

# RISK ASSESSMENT

For

## MFA Infrastructure

[DocDB ID 5839]

### Document Details

GENERAL			
<b>Description</b>	<b>Technical Risk Assessment: MFA Infrastructure</b>		
<b>Purpose</b>	A technical risk assessment is a useful tool to evaluate the individual elements of process or service for residual risks. Through a technical risk assessment, you define the Threats and Vulnerabilities (actors/actions that can exploit a specific flaw) along with the Risk and Mitigation (outcome of exploitation of a flaw and what you are doing to prevent exploitation). Any flaws or avenues for exploitation left over after applying the compensatory controls defined in the Mitigation is documented as a Residual Risk. It is this Residual Risk that is primarily considered and accepted before a service is offered.		
<b>Document Owner</b>	Michael Rosier	<b>Owner Org</b>	Core Computing Division
<b>Effective Date</b>	06/01/2016	<b>Review Date</b>	Annually

VERSION HISTORY			
Version	Date	Author(s)	Change Summary
1.0	06/01/2016	Michael Rosier	Original Version

## Contents

Document Details.....	1
Information and Security Contacts: .....	4
SYSTEM IDENTIFICATION .....	5
System Name/Title.....	5
System Type .....	5
Responsible Organization .....	5
System Operational Status.....	5
General Description/Purpose .....	5
System Architecture and Boundaries.....	5
System Inventory .....	5
Description .....	6
Risk Identification & Methodology .....	15
Likelihood Determination, Impact Analysis, and Risk Level.....	15
Threat Source Identification .....	15
Motivation and Threat Actions .....	15
Residual Risk Definition.....	15
Identified Threats, Vulnerabilities, Risks, Mitigations, and Residual Risks .....	16
Threats: Unauthorized Access .....	16
Threat: Unauthorized Access – User credentials with Citrix.....	16
Threat: Unauthorized Access – User credentials .....	16
Threat: Unauthorized Access – Password guessing .....	16
Threat: Unauthorized Access – Internet Search .....	17
Threat: Unauthorized Access – Social Engineering.....	17
Threat: Unauthorized Access – Sensitive data leakage .....	17
Threats: Unauthorized Physical Access.....	18
Threat: Unauthorized Physical Access .....	18
Threats: Malicious Content.....	18
Threat: Malicious Content .....	18
Threats: Environmental Threats .....	19
Threat: Environmental Threat.....	19



## Information and Security Contacts:

Title	Name	Email	Telephone	Initials
System Manager / Service Provider	Briant Lawson (XenApp)	<a href="mailto:blawson@fnal.gov">blawson@fnal.gov</a>	630.840.5524	
	Ken Fidler (VDA's)	<a href="mailto:fidler@fnal.gov">fidler@fnal.gov</a>	630.840.2763	
Application Managers – Citrix NetScaler/XenApp	Briant Lawson	<a href="mailto:blawson@fnal.gov">blawson@fnal.gov</a>	630.840. 6521	
	Ken Fidler	<a href="mailto:fidler@fnal.gov">fidler@fnal.gov</a>	630.840.2763	
Management Contact(s)	Jon Bakken (Division)	<a href="mailto:bakken@fnal.gov">bakken@fnal.gov</a>	630.840.4790	
	Mark Kaletka (Division)	<a href="mailto:kaletka@fnal.gov">kaletka@fnal.gov</a>	630.840.2965	
	Michael Rosier (Dept.)	<a href="mailto:mrosier@fnal.gov">mrosier@fnal.gov</a>	630.840.838	

## SYSTEM IDENTIFICATION

### System Name/Title

Fermilab identifier CSP- GSS-5839 has been assigned to the system discussed throughout this Risk Assessment.

### System Type

This system uses a multi-factor authentication gateway to provide access to a number of business and financial resources through an application virtualization solution. Some components of this solution are hosted within the Information Systems Major Application Boundary.

### Responsible Organization

Fermi National Accelerator Laboratory  
PO Box 500  
Batavia, IL 60510

### System Operational Status

It is in the operational phase of its life-cycle.

### General Description/Purpose

This technical risk assessment examines the threats, vulnerabilities, risks, mitigations and residual risks for the various methods implemented to achieve multi-factor authentication for both standard and privileged users.

## System Architecture and Boundaries

### System Inventory

**Table 1: MFA Infrastructure systems**

Hostname	Function	Physical Location	Hardware	Operating System
fermi-ts-rsa1.fnal.gov	Remote Desktop	FCC2	VM	Windows Server 2012 R2
fermi-ts-rsa2.fnal.gov	Remote Desktop	FCC2	VM	Windows Server 2012 R2
fermi-ts-rsa3.fnal.gov	Remote Desktop	FCC2	VM	Windows Server 2012 R2
fermi-ts-rsa4.fnal.gov	Remote Desktop	FCC2/FCC3	VM	Windows Server 2012 R2
fermi-ts-piv1.fnal.gov	Remote Desktop	FCC2	VM	Windows Server 2012 R2
fermi-ts-piv2.fnal.gov	Remote Desktop	FCC2	VM	Windows Server 2012 R2
fermi-ts-piv3.fnal.gov	Remote Desktop	FCC2/FCC3	VM	Windows Server 2012 R2
ctxns01.fnal.gov	NetScaler	FCC2	Citrix HW	Citrix NetScaler 11
ctxns02.fnal.gov	NetScaler	FCC3	Citrix HW	Citrix NetScaler 11
ctxsrv01.fnal.gov	Delivery Controller (RSA)	FCC2/FCC3	VM	Windows Server 2012 R2
ctxsrv02.fnal.gov	Delivery Controller (PIV)	FCC2/FCC3	VM	Windows Server 2012 R2

ctxsrv03.fnal.gov	Storefront	FCC2/FCC3	VM	Windows Server 2012 R2
ctxsrv04.fnal.gov	Storefront	FCC2/FCC3	VM	Windows Server 2012 R2
ctxsrv05.fnal.gov	SQL/License/Director	FCC2/FCC3	VM	Windows Server 2012 R2
proxext01.fnal.gov	Squid Proxy Server	FCC2/FCC3	VM	Red Hat Enterprise Linux 7
mfaprint.fnal.gov	MFA Print Server	FCC2/FCC3	VM	Windows Server 2012 R2

## Description

The following architectures have been implemented to provide multi-authentication for both standard and privileged users:

1. **Citrix MFA Environment** - Terminal Servers and Desktops fronted by a Citrix XenDesktop and Citrix NetScaler environment for standard and privileged users, accepting both RSA SecurID and PIV-I authentication.
2. **RSA SecurID Direct** - Terminal Servers and Desktops each with an RSA agent installed accepting direct connections from client systems for standard users.
3. **PIV-I Direct** - Terminal Servers and Desktops configured to accept PIV-I connections directly from client systems for privileged users.

The Citrix MFA Environment is considered to be the most scalable and strategic architecture for both standard and privileged users. The two “Direct” architectures will be used in some cases or even as a backup to the Citrix architecture, which will require occasional downtimes for patching and upgrades.

### *Citrix MFA Environment*

In order to provide a scalable environment for users who need to access computing resources with Multi-Factor Authentication (MFA), a Citrix NetScaler/XenApp/XenDesktop environment has been deployed. This environment supports a wide range of clients, such as tablets or phones running Android, iPad, or Windows, Windows PC’s, Mac, and Linux. Depending on the type of authentication used, some of these devices may only support using RSA. Mac and Windows have been tested and work with smartcards, such as PIV-I.

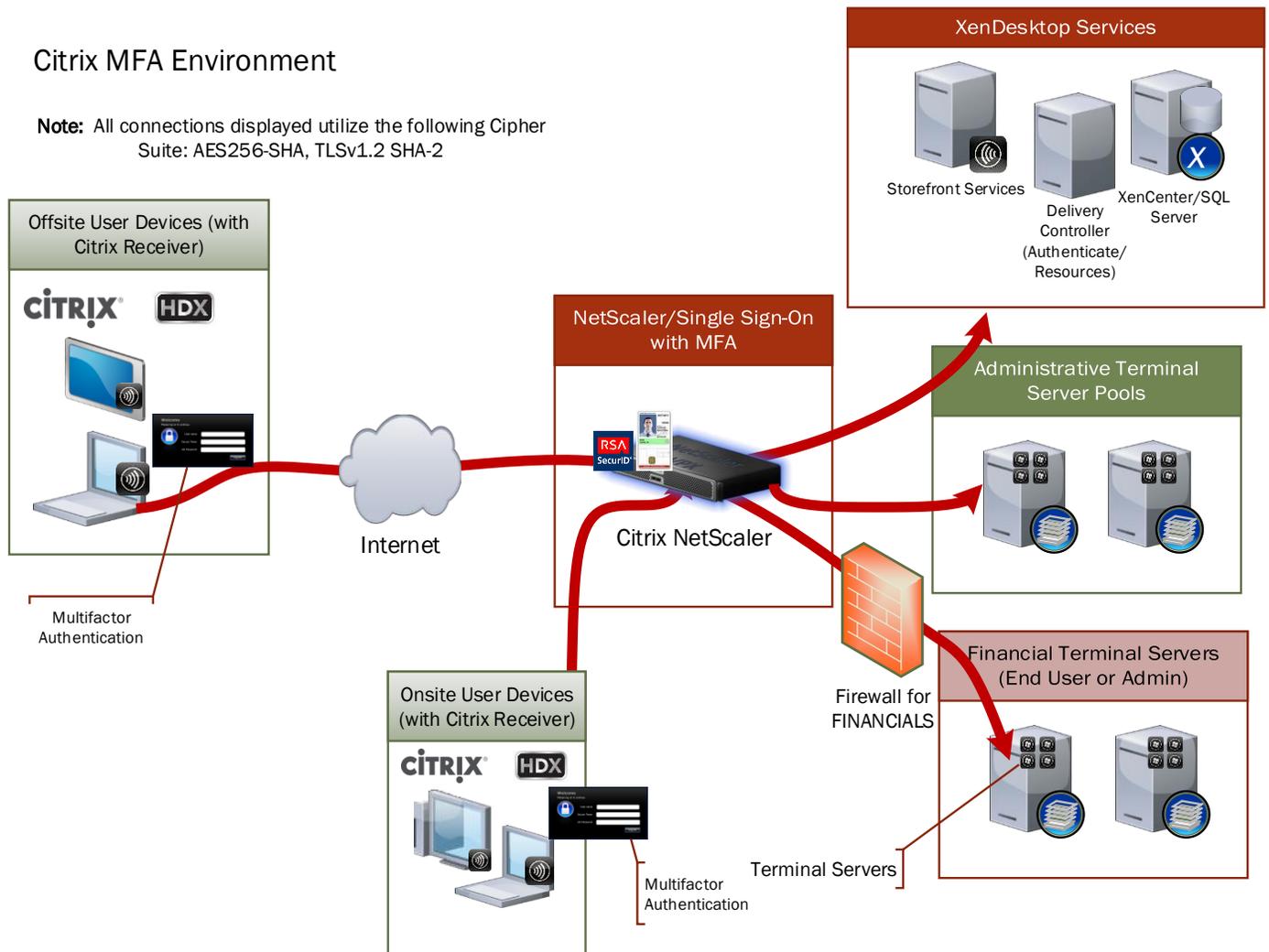
### **Security Highlights of the Citrix MFA Environment**

- Citrix NetScaler session timeout: 30 minutes
- Citrix application session timeout: 18 hours (Actual application timeouts still apply)
- Citrix component servers and VDAs patched monthly.
- Domain policies (including security) apply to Citrix component servers and VDAs.
- Citrix NetScaler appliances patched monthly or when critical updates are available.
- Squid White List Proxy used to allow external connections to providers, applications, and taxing bodies.
- Central Authentication configured for end user and system administrator logons.
- Single Sign-On enabled to minimize how often passwords are required to access resources.
- Authentication is first established with RSA or PIV-I; with RSA the username and password are attempted after successful token authentication to reduce account lockouts.
- In order to keep files from within the MA boundary at all times, an Active Directory GPO is used to control which features are available to clients. Remote copy/paste and device redirection have been disabled by policy. Group policy prevents local override of these RDP restrictions.

- Remote Desktop users have NOT been granted local administrative privileges on the Citrix MFA terminal servers or desktops used to access the financial systems applications.
- Network firewall rules limit which inbound services are available to MFA terminal servers and desktops. All remote sessions are required to use encryption, enforced by group policy and the Citrix NetScaler. Outbound access over RDP or any other protocol allowing interactive sessions is not allowed unless explicitly allowed through the firewall.
- Network firewall rules limit onsite traffic (inbound and outbound) from MFA terminal servers and desktops used to access the financial systems to nodes providing only DNS, authentication, WSUS (patching), Antivirus, and KMS (license) services.
- Removable media disabled through Citrix.

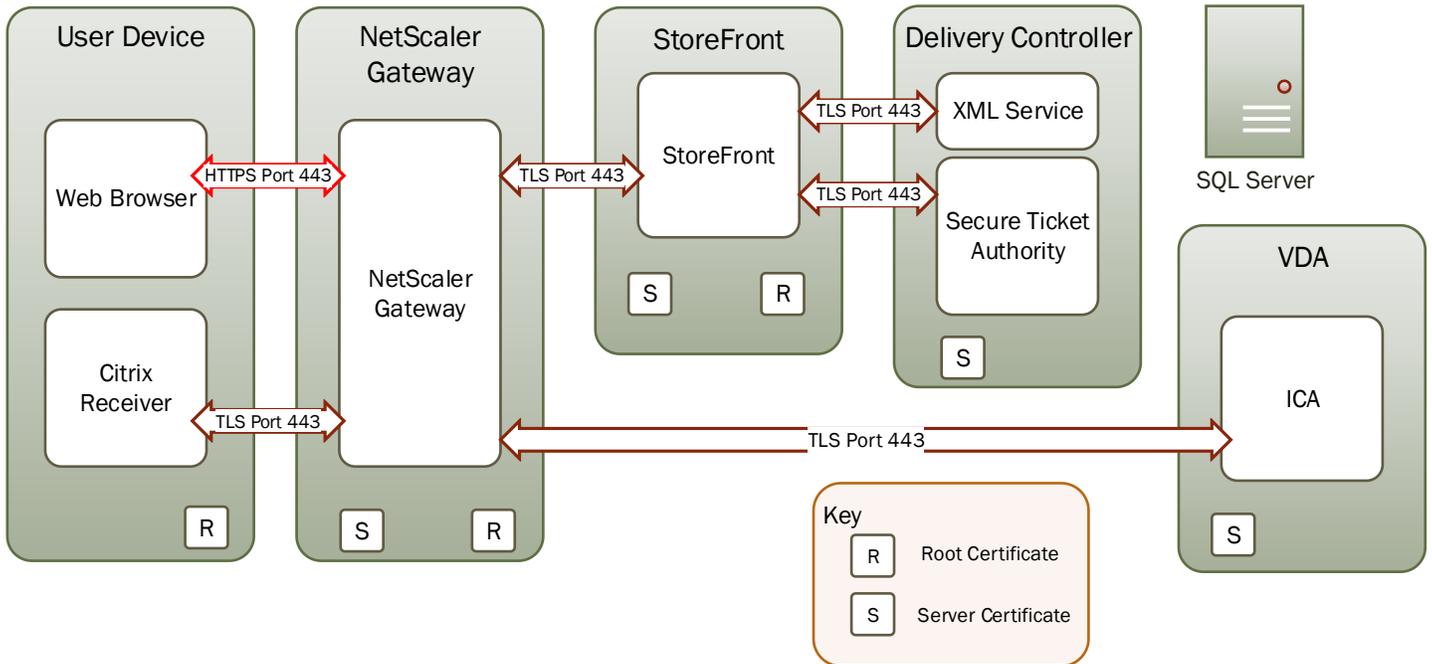
## Citrix MFA Environment

**Note:** All connections displayed utilize the following Cipher Suite: AES256-SHA, TLSv1.2 SHA-2



## How the Citrix components interact

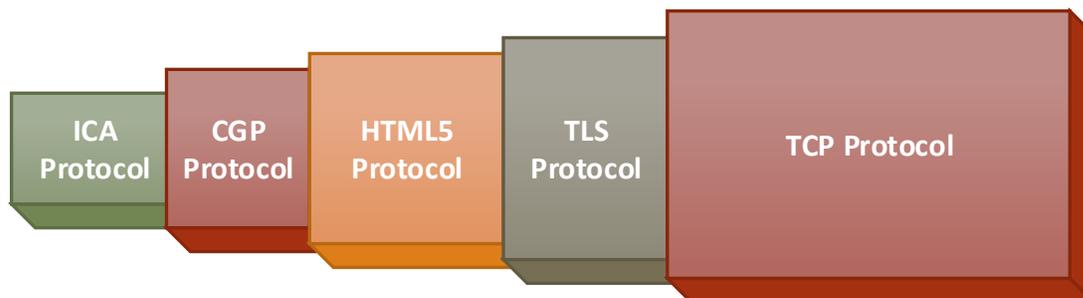
Traffic between the web browser on the user device and NetScaler Gateway is secured using HTTPS. All other traffic is secured using TLS. The diagram below shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.



## HTTPS in the VDA (Citrix ICA client running on Windows or Linux)

The ICA stack speaks multiple layers. ICA protocol at the core (1494); it is wrapped in the more elaborate Common Gateway Protocol, or CGP (2598), then the web sockets HTTP protocol (for HTML5-based Receiver only), and finally by TLS (443) before transmission over TCP/IP. Here's a picture of the network stack:

### Citrix ICA/CGP/HTML5/TLS/TCP stack in XenApp and XenDesktop 7.9

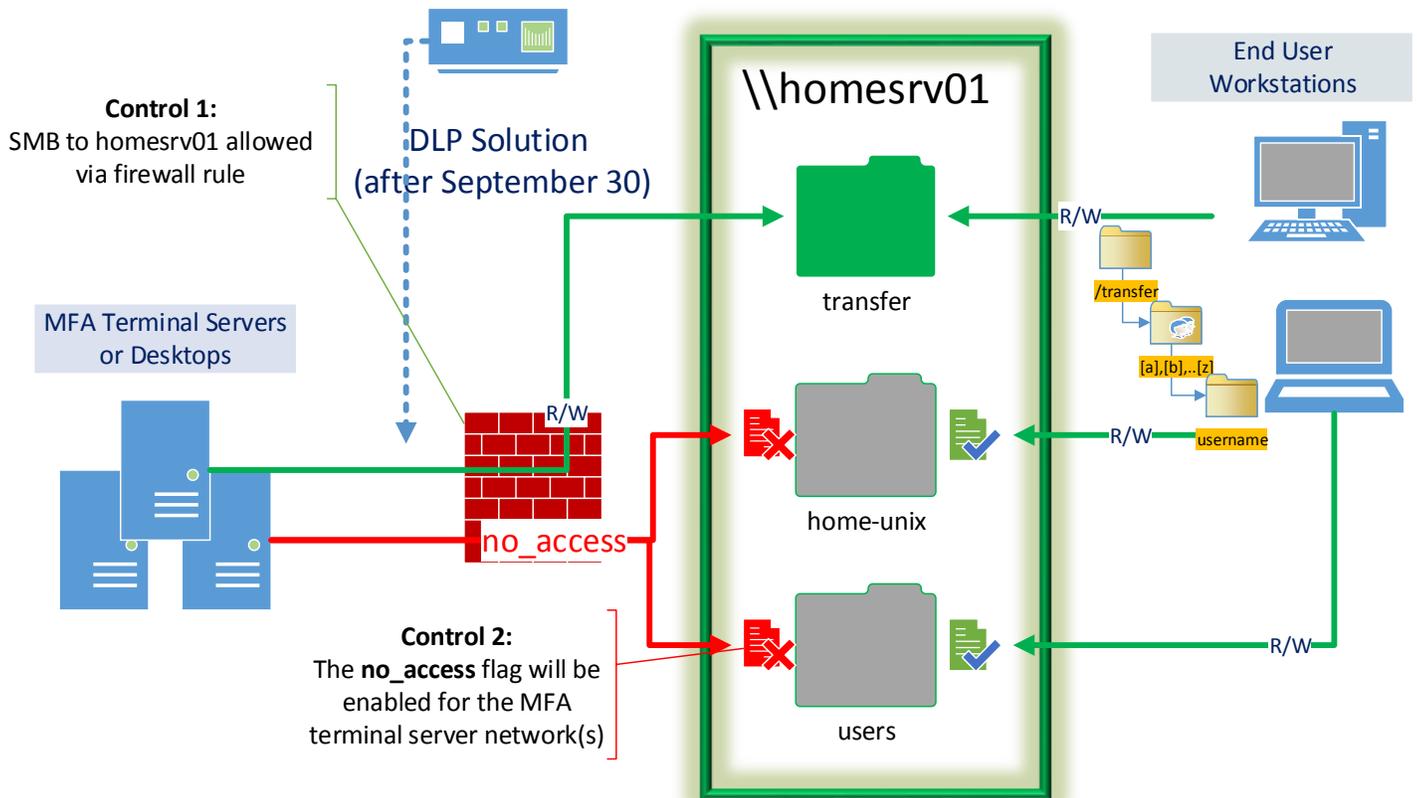


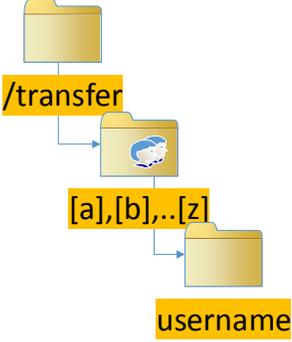
## File Transfer – MFA Standard User Environment

Although it is expected that business sensitive and PII data should be contained within the MFA Standard User Environment, less sensitive data needs to be shared outside of the environment. In order to do this in a controlled manner, a transfer folder has been setup on homersrv01 (NAS filer). Each MFA user will have their own subfolder to perform these transfers.

In order to discourage users from permanently storing files in their transfer area, user quotas of ~50-100 MB have been configured. In addition, a cleanup script will purge files that haven't been modified after 5 days. These settings should encourage users to limit their activities to file transfers or other short-lived activities.

After September 30, 2016, either a network-based or agent-based DLP solution will be implemented to protect against data leakage. The implementation should be transparent to end users.



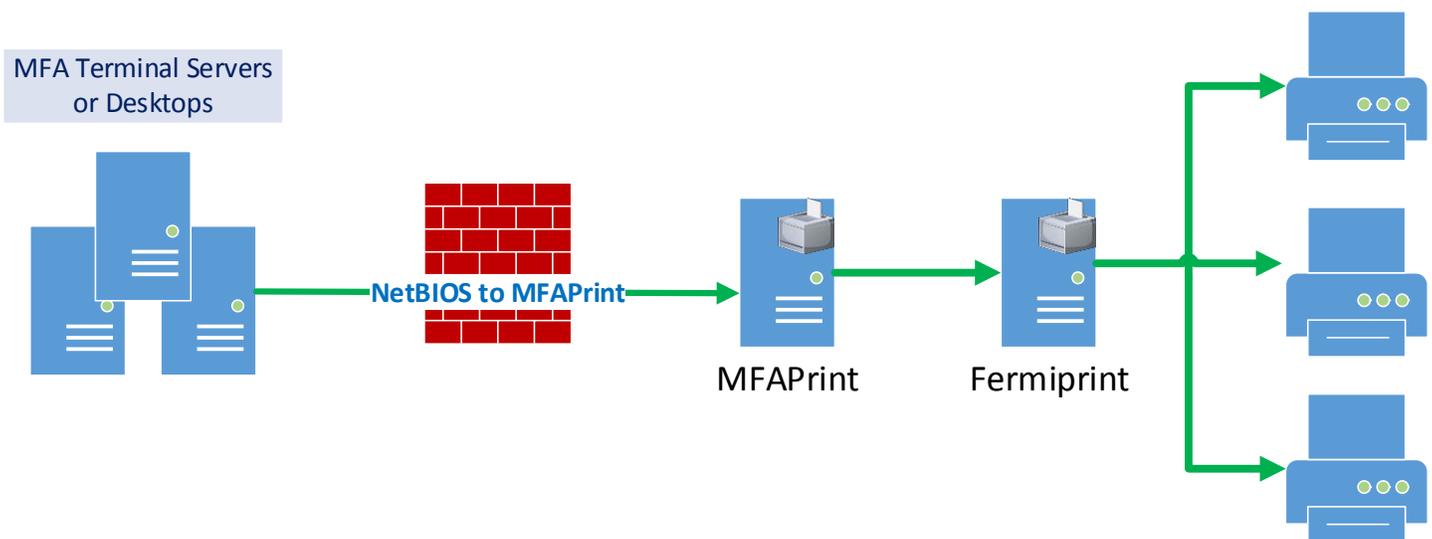
File Transfer Service Folder Structure	Controls
	<ul style="list-style-type: none"> <li>➤ Data retention = 5 days</li> <li>➤ Default Quota = ~50-100 MB</li> <li>➤ User Permissions = R/W only for user assigned to folder</li> <li>➤ SMB to homesrv01 from MFA environment restricted by network firewall</li> <li>➤ SMB to homesrv01 from other campus networks is allowed</li> <li>➤ No other shares on homesrv01 will be accessible from within the MFA environment (enforced by NAS controls → no_access flag)</li> <li>➤ DLP solution will be implemented after the September 30<sup>th</sup> deadline</li> </ul>

### Printing in the MFA Standard User Environment

In order to control which printers a standard user can submit a job to, a dedicated print server (mfaprint.fnal.gov) has been configured. This includes the SecurePrint queue and a number of queues associated with printers found in either locked offices or with sufficient physical security to accept sensitive data. An approval process is being developed to handle requests to add new printers to the MFA Standard User Environment.

Print queues on the MFA Print Server are mapped to queues on Fermiprint Server using LDP (tcp/646), so essentially print jobs from the approved queues are forwarded to Fermiprint for processing. Please see the following diagram for an overview of the architecture.

### MFA Print Server Architecture



### Summary of Controls – MFA Standard User Printing:

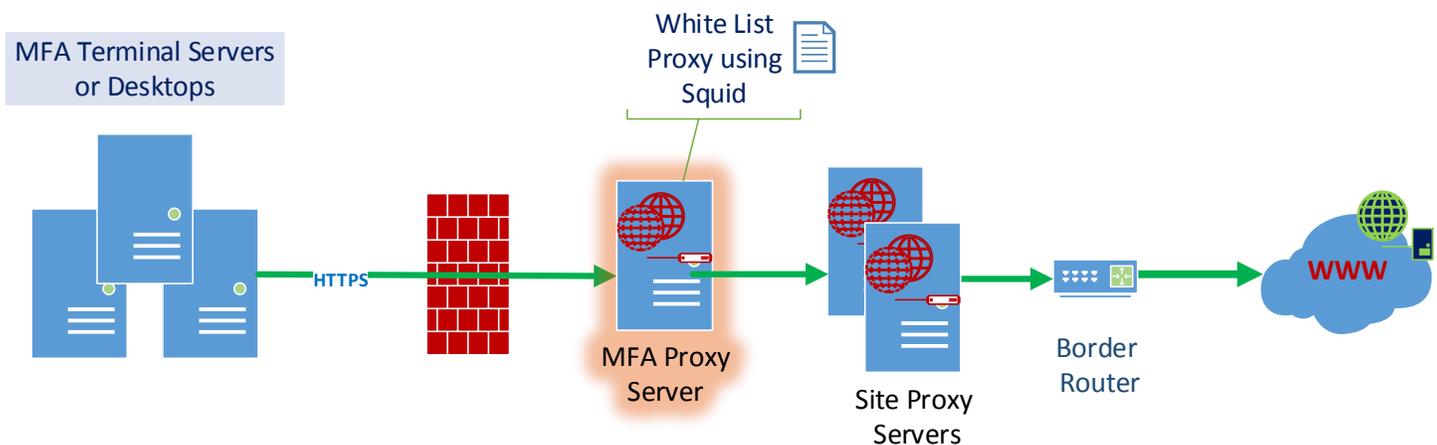
1. MFA terminal servers or desktops for standard users can only install printers published from mfaprint.fnal.gov. Network firewall rules prevent users from directly accessing resources on Fermilab or any other print servers.
2. The MFA print server (mfaprint.fnal.gov) has only a limited set of approved print queues defined, including SecurePrint.
3. An approval process will handle requests to add or remove printers from the MFA Print Server.

### External Web traffic in the MFA Environment (Standard and Privileged users)

A number of standard users have the need send and receive data to and from DOE, IRS, various tax sites, benefits providers, and other organizations we do business with regularly. In order to limit traffic to a small list of approved sites, a squid proxy server with a white list configuration has been deployed. The MFA Proxy is running a standard build of RHEL 7.

Local http/https traffic will bypass the proxy, requiring ports to be opened through the network firewall instead. When a new external site needs to be configured, the ticket will be routed through the Computer Security Operations Group for approval just as network firewall rule requests are approved.

### MFA Proxy for External Web Traffic

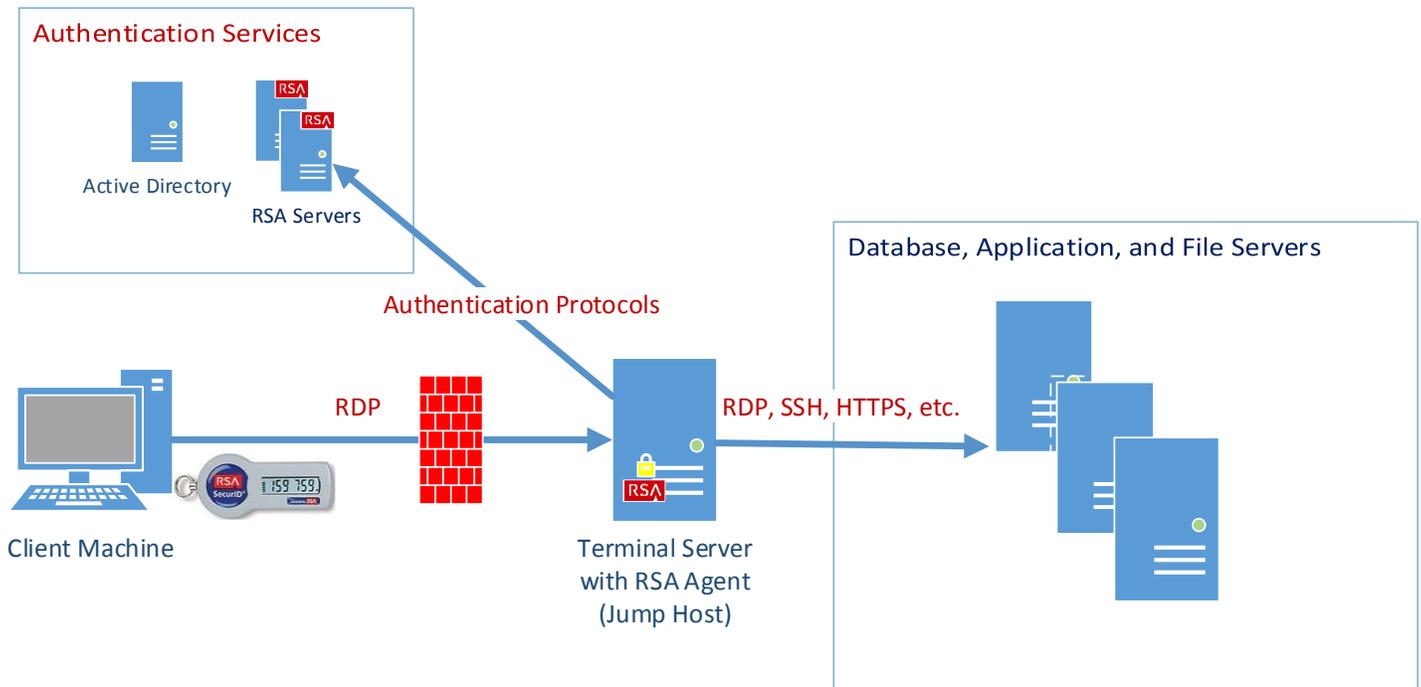


## RSA SecurID Direct

In this architecture the end user will connect to a terminal server with the RSA Agent software installed and configured to prompt for a username and password as well as an RSA Passcode (user PIN + token code).

In the example diagram below, you see a Windows Terminal Server used as a jump host to access various types of resource servers. The resource servers do not have the RSA agent software installed, but likely require direct sessions to come from a host that does require multi-factor authentication.

## RSA SecurID Direct



### RSA User Configuration

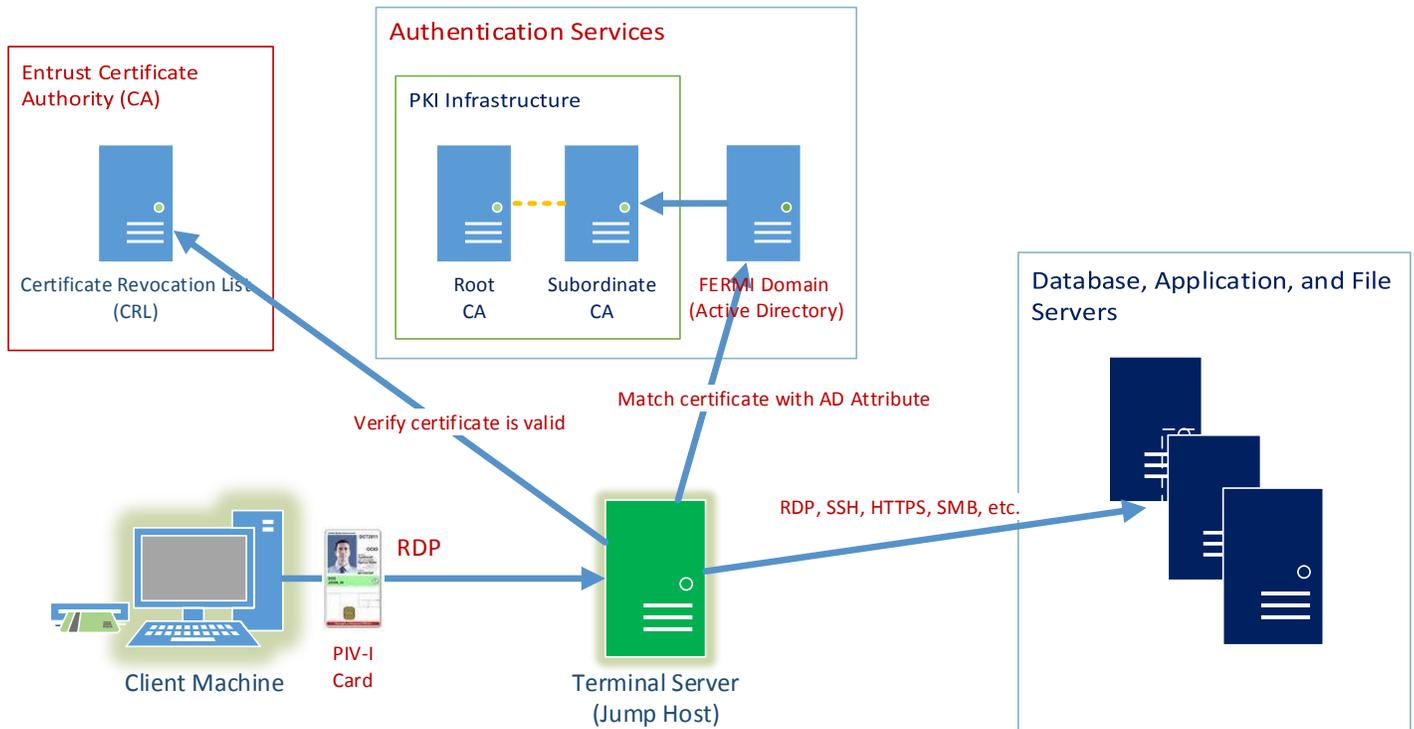
1. User submits a ticket in SNOW to obtain either a hardware or software token.
2. Configure a PIN to activate the token.
3. Answer security questions that aid in identity verification when recovering from a forgotten PIN.

### PIV-I Direct

In this architecture the end user will insert a PIV-I card into a smart card reader, either internal to or directly attached to their machine. Depending on the operating system, additional software or configuration might be needed. In a typical scenario, the user will connect to a terminal server or similar host configured to accept smart card authentication.

In the example diagram below, you see a Windows Terminal Server used as a jump host to access various types of resource servers. The resource servers might not accept smart card authentication, but they are configured to limit direct connections with nodes that do require smart card authentication.

## PIV-I Direct



### PIV-I User Configuration

1. User must go through an enrollment process to obtain a PIV-I card through the USAccess system (requires multiple forms of ID, photo, and fingerprints).
2. PIV-I card issuance requires fingerprint verification before a user will receive their card.
3. PIV-I cardholder must export public key and submit a ticket to configure their domain user account attributes to match certain values presented by the card; In the FERMI Domain, the **altSecurityIdentities** and **userPrincipalName** attributes are modified.

### PIV-I Domain Configuration Overview

1. Entrust certificate was installed into the domain for all non-domain controller systems, then propagated by GPO.
2. Group policies are used to enforce smart card authentication for jump hosts accessing systems or applications used for privileged functions.
3. Self-generated domain certs installed on each DC; a unique certificate for each server generated by Fermilab CA servers.

4. Windows domain controllers check in every 10 days with the subordinate CA to make sure the domain certificate has not been revoked. Our certificate for the domain is set to expire after 10 years.
5. When a user on a client machine presents a certificate at logon, a Certificate Revocation List (CRL) is checked to make sure the certificate has not been revoked.

## Risk Identification & Methodology

- A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability.
- A vulnerability is a weakness that can be accidentally triggered or intentionally exploited.
- A threat-source does not present a risk when there is no vulnerability that can be exercised.

### Likelihood Determination, Impact Analysis, and Risk Level

The likelihood that each vulnerability will be exploited and the impact of a successful exploit is indicated by the pair of rankings associated with each vulnerability below. Following each vulnerability is the risk level obtained by using the following matrix:

		Impact		
		Low	Medium	High
Threat Likelihood	Low	Low	Low	Low
	Medium	Low	Medium	Medium
	High	Low	Medium	High

### Threat Source Identification

There are no threat sources which have not been identified in the Risk Assessment for the General Computing Enclave.

### Motivation and Threat Actions

There are no motivations and threat actions which have not been identified in the Risk Assessment for the General Computing Enclave.

### Residual Risk Definition

Residual risks are divided into categories based on expected frequency of occurrence after full implementation of all security controls. We consider an occurrence rate to be:

- LOW** if it is expected to happen <10 times per year
- VERY LOW** if it is expected to happen <1 time per year
- EXTREMELY LOW** if it is expected to happen <1 time per five years

## Identified Threats, Vulnerabilities, Risks, Mitigations, and Residual Risks

### Threats: Unauthorized Access

**Threat:** Unauthorized Access – User credentials with Citrix

**Vulnerability:** Exposure of user credentials through network access.

**Risk:** (EXTREMELY LOW) The user's account password can be sniffed with a tool.

**Mitigation:** All users access Citrix XenDesktop either via the local area network or the Internet via Citrix NetScaler are required to authenticate with centrally-managed Active Directory accounts and a Fermilab issued RSA token or PIV-I card. The sessions are protected by Secure Socket Layer version 2 (SSL v2) or Transport Layer Security (TLS). This secures network traffic from passive eavesdropping, active tampering, or message forgery. User authentication occurs with LDAPS to centralized Active Directory servers. Credentials are passed to Citrix application resources for Single Sign On over Secure ICA.

**Residual Risk:** (EXTREMELY LOW)

**Threat:** Unauthorized Access – User credentials

**Vulnerability:** Exposure of user credentials through cache.

**Risk:** (EXTREMELY LOW) The user's account password can be obtained from cache on the Citrix NetScaler appliance.

**Mitigation:** Interactive access to NetScaler management functions, i.e. web GUI, SSH, FTP, TELNET, is not allowed on any network interface not designated as a management interface. NetScaler management functions are only presented on a single interface located on a restricted subnet not routable off site and is not generally accessible onsite. Details regarding how credentials by the appliance are cached are not provided by the vendor.

**Residual Risk:** (EXTREMELY LOW)

**Threat:** Unauthorized Access – Password guessing

**Vulnerability:** Brute force password guessing using the User Interface (UI).

**Risk:** (EXTREMELY LOW) Attack is initiated to the web site (Citrix) to "guess" the password for an account. In the case of standard users, this could mean loss of FERMI credentials (non-admin account). For a privileged user, this could mean the loss of SERVICES credentials (non-admin).

**Mitigation:** Users are forced to use complex passwords. Users are forced to reset their passwords per the Fermilab password policy, and are not allowed to re-use a previous password. After several failed password attempts, the account will be temporarily locked out. Multifactor authentication is required for all sessions, so a compromised username and password alone will not allow an attacker to gain access to resources. Standard users are setup with RSA SecurID. Privileged users are required to use PIV-I cards.

**Residual Risk:** (EXTREMELY LOW)

**Threat:** Unauthorized Access – Internet Search

**Vulnerability:** Data gathered from “googling”.

**Risk:** (EXTREMELY LOW) Outside user searching the Internet has ability to view potentially sensitive data.

**Mitigation:** Data stored on resource servers requires authenticated access to view. In this environment, multifactor authentication is required. Citrix XenDesktop and Citrix NetScaler systems do not store any sensitive data, but instead provide access to resources that do store sensitive data and are designated for that role. Web spiders, such as Google, only view public, non-authenticated data.

**Residual Risk:** (EXTREMELY LOW) Social engineering could be performed with information gathered from “googling”. This is mitigated through the provisioning of cards, tokens, and domain credentials using established procedures.

**Threat:** Unauthorized Access – Social Engineering

**Vulnerability:** Social engineering attempt to obtain password.

**Risk:** (VERY LOW) Unauthorized person obtains password by posing as insider (e.g., IT department)

**Mitigation:** The informed user community is trained not to reveal passwords. Fermilab policy forbids writing down passwords. Furthermore, access to resources requires MFA (includes RSA Token or PIV-I card), so a username and password is not the only credential required to gain access to an interactive session or data.

**Residual Risk:** (EXTREMELY LOW) No residual risks identified.

**Threat:** Unauthorized Access – Sensitive data leakage

**Vulnerability:** A user may unintentionally or purposely move sensitive data, including protected PII, outside of the MA boundary to systems not designated to store such data. An example destination would be a user’s desktop or a general purpose file share where fewer controls might be in place to protect sensitive information.

**Risk:** (EXTREMELY LOW) Sensitive data could be exposed to unauthorized individuals causing an embarrassment to the laboratory. The exposed data could be used maliciously.

**Mitigation:** The following controls have been configured to mitigate sensitive data leakage:

1. Network drives mapped through the Citrix client are configured read-only, so data cannot be written back out through the client drive mappings.

2. With the exception of a dedicated user transfer share, only shares that exist inside of the Information Systems Major Application Boundary can be mapped by the MFA terminal servers or desktops presented through Citrix or accessed directly.
3. Web traffic is limited to a small number of approved sites Fermilab does business with. This is controlled by a Squid proxy server configured with a white list of domains and URL's.
4. Printing is limited to the SecurePrint queue and printers that have been approved for secure printing, such as those in locked offices or with sufficient physical controls to limit unauthorized individuals from accessing printouts containing sensitive information.
5. Remote access to the Citrix MFA environment is restricted to users that reside in an Active Directory Group in the Fermi Domain. This group is audited frequently to ensure only members that have access to resources in scope are allowed to login and access shares.

**Residual Risk:** (EXTREMELY LOW) No residual risks identified.

## Threats: Unauthorized Physical Access

**Threat:** Unauthorized Physical Access

**Vulnerability:** Physical access to Citrix Software Application servers or NetScaler appliances

**Risk:** (EXTREMELY LOW) Malicious user obtains the physical media that stores the data.

**Mitigation:** All computing assets used for delivery of Citrix XenDesktop and Citrix NetScaler for systems requiring multifactor authentication (MFA) are housed in the Feynman Computing Center datacenters, which are secured from unauthorized access. All business processes and application access occurs on the VDA's (terminal servers or desktops), so there are no interactive user logons allowed to the Citrix Infrastructure except for those who manage the environment from administrative consoles. There is no additional risk of unauthorized physical access that is not already identified and accepted for these datacenters.

**Residual Risk:** (EXTREMELY LOW) When the Citrix systems are excessed or require media to be replaced, a malicious user could obtain the media once outside of the datacenter. The Citrix servers do not actually store user or application data related to the resource servers.

## Threats: Malicious Content

**Threat:** Malicious Content

**Vulnerability:** Upload of executables or code

**Risk:** (VERY LOW) A user may unintentionally or purposely upload malicious code to one of the financial systems terminal server or data storage location. Users that download the code or run it inside the environment may be infecting their systems or causing other damage.

**Mitigation:** Fermilab policy requires anti-virus protection for network access. All Citrix XenDesktop, standard user terminal servers, administrative terminal servers and virtual desktops in the environment will have modern anti-virus

scanning software installed which is centrally managed, monitored and updated regularly. Many systems will not allow access to the RDP clipboard where copy/paste functions can be performed between systems.

**Residual Risk: (VERY LOW)** A user might still be able to upload malicious content through folders setup specifically to allow users and administrators to transfer patches and other data into the environment. These types of folders will be setup with file auditing enabled and "deny" in the "traverse folder/execute file" box for a folder used to transfer data.

## Threats: Environmental Threats

**Threat:** Environmental Threat

**Vulnerability:** Service outage at local internet service provider

**Risk: (LOW)** Lack of access to information and ability to enter information into the system.

**Mitigation:** Fermilab maintains redundant network paths to provide resilient connectivity.

**Residual Risk: (EXTREMELY LOW)** Connectivity problems between Fermilab and remote users could cause service interruptions.

**Threat:** Environment or Application Jailbreaking

**Vulnerability:** A user can 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.

**Risk: (LOW)** Application jailbreaking can provide an attacker with an initial foothold into the environment and domain and leverage this initial foothold to gain access to the internal network, escalate privileges, move laterally, and compromise the entire enterprise environment.

**Mitigation:** The following controls have been configured:

1. Although command shell access from within an application is not disabled, users access the environment with non-privileged accounts. This requires the user to elevate their privileges
2. A Squid web proxy which sits outside of the Citrix environment limits access to external resources by using a whitelist. All entries are evaluated and approved before they are added to the list.
3. MFA terminal servers have restricted access to resources on the network. For example, only a few file servers are allowed to be accessed R/W, a limited set of database and application servers are accessible over the network, and other traffic is limited to key network services such as DNS, authentication, NTP, Antivirus, Patching, etc.
4. GPO's restrict the ability to change key settings in Internet Explorer.
5. Unnecessary services have been disabled both on the MFA terminal servers and Citrix component servers.
6. Login scripts running from non-MFA servers have been disabled.

**Residual Risk: (EXTREMELY LOW)** A user can still use connect to another server, such as a database or application server, then elevate their privileges or breakout of the environment. This risk is further mitigated by the controls put into place

within the Information Systems Major Application Boundary. All critical resource servers in the MA Boundary are behind a network firewall and have limited access to other systems.