# Table of Contents

About the Validated Design Guide .......................................................... 3
Introduction .............................................................................................. 4
Audience ..................................................................................................... 4
Business Case ............................................................................................ 4
  Mobility ................................................................................................. 5
  Security ................................................................................................. 6
  Management ............................................................................................ 6
User Profiles ............................................................................................... 6
Federal Secure Desktop Architecture Overview ........................................ 7
Solution Validation ..................................................................................... 9
  Lab Equipment List ................................................................................ 9
  Solution Components ............................................................................ 9
  Optional Components ............................................................................ 9
Key Components of the Architecture ....................................................... 10
  Core Components ................................................................................ 10
    vSphere and vCenter .......................................................................... 10
    VMware Horizon View ....................................................................... 10
    VMware vCloud Networking and Security and vShield Endpoint ....... 10
    CAC Cards ....................................................................................... 10
    HBSS ............................................................................................... 10
    Zero Clients ..................................................................................... 10
    802.1X Network Access Control ....................................................... 11
Additional Components ........................................................................... 11
  Management .......................................................................................... 11
  Compliance ............................................................................................ 11
  Persona and User-Installed Apps. .......................................................... 11
Architecture Overview .............................................................................. 12
  Server Architecture ............................................................................... 12
  Storage .................................................................................................. 12
  Networking ............................................................................................ 13
  Security ................................................................................................ 13
    CAC Card Support ............................................................................ 13
    McAfee HBSS .................................................................................. 15
    802.1X Authentication ...................................................................... 15
    vCloud Networking and Security and vShield Endpoint .................. 15
Management ............................................................................................ 16
  Endpoint Management ......................................................................... 16
  Persona Management .......................................................................... 17
Key Deployment Considerations ............................................................. 18
  Initial Setup .......................................................................................... 18
  CAC Certificate Setup ......................................................................... 18
  Deploying the Base Image and Desktop Pools .................................... 19
  McAfee HBSS ..................................................................................... 20
  Configuring Zero Clients and 802.1X Authentication ......................... 20
  User Connection Flow Sequence ......................................................... 21
Summary .................................................................................................. 21
About the Authors ..................................................................................... 22
About the Validated Design Guide

VMware® Validated Design Guides provide an overview of a solution architecture and implementation. The validated designs and solutions have been created through architectural design development and lab testing. The guide is an introduction to proof of concepts, emerging new technology and architectures, and enhancement of customer use cases.

The Validated Design Guides:
- Incorporate generally available products into the design
- Employ repeatable processes for the deployment, operation, and management of components within the solution

Validated Designs are tested for a specific use case or architectural practice on a limited scale and duration. These guides ensure the viability of theoretical designs or concepts in real-world practices.

The Validated Design Guides include:
- Use cases catered to the design
- Products validated as part of design testing
- Software used for each component of the design
- Configurations used to support the design test cases
- A list of design limitations and issues discovered during testing
Introduction

This Validated Design Guide is an overview of the VMware Horizon View™ Federal Secure Desktop™ solution, which is based on the VMware Horizon View Mobile Secure Workplace™ solution. The architecture uses products from VMware and its ecosystem of partners to build a comprehensive solution that satisfies the specific requirements of use cases within the federal vertical such as mobility, bring your own device (BYOD), security, and compliance.

This document provides an overview of the logical solution architecture and results of the tested configuration. The solution is not exclusive to the products tested within the architecture. Consult your VMware representative for more information about how to modify the architecture with your preferred vendors.

Audience

This document is intended to assist solution architects, sales engineers, field consultants, advanced services specialists, and customers who will configure and deploy a secure desktop solution for federal agencies or organizations.

Business Case

Recent natural events, including the North American blizzard of 2010 and Hurricane Sandy, caused heavy damage to the federal infrastructure and closed regional federal offices for many work days. While such disasters cost the government millions of dollars, they can serve as the ideal use case to support the recently enacted Telework Enhancement Act of 2010, H.R. 1722.

Nearly every federal IT organization today is working to embrace mobile computing for a number of reasons, including:

• Lowering its carbon footprint and energy costs by reducing employee commutes
• Improving employee satisfaction and work/life balance, especially for workers who maximize use of mobile devices and who expect more flexible mobile work arrangements
• Striving for an always-on, agile e-government infrastructure that gives employees immediate access to information
• Supporting Continuity of Operations (COOP) in the event of emergencies by helping employees do their jobs effectively from home or remote locations

The Telework Enhancement Act and initiatives around disaster recovery and COOP pose both an opportunity and a challenge for federal IT leaders. Users expect and require access to applications and data on a variety of devices to maximize productivity; but IT is pressured to secure information, control critical processes and data, and ensure that all compliance requirements are met.
What Is Federal Secure Desktop?

The VMware Horizon View Federal Secure Desktop solution is built on the VMware validated Mobile Secure Workplace solution. It provides secure access for end users to desktops that meet various federal compliance requirements. The solution design supports end-user mobility, streamlines application updates, enhances data security, and delivers the highest-fidelity user experience.

Figure 1: Mobile Secure Workplace Solution

This solution enables the audience to address the following three key requirements addressed by the VMware Mobile Secure Workplace solution:

- Mobility
- Security
- Management

Mobility

The Federal Secure Desktop solution, built on VMware Horizon View, places desktops in the datacenter. The solution provides users access to their remotely displayed desktop through any device via the FIPS 140-2 certified PCoIP protocol. Desktops can be accessed from zero clients, workstations, thin clients, or mobile devices. With VMware Horizon View Persona Management, Federal Secure Desktop provides true session persistence across devices and sessions. The variety of endpoints enables true BYOD support, and session persistence enables session mobility across devices.
Security

With support for Common Access Cards (CAC) built into and validated in the design, the Federal Secure Desktop solution supports and extends an existing data and application security infrastructure. In addition to providing the right level of access to the right resources, the solution also simplifies patch management and update management for all desktops. IT administrators can update and patch desktops in the datacenter to the latest version, ensuring that no vulnerabilities exist in the environment due to unpatched or orphaned systems. Data resides in the datacenter and is protected by VMware vCloud® Networking and Security™ and VMware vShield Endpoint™, which provide superior security to the environment. The design uses PCoIP-based zero clients from Teradici, which provide the utmost endpoint security. Teradici also incorporates 802.1X authentication to allow only authorized devices to connect to the network.

Management

One of the key challenges facing organizations today is to obtain an overview of their desktop environment and manage the environment, desktops, access policies, and service levels. The Federal Secure Desktop solution, with optionally integrated VMware vCenter™ Operations Manager™ for Horizon View, provides an integrated dashboard with intelligent data on all desktop-related events. This helps IT administrators provide the right amount of intervention and guidance when virtual infrastructure performance falls below an expected range of behavior. The solution can also include VMware vCenter Configuration Manager™ (vCM) for importing suggested configurations and to meet regulatory compliance.

User Profiles

The Federal Secure Desktop solution is applicable to all use cases in federal agencies which require mobility, a high level of security, and always-on access to desktops. These use cases include but are not limited to teleworkers and first responders. The workload profiles include a spectrum of users: office-based and home office-based workers, remote-office knowledge workers, power users, and mobile workers.

The validated design in this document supports the unique requirements of these user profiles and helps the IT team manage the environment securely.
Federal Secure Desktop Architecture Overview

The Federal Secure Desktop solution is built on the VMware validated Mobile Secure Workplace solution. The following diagram shows the logical topology for the Federal Secure Desktop solution:

The architecture consists of:

- VMware Horizon View infrastructure
- Access infrastructure with CAC card setup, 802.X, and zero clients

The VMware Horizon View infrastructure consists of two virtual machine clusters for scalability purposes, a management cluster and a virtual desktop cluster. The management cluster includes all the management components required for VMware Horizon View base architecture along with VMware vCenter Operations Manager, vCloud Networking and Security, and vShield Endpoint.
The virtual desktop cluster is dedicated to hosting stateless virtual desktops accessed by end users. The environments are segregated to effectively utilize underlying hardware resources, and support storage layer tiering where required.

The management architecture can host multiple connection servers, load balanced to provide redundancy and availability. Users can access the closest desktop immediately by accessing the network of load balancers with a single namespace. Remote users can access the environment through Horizon View Security Servers deployed in the demilitarized zone (DMZ). Usage of Horizon View security servers ensures secure access to remote desktops via PCoIP, while maintaining an optimal user experience.

The CAC infrastructure is set up in a standard format as it would be in a physical environment. The certifications are provided by DISA, and the specifications can be found in the Common Access Card (CAC) User Guide.

Certifications are provided via a CAC on NIPRNet (Non-classified Internet Protocol Router Network). This emulates the standard access method that is used by federal agencies. The United States Department of Defense (DoD) integration is achieved by allowing the Certificate Authorities (CAs) to use the relevant fields in the certificate chain, with the DISA CA as the trusted source.

To secure desktops and meet federal requirements, HBSS combined with McAfee’s ePolicy Orchestrator (ePO) and other host-based intrusion prevention systems (HIPSs) were added to the environment.

To provide enhanced security, 802.1X authentication was added to the solution to lock down the devices that can connect to the network. In conjunction with zero clients as the access devices, 802.1X authentication locks down the environment securely while giving end users mobility and a superior user experience.

The architecture is scalable and is based on the standard reference architectures published by VMware.
Solution Validation

For functional testing and validation, the solution was implemented with 100 desktops and deployed on the hardware in Table 1. The solution implemented in the lab was designed to scale to many thousands of desktops according to the sizing guidelines provided in VMware published reference architectures. The architecture was built in pods or building blocks so the solution could be scaled easily.

Lab Equipment List

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>5 – 1U servers with 2 Intel Xeon E7 8837 2.67GHz processors, 96GB RAM</td>
</tr>
<tr>
<td></td>
<td>1 – 2U servers with 2 Intel Xeon E7 8837 2.67GHz processors, 128GB RAM</td>
</tr>
<tr>
<td>Hard drives</td>
<td>8 – 300GB Intel 320 SSD Drives</td>
</tr>
<tr>
<td></td>
<td>8 – 600GB 7200RPM HDD</td>
</tr>
<tr>
<td>Attached storage</td>
<td>iSCSI storage array, Raw Disk Capacity: 8TB, Raw Flash Cache 160GB, 24GB RAM, 4 – 1GbE network ports</td>
</tr>
<tr>
<td>Networking</td>
<td>Layer 2 – 10/100/1000 24-port switch</td>
</tr>
</tbody>
</table>

Table 1: Lab Equipment

Solution Components

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere®</td>
<td>5.0.1</td>
</tr>
<tr>
<td>vSphere with VMware vCenter</td>
<td>5.0</td>
</tr>
<tr>
<td>VMware Horizon View</td>
<td>5.1</td>
</tr>
<tr>
<td>VMware Horizon View Composer</td>
<td>3.0</td>
</tr>
<tr>
<td>vCloud Networking and Security</td>
<td>5.1.2a</td>
</tr>
<tr>
<td>vShield Endpoint</td>
<td>5.0.1</td>
</tr>
<tr>
<td>CAC</td>
<td>CAC infrastructure with federal NIPR and SIPR cards</td>
</tr>
<tr>
<td>Desktop antivirus</td>
<td>McAfee ePO AV stack</td>
</tr>
<tr>
<td>HBSS</td>
<td>McAfee HBSS</td>
</tr>
<tr>
<td>Clients</td>
<td>Teradici zero clients</td>
</tr>
</tbody>
</table>

Table 2: Solution Components

Optional Components

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Operations Manager for Horizon View</td>
<td>1.0</td>
</tr>
<tr>
<td>Load balancer</td>
<td>F5 BIG-IP LTM, GTM, and APM</td>
</tr>
</tbody>
</table>

Table 3: Optional Components
Key Components of the Architecture

Though the solution architecture is vendor agnostic, the following components are part of the validated design:

Core Components

vSphere and vCenter
The solution is built on top of vSphere, the industry-leading virtualization platform. There are many benefits to using vSphere, and more information on the platform can be found on the VMware Web site.

VMware Horizon View
The central component of the solution architecture is VMware Horizon View, the industry-leading virtual desktop infrastructure (VDI) product.

VMware vCloud Networking and Security and vShield Endpoint
VMware vCloud Networking and Security is the leading software-defined networking and security solution that enhances operational efficiency, unlocks agility, and enables extensibility to rapidly respond to business needs. It provides a broad range of services in a single solution, including virtual firewall, VPN, load balancing and VXLAN extended networks.

VMware vShield Endpoint strengthens security in VMware vSphere and Horizon View environments while improving performance for endpoint protection by orders of magnitude, offloading antivirus and antimalware agent processing to a dedicated secure virtual appliance delivered by VMware partners.

Visit the VMware Web site for more information on vCloud Networking and Security and vShield Endpoint.

CAC Cards
The CAC, a smart card about the size of a credit card, is the standard identification for active-duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel in secure Federal environments. It is also the principal card used to enable physical access to buildings and controlled spaces, and provides access to defense computer networks and systems. More information on CAC cards can be found at the DoD ID Card Reference Center.

The DoD has adopted and used the Public Key Infrastructure (PKI)-based CAC for years as their primary authentication method into the NIPRNet. NIPRNet is composed of Internet Protocol routers owned by the DoD.

Several agencies have also migrated to SIPR (Secure Internet Protocol Router) hardware tokens as their primary authentication method for accessing the SIPR network. Other agencies are also moving toward a PKI-based Personal Identity Verification (PIV) card for authentication into the federal network.

HBSS
HBSS is the official name given to the DoD commercial-off-the-shelf (COTS) suite of software applications used within the DoD to monitor, detect, and counter attacks against computer networks and systems. For this validation, we used McAfee HBSS products to meet the compliance requirements. HBSS is the McAfee ePO suite with antivirus HIPS.

McAfee HBSS is a requirement for most datacenters, and is required by the Department of the Navy. HBSS is required for managing every endpoint general-purpose operating system (servers and desktops). The major requirement for any 802.1X deployment is the use of FIPS 140-2 validated crypto modules to protect the data.

Zero Clients
PCoIP zero clients are ultra-secure, easy-to-manage devices that offer the richest user experience in a VMware Horizon View environment. PCoIP zero clients are based on the TERA chipset by Teradici and are available in a variety of form factors from a number of trusted OEMs. Further information is available at www.teradici.com.
802.1X Network Access Control
PCoIP zero clients support 802.1X network device authentication using EAP-TLS certificates. Under this method, all network endpoint devices must be authenticated before they are granted access to the network. This is a typical method of device authentication for high-security environments, providing an additional layer of security beyond username and password credentials.

The 802.1X authentication protocol has grown in usage. IEEE 802.1X is an IEEE standard for port-based Network Access Control (PNAC) that provides an authentication mechanism for devices trying to attach to a LAN or WLAN.

The DoD has added a requirement that all network ports or on-ramps be protected. Applications, servers and data are normally protected; however, most network ports are left open. Typically, users access a network by simply plugging into a port, and a network address is allocated for the connection. Computers without proper access to data and servers are open to attacks launched from the network. Network port protection lockdown restricts anonymous access and prevents these “attacks.”

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (thin client or zero client) that tries to attach to the LAN or WLAN. The term ‘supplicant’ is also used interchangeably to refer to the software running on the client device that provides credentials to the authenticator. The authenticator is a network device such as an Ethernet switch or wireless access point. The authentication server is typically a host running software supporting the RADIUS and EAP protocols.\(^1\)

In this validation, routing was done at the switch (authenticator). We created a DMZ VLAN and configured 802.1X on the switch to speak to our authentication server (Microsoft Network Policy Server serving as a RADIUS server). Additionally, vCloud Networking and Security was used for portgroup protection on intra-virtual-machine traffic.

Additional Components
Management
One of the biggest challenges faced by an IT group is on-demand management of the entire environment and the ability to identify and plan the infrastructure. VMware vCenter Operations Manager for Horizon View provides the management infrastructure required for the environment.

Compliance
One of the key requirements of many vertical industries is the ability to manage compliance with various industry regulations. VMware Horizon View is compliant with FIPS 140-2.

Teradici Tera2 Zero Client supports AES-256 and NSA Suite B crypto security protocols.

Persona and User-Installed Apps
Many use cases defined in the solution have a requirement to persist user information across sessions. But the biggest cost savings both in terms of CapEx and OpEx can be achieved by using stateless desktops. To effectively meet both goals, VMware Horizon View has a feature called Persona Management to maintain user data and profile persistence across stateless sessions. In addition to profile persistence, some use cases require support for user-installed applications. This can be achieved by implementing some of our partner products.

---

Architecture Overview

Server Architecture

In the Federal Secure Desktop solution design, it is important to separate the management and desktop components as two discrete blocks of infrastructure. In this design, we created a management cluster and a VMware Horizon View cluster, in order to establish a subscription- or consumption-based model. This methodology is important for the solution to scale easily, as another Horizon View pod can be plugged into the architecture as required, and services can be extended to accommodate the expansion.

VMware vCloud Networking and Security and vShield Endpoint were configured to provide the security architecture, specifically around virtual desktop communication and application protocol flow in and out of the management, services, and desktop pool security zones.

In order to satisfy strict federal desktop requirements, the architecture also included integration of CAC and HBSS components.

The infrastructure components required for the environment are configured in the management cluster, and View Services is configured in the View Services cluster.

The management cluster includes two Active Directory virtual machines for redundancy, a vCenter server with a SQL Server virtual machine and a Certificate Authority with CAC enabled, along with the McAfee HBSS components (ePO server, AV server).

The View Services cluster includes the Horizon View Connection Server, vCenter Compliance Manager, vShield Security Manager, and Horizon View Security Servers. These form the core and optional services required for the environment.

Separate resource pools were added to simulate the various user profiles accessing the environment. The vCloud Network and Security Edge gateway component was configured to ensure that these resource pools are segregated and cannot talk to each other.

Storage

Following the Mobile Secure Workplace base design, in the Federal Secure Desktop design the typical storage configuration was logically segregated into two clusters: management and VDI. The management cluster in turn is segregated into general, SQL, vCloud Networking and Security, and third-party (if necessary) segments. The VDI cluster is segregated into virtual desktops and user and corporate data segments. This logical segregation is in alignment with the workloads in these datastores.

The general datastore cluster in the management segment consists of Active Directory, DNS, Horizon View Connection Server, Horizon View Security Servers, and McAfee HBSS components. All general infrastructure components are located in this segment. Storage best practices were followed when the datastores were created (e.g., two instances of AD, and Horizon View Connection Server and Horizon View Security Server are located in two separate datastores for failover protection).

The SQL logical cluster contains the datastores for all SQL databases used for Composer and vCenter, and the vCloud Networking and Security cluster contains the datastores for all vCloud Networking and Security virtual machines. In addition to the above, a separate datastore cluster can be added if necessary to host all third-party software that needs to be included in the design.

The VDI logical cluster contains datastores for virtual desktops and user and corporate data.

Typically, the management logical cluster can be Fiber Channel or iSCSI, and the virtual desktop datastores are in SSD for higher performance. The user data and corporate data are located in NFS datastores.
In this lab design, the management logical cluster (general, SQL, vCloud Networking and Security, and third-party virtual machine datastores) is located in iSCSI datastores. The VDI cluster (virtual desktops) is located in SSD and the user data is located in NFS datastores. For production environments, it is recommended that IT administrators review storage best practices documentation to determine the best storage options for various types of virtual machines.

**Networking**

For this architecture, vSphere network-distributed switch technology was leveraged to simplify the configuration.

Standard VLANs were used to segregate vSphere management, services management, and desktop virtual machine traffic. All uplink ports were configured as VTP trunk ports into the vSphere hosts. All networking was then broken out at the virtual distributed switch (vDS) level.

**Security**

The Federal Secure Desktop solution places very high emphasis on security and meets all the compliance requirements of a federal deployment. The key components of Security integrated into this architecture are:

- CAC card support
- McAfee HBSS
- 802.1X authentication
- vCloud Networking and Security and vShield Endpoint
- Zero clients

We will look at some of these key components in more detail in the sections that follow.

**CAC Card Support**

VMware Horizon View has supported the use of smart cards for years. Several federal agencies have successfully deployed VMware solutions, which meet the smart card standards. VMware Horizon View supports both Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) to ensure that digital certificate status is up to date and valid.

Teradici has tested these specific smart card models:

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>SPECIFICATION AND/OR APPLET</th>
<th>MIDDLEWARE PROVIDER</th>
<th>SUPPORTED BY Firmware</th>
<th>DESCRIPTION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyberflex Access 64K V2c</td>
<td>CAC (GSC-IS), ActivClient v2.6.1 applet</td>
<td>ActivIdentity</td>
<td>Yes (FW3.2.0 and higher)</td>
<td>Also referred to as the Gemalto Access 64Kv2</td>
<td>None</td>
</tr>
<tr>
<td>ID-One Cosmo v5.2D 64K</td>
<td>CAC (GSC-IS), ActivClient v2.6.1 applet</td>
<td>ActivIdentity</td>
<td>Yes (FW3.2.0 and higher)</td>
<td>Also referred to as the Oberthur Cosmo 64V5.2D</td>
<td>None</td>
</tr>
<tr>
<td>ID-One Cosmo v5.2D 72K</td>
<td>CAC (GSC-IS), ActivClient v2.6.1 applet</td>
<td>ActivIdentity</td>
<td>Yes (FW3.2.0 and higher)</td>
<td>Also referred to as the Oberthur ID One V5.2</td>
<td>None</td>
</tr>
<tr>
<td>Cyberflex Access v2c 64K</td>
<td>CAC (GSC-IS), ActivClient v2.6.1 applet</td>
<td>ActivIdentity</td>
<td>Yes (FW3.2.0 and higher)</td>
<td>Also referred to as the Gemalto Access 64Kv2</td>
<td>None</td>
</tr>
<tr>
<td>ID-One Cosmo v5.2D 72K</td>
<td>CAC (PIV Transitional), ActivClient v2.6.2 applet</td>
<td>ActivIdentity</td>
<td>Yes (FW3.2.0 and higher)</td>
<td>Also referred to as the Oberthur ID One V5.2 Dual</td>
<td>This card has both contact and contactless interfaces. Teradici only supports the contact interface.</td>
</tr>
<tr>
<td>PRODUCT</td>
<td>SPECIFICATION AND/OR APPLET</td>
<td>MIDDLEWARE PROVIDER</td>
<td>SUPPORTED BY Firmware</td>
<td>DESCRIPTION</td>
<td>NOTES</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>Gemalto GemComb-iXpresso R4 dual interface</td>
<td>CAC (PIV Transitional), ActivClient v2.6.2 applet</td>
<td>Actvidentity</td>
<td>Yes (FW3.3.0 and higher)</td>
<td>Also referred to as the Gemalto GCX4 72K DI</td>
<td>This card has both contact and contactless interfaces. Teradici only supports the contact interface.</td>
</tr>
<tr>
<td>ID-One Cosmo v5.2D 72K</td>
<td>CAC (PIV Endpoint), ActivClient v2.6.2 applet</td>
<td>Actvidentity</td>
<td>Yes (FW3.3.0 and higher)</td>
<td>Also referred to as the Oberthur ID One V5.2 Dual</td>
<td>This card has both contact and contactless interfaces. Teradici only supports the contact interface.</td>
</tr>
<tr>
<td>Gemalto GemComb-iXpresso R4 dual interface</td>
<td>CAC (PIV Endpoint), ActivClient v2.6.2 applet</td>
<td>Actvidentity</td>
<td>Yes (FW3.3.0 and higher)</td>
<td>Also referred to as the Gemalto GCX4 72K DI</td>
<td>This card has both contact and contactless interfaces. Teradici only supports the contact interface.</td>
</tr>
<tr>
<td>Gemalto TOP DL GX4 144K</td>
<td>CAC (PIV Endpoint), ActivClient v2.6.2 applet</td>
<td>Actvidentity</td>
<td>Yes (FW3.3.0 and higher)</td>
<td>Also referred to as the Gemalto GCX4 144K</td>
<td>This card has both contact and contactless interfaces. Teradici only supports the contact interface.</td>
</tr>
<tr>
<td>Oberthur ID-One Cosmo 128 v5.5 for DoD CAC</td>
<td>CAC (PIV Endpoint), ActivClient v2.6.2 applet</td>
<td>Actvidentity</td>
<td>Yes (FW3.3.0 and higher)</td>
<td>Also referred to as the Oberthur ID One 128 v5.5 Dual</td>
<td>This card has both contact and contactless interfaces. Teradici only supports the contact interface.</td>
</tr>
<tr>
<td>Cosmopolitan 64K V5.2</td>
<td>CAC (GSC-IS), ActivClient v2.6.2 applet</td>
<td>Actvidentity</td>
<td>Yes (FW3.2.0 and higher)</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>ID-One Cosmo v7.0 with Oberthur PIV Applet Suite 2.3</td>
<td>CAC (PIV Endpoint), ActivClient v2.3.2 applet</td>
<td>Actvidentity</td>
<td>Yes (FW3.4.0 and higher)</td>
<td>A PIV Endpoint card uses the T=1 protocol</td>
<td>None</td>
</tr>
<tr>
<td>GemComb-iXpresso</td>
<td>CAC (PIV Endpoint), ActivClient v2.6.2 applet</td>
<td>Actvidentity</td>
<td>Yes (FW3.3.0 and higher)</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>ID-One Cosmo 64 v5.2D Fast ATR with PIV application SDK</td>
<td>CAC (PIV Endpoint), ActivClient v2.6.2 applet</td>
<td>Actvidentity</td>
<td>Yes (FW3.3.0 and higher)</td>
<td>Also referred to as the Gemalto TOP DL GX4 72K</td>
<td>None</td>
</tr>
<tr>
<td>Cyberflex Access 64K V2c</td>
<td>ACS PKI 1.12</td>
<td>Gemalto Access Client</td>
<td>Yes (FW4.0.0 and higher)</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Cyberflex Access 64K V2c</td>
<td>ACS PKI 1.14</td>
<td>Gemalto Access Client</td>
<td>Yes (FW4.0.0 and higher)</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Axalta Cryptoflex .NET</td>
<td>Gemalto .NET</td>
<td>Gemalto / Windows</td>
<td>Yes (3.4.1 and higher)</td>
<td>Implements the Gemalto .NET standard. The middleware is built into Windows.</td>
<td>None</td>
</tr>
</tbody>
</table>
Table 4: Teradici-Supported CAC Card Models

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>SPECIFICATION AND/OR APPLLET</th>
<th>MIDDLEWARE PROVIDER</th>
<th>SUPPORTED BY Firmware</th>
<th>DESCRIPTION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeNet SC650</td>
<td>Coolkey applet</td>
<td>90meter</td>
<td>Yes (3.5.1 and higher)</td>
<td>Yes (FW3.2.0 and higher)</td>
<td>This card uses 3V power, which many readers do not supply. Please see the reader list for compatible readers.</td>
</tr>
</tbody>
</table>

**Notes:** Your card may be on the supported card list; however, the applet of the card may not be supported.

PCoIP zero clients locally terminate the smart card readers for pre-session authentication. This means that they are not re-directed via USB. As such, the View Agent’s PCoIP smart card component must be installed for the guest OS to see the smart card reader (this is not installed by default).

Pre-session smart card authentication to remote workstations using PCoIP host cards is not supported at this time.

Supported devices are subject to change. Visit the Teradici Web site for the latest updates, or open a ticket with Teradici Systems Engineering to request support for additional readers and smart card variants.

**Note:** Although only zero clients from Teradici are highlighted in the above table, thin client partners like Wyse and HP have full product lines supporting PKI-enabled devices and token access to the federal agency network.

**McAfee HBSS**

For virtual desktop antivirus protection, McAfee MOVE AV is fully validated and compatible with VMware vShield Endpoint, included with vSphere 5.1.

![Figure 3: A Single McAfee MOVE Virtual Appliance Installed on the Hypervisor Provides Antivirus Protection for Multiple Virtual Machines](image)

HBSS provides advanced mitigation efforts necessary to detect, defend, react and deter, in real time, against known cyber-threats. In the current DoD network environment, HBSS is critical to maintaining network security, and addresses current network vulnerabilities to prevent future intrusions. Refer to the DISA Web site for more information on the HBSS components. For more information on McAfee MOVE AV and HBSS configuration and best practices for the Federal desktop, please refer to the McAfee MOVE /VMware Collaboration Best Practices guide.

**802.1X Authentication**

Depending on the authentication setting on a switch or router, 802.1X authentication can allow a remote router to connect authenticated VPN users to a secure network through a VPN tunnel. Users are then authenticated in the secure network through a RADIUS server. In Federal Secure Desktop, the design covers end-to-end security practices. In the lab validation, we enabled 802.1X authentication on the switch port. Please refer to your network equipment user guide for more information on how to enable 802.1X authentication.

**vCloud Networking and Security and vShield Endpoint**

The following virtual appliances were deployed in the design:

- **Edge** – Secures the edge of the virtual datacenter by being configured to be the firewall, VPN, Web load balancer, NAT and DHCP services to monitor packet headers for source and destination IP addresses.
- **App** – Protects applications in the virtual datacenter from network-based threats.
• **vShield Endpoint** – Included in vSphere 5.1, vShield Endpoint strengthens security for virtual machines and their Windows Server hosts while improving performance.

VMware vCloud Networking and Security App can be used as a load balancer for internal View Connection Servers accessed exclusively by users inside the corporate network. The external connections are load balanced via network load balancers.

**Management**

The Horizon View Administrator console shows the health of various components deployed within the infrastructure (not including third-party products). This level of information is very basic but can be sufficient for many organizations.

For organizations that require enhanced monitoring and management, including capacity planning, this architecture integrates the VMware vCenter Operations Manager for Horizon View as an optional component. When integrated, this product provides end-to-end visibility into the Horizon View environment. The patented analytics and integrated approach to performance, capacity, and configuration management delivers simplified health and performance management along with a better end-user experience, as any issues can be identified and solved proactively.

In addition to the above analytics, the architecture also supports adding more third-party analytics and monitoring tools to suit any such organizational needs.

**Endpoint Management**

We validated the Teradici zero client that has no local embedded OS footprint.

PCoIP Zero Client Management software is a simple, web-based tool with automated configuration to manage the entire ecosystem of PCoIP devices.

The PCoIP Management Console is a web-based management tool that allows administrators to deploy and manage an entire enterprise deployment of PCoIP devices from a central console, further streamlining the already minimal management of a PCoIP infrastructure.

With the PCoIP Management Console, administrators can:

• Monitor, configure and update all PCoIP devices from anywhere
• Graphically view status and connection information
• Remotely access and update configuration settings
• Auto-configure devices when devices are discovered on the network
• Manage devices individually or by group (i.e., location, department, function)
• Schedule firmware updates, profile application modifications, and power state changes
• Assign static connections between PCoIP hardware host and client devices
• Apply configuration data to individual devices or groups of devices
• Deploy bulk firmware updates
• Support multiple device discovery mechanisms
• View and manage device logs
• Manage the power of devices
Persona Management

In a traditional physical desktop with local storage, all the changes a user makes to their profile are stored on the local hard disk. In the virtual desktop world, desktops are available in two versions: dedicated desktops (also known as persistent desktops) in which users are assigned a specific desktop and use that desktop each time they log in; and floating desktops (also known as nonpersistent) which provide the user any available desktop for each session. For dedicated desktops, the user’s profile is stored in a persistent data disk. But dedicated desktops are not storage efficient and increase the total cost of ownership for the solution.

The Federal Secure Desktop solution (like the Mobile Secure Workplace solution) employs floating desktops with Persona Management enabled. This feature seamlessly preserves a user’s profile on a network share for safekeeping between sessions. Persona Management persists data and settings stored in the profile without specific knowledge of how a particular application works. This enables the architecture to be more storage-efficient. The Persona Management feature is also efficient during login times, as it downloads only the files that Windows requires, such as user registry files. Other files are copied to the desktop when the user or an application opens them from the profile folder, thus increasing efficiency.
Key Deployment Considerations

The deployment details can be segregated into five key categories:

• Initial setup
• CAC certificate setup
• Deploying the base image and desktop pools
• McAfee HBSS
• Configuring zero clients and 802.1X authentication

The following section covers the details and key considerations in each category.

Initial Setup

One of the key considerations in deploying this federal solution is that, in a typical DoD environment, there are multiple unreachable domains, and control is often not at the local level. When the View Connection Server is installed, ensure that it is installed as a local/internal server, and the connection to `<HTTP:// FQDN Of ViewManager/admin>` is verified. Ensure that no other service is using ports 80 and 443. Also, ensure that the IIS service is not running in the View Connection Server and that all ports listed in the VMware Knowledge Base article Network connectivity requirements for VMware View Manager 4.5 and later are open.

A typical DoD setup can have multiple domains, so it is important to exclude non-essential domains from each Horizon View installation to reduce start-up times. The non-essential and unreachable domains can be excluded by the VDMAdmin command:

```
vdmadmin -N -domains -exclude -domain <Domain Name> -add
```

CAC Certificate Setup

All U.S. federal employees are mandated to use PIV cards. The three variations are:

• Federal PIV Cards
• Common Access Cards (CAC)
• SIPR Tokens

DoD has adopted the PKI-based CAC as their primary authentication method into the NIPRNet. NIPRNet is composed of Internet Protocol routers owned by the DoD.

Several agencies have also migrated to SIPR hardware tokens as their primary authentication method for accessing the SIPR network. Other agencies are also moving toward a PKI-based PIV card for authentication into the federal network.

All are based on PKI/X.509 certificates and any one of them can be used to access virtual desktops in this design.

PKI is designed to allow secure communications, nonrepudiation, and authentication between two entities. It uses two keys to generate a web of trust.

In this design, the Certificate Authority (CA) is used to issue certificates and key pairs to entities (servers, devices, users, etc.). In our design, we use a combination of Root Certificate Authority (Root CA) and Intermediate CA for scalability purposes. Root CA has the highest authority to issue certificates and delegates some of the workload to the Intermediate CA for scalability and redundancy. Refer to the VMware Horizon View Administration guide for more information.
To enable smart cards to work with Horizon View, the following steps must be performed:

1. Obtain all required root and intermediate CA certificates.
2. Import certificates into a keystore file.
3. Build a locked.properties file. Make the following entries to the file:
   
   ```
   trustKeyfile=masterkeystore
   trustStoretype=JKS
   useCertAuth=true
   ```
4. Put keystore and locked.properties into the `<installdir>/server/sslgateway/conf` folder.
5. Restart the View Connection Server to make your changes take effect.

To obtain DoD root or intermediate certificates, visit the Military CAC Web site.

### Deploying the Base Image and Desktop Pools

When deploying a base image for this solution, it is critical to start from a new image instead of using a physical to virtual desktop image. Optimize the image based on the recommendations in the VMware Horizon View Administration guide and configure the image based on organizational policies. Accordingly, disable Windows Firewall on the domain network if allowed, or open ports 4172 UDP, 4172 TCP, 3389 TCP (only if RDP is to be used), 32111 TCP, and 9427 TCP in the Windows Firewall and any other client-side, port-filtering applications being used.

For Single Sign-On to function, the Terminal Service/Remote Desktop service must be enabled. By default, all images based on Federal Desktop Core Configuration (FDCC) have the service disabled, and you need to perform the following steps to enable the service:

1. In Windows Vista or Windows 7, right click Computer from the Start Menu and select Properties. On the upper left side of the Properties dialog, select Remote Settings.
2. In the Remote Settings dialog, make sure Allow connections only from computers running remote desktop with network level authentication is checked and then click Select Users to assign the users that are allowed to connect.
3. In the Remote Desktop Users dialog, click Add, and in the Select Users dialog enter the group or groups that contain all potential Horizon View users and the View Connection Server service account (typically the Domain Users group from the local authentication domain).
4. Ensure there are no denials for remote desktop connectivity. By default these images typically have Everyone denied access. This explicit deny will override the Allow that was set up in the above steps.
   a. Open a command prompt using Run As Administrator.
   b. Type `gpedit.msc <Enter>`.
   c. In the Local Group Policy Editor navigate to Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment.
   d. In the right panel, scroll down to Deny log in through Terminal Services. Double-click and check to see if there are any groups there. If there are any groups listed, they will be unable to connect to a Horizon View desktop. Select each group (especially the Everyone group) and click Remove to remove them from the deny list. Then click OK.
5. Scroll up to **Allow log in through Remote Desktop Services** and double-click. By default, Administrators and Remote Desktop Users are granted this right. Add the Domain Users group from the authentication domain (or any group or groups that contain all the potential Horizon View desktop users and the View Connection Server service account). Click **OK** and close the Group Policy Editor.

**Note:** Ensure that the domain-level GPO does not override the above settings. After the base image is created, to activate it in DoD, a valid CAC card is required. CAC can be passed through to the image via the vSphere 5 client through the console, with the USB controller added to the parent image to allow this (Dameware and RDP can also be used). Once the CAC is passed through, activate Windows, select the certificate, and enter a CAC PIN under Control Panel\System and Security\System.

6. Finally, ensure that VMware Tools is installed before installing Horizon View Agent.

For desktop pools in this architecture, it is recommended that you use floating pools with ThinApp, Persona and User Data locations redirected at login. To enhance the user experience, third-party persona management tools can also be used.

As a best practice for this solution, ensure that users are logged out 120 minutes after disconnect and that the desktops are refreshed immediately after logout. Ensure that PCoIP is set as the default protocol to access desktops, and disable users from choosing the protocol. Also, for a better user experience, ensure that Adobe Flash Quality is set to Medium in the pool settings in the View Connection Server.

**McAfee HBSS**

For optimal performance of McAfee HBSS, the following considerations are recommended:

- Set **McAfee agent to server communication interval** to 720 minutes or less
- Set **policy enforcement interval** to 30 minutes or less
- Perform a full scan on the parent image before building pools
- If allowed, only scan on Read, not Write
- Disable the setting **Run Missed Jobs at startup**

**Configuring Zero Clients and 802.1X Authentication**

Zero clients based on the Teradici TERA chipset are ultra-secure, easy-to-manage devices that offer the richest user experience in this solution. In addition to supporting a variety of authentication methods (SIPR Tokens, CAC cards) and encryption types (TLS 1.0 with AES-128-CBC-SHA, TLS 1.0 with AES-256-CBC-SHA, Suite B ciphers, AES-128-GCM, AES-256-GCM and Salsa20-256-Round12), zero clients also support 802.1X network device authentication using EAP-TLS certificates. Under this method, all network endpoint devices must be authenticated before they are granted access to the network, thus adding an additional layer of security beyond username and password credentials. To configure this, an 802.1X-supported switch was used in this architecture.
User Connection Flow Sequence

This sequence shows how a desktop, laptop, or mobile device connects to virtual machines in a datastore managed by VMware vSphere. This includes secure implementations that require a NIPRNet token or tokens from the newer SIPRNet.

Summary

The Federal Secure Desktop solution provides a validated end-to-end architecture for DoD and other federal agency deployments which takes into account all the key components required for a secure Horizon View implementation.

This architecture, built with VMware Horizon View and ecosystem partner components, was tested for the ability of various integrated products to provide a validated solution. The architecture, while tightly integrated, is also built to be modular so customers can pick and choose the various components that fit their specific needs. The architecture is also scalable per the guidelines provided in VMware Horizon View reference architectures.

This design caters to the three key virtual desktop requirements in any federal organization—mobility, security and management. With VMware Horizon View and other management products like vCenter Operations Manager, this design enhances the security requirement by adding federal-specific components like Common Access Cards, SIPR Tokens, and HBSS. The solution also provides enhanced network-level security, integrating 802.1X authentication with zero clients.
About the Authors


The authors would like to thank Glenn Exline, Systems Engineering Manager at VMware; Elcio Mello from Teradici; and Christie Karrels and Christopher Beckham from McAFeefor their contributions to the content and validation of the solution.

To comment on this paper, contact the VMware End-User Computing Solutions Management and Technical Marketing team at twitter.com/vmwareeucsmtm.