en\\_us/documents/support/payment-card-industry-and-citrix-xenapp-and-xendesktop-deployment-scenarios.pdf](http://www.citrix.com/content/dam/citrix/en_us/documents/support/payment-card-industry-and-citrix-xenapp-and-xendesktop-deployment-scenarios.pdf)

Citrix solutions for Healthcare and Compliance

[https://www.citrix.com/content/dam/citrix/en\\_us/documents/products-solutions/citrix-solutions-for-healthcare-and-hipaa-compliance.pdf](https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-solutions-for-healthcare-and-hipaa-compliance.pdf)

Citrix XenApp and XenDesktop FIPS 140-2 Sample Deployments

[https://www.citrix.com/content/dam/citrix/en\\_us/documents/about/citrix-xenapp-and-xendesktop-76-fips-140-2-sample-deployments.pdf](https://www.citrix.com/content/dam/citrix/en_us/documents/about/citrix-xenapp-and-xendesktop-76-fips-140-2-sample-deployments.pdf)

Mandiant: <https://www.mandiant.com>

Hacking Exposed: <http://www.hackingexposed.com>

Chapter 7 of Hacking Exposed 7: Network Security Secrets and Solutions  
August 3, 2012 | ISBN-10: 0071780289 | ISBN-13: 978-0071780285

NIST National Checklist Program Repository

<https://web.nvd.nist.gov/view/ncp/repository>

The National Checklist Program (NCP), defined by the [NIST SP 800-70 Rev. 2](#)

Australia ASD Guidance:

<http://www.asd.gov.au/infosec/mitigationstrategies.htm>

UK Guidance:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/317481/Cyber\\_Essentials\\_Requirements.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf)



## Contributors

### **Citrix Systems:**

Kurt Roemer	Chief Security Strategist
Faisal Iqbal	Director, Sales Engineering
Christian Reilly	Vice President, CTO office
Chris Mayers	Chief Security Architect
Stacy Bruzek	Director, Solutions Marketing
Vishal Ganeriwala	Senior Director, Technical Marketing
Mayunk Jain	Senior Manager, Technical Marketing
Martin Zugec	Architect, Technical Marketing

### **Mandiant Consulting:**

Charles Carmakal	Vice President, Security Consulting Services
Tony Lee	Technical Director, Security Consulting Services

#### About Citrix

Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2015 of \$3.28 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at [www.citrix.com](http://www.citrix.com).

#### About FireEye, Inc.

Mandiant, a FireEye company, provides incident response and security assessment services to help organizations detect, prevent, and respond to cyber attacks. FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000. Learn more at <https://www.fireeye.com/services.html>

Publication date: December 1, 2016

Copyright © 2016 Citrix Systems, Inc. All rights reserved. Citrix, Citrix Receiver, and StoreFront are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.