VMware, Inc.
3401 Hillview Ave, Palo Alto, CA 94304, USA, Tel: (877) 486-9273, www.vmware.com

Guidance Supplement

VMware Horizon Connection Server 8 2209 (8.7)

Common Criteria (CC) Evaluated Configuration Guidance

Document Version: 1.0
Document Date: April 25, 2023

vmware®

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
United States of America

Phone: +1 (877) 486-9273
http://www.vmware.com

VMware Horizon

https://www.vmware.com/products/horizon.html

VMware Security Response Center

http://www.vmware.com/support/policies/security_response.html

security@vmware.com

REVISION HISTORY

Ver #	Description of changes	Modified by	Date
1.0	Initial release of document	Justin Fisher	April 25, 2023

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

1.1 Purpose

This document describes the operational guidance and preparative procedures for VMware Horizon Connection Server, which is a component of VMware Horizon™. This document defines the necessary steps to configure the Target of Evaluation (TOE) for use and provides guidance for the ongoing secure usage of the TOE.

The evaluated configuration of the VMware Horizon Suite includes the following components:

- VMware Horizon Client for Windows
- VMware Horizon Client for Android
- VMware Horizon Connection Server
- VMware Horizon Agent for Linux
- VMware Horizon Agent for Windows
- VMware Unified Access Gateway (UAG)

Separate guidance documents exist for each component. Refer to the NIAP Product Compliant List (PCL) at https://www.niap-ccevs.org/Product/PCL.cfm for each product validation and its associated documentation.

1.2 Document Reference

This document serves as a supplement to the standard VMware documentation set, and as such references (either implicitly or explicitly) the documents referenced in this section.

General security, installation, and operational guidance for the Horizon Suite can found at the following links:

- Horizon Security
- Horizon Installation and Upgrade
- Horizon Overview and Deployment Planning

Component-specific guidance can be found at the following links:

- Horizon Administration
- Cloud Pod Architecture in Horizon
- Linux Desktops and Applications in Horizon
- Windows Desktops and Applications in Horizon

Note that some functionality referenced in the documentation is considered to be non-interfering with respect to security because it did not fall within the scope of the security requirements applied by the Common Criteria evaluation. A full list of excluded functions is included in section 1.3 below.

1.3 Features and Functions Not Included in the TOE Evaluation

This product was evaluated against applicable requirements in the Protection Profile for Application Software and Functional Package for Transport Layer Security (TLS). Listed below are those functions that are explicitly excluded from the evaluation scope and will not be configured or activated as part of placing the product into its evaluated configuration:

- Cloud deployment – VMware Horizon supports several different cloud environments; Common Criteria certification excludes cloud-based deployments so only on-premises installations are considered to be within the evaluation scope.
- OpenSSL – OpenSSL is present in the product but is excluded from the evaluated configuration because it is used for external interfaces that are not within the evaluation scope. Specifically, OpenSSL is used for remote client interfaces when a UAG is not present in the environment and clients access the Connection Server directly.
- Enrollment Server functionality – A Connection Server may be configured as an Enrollment Server for end-user certificate-based credentials. This is excluded from evaluation scope because the evaluated configuration requires Horizon Client users to authenticate using PKI tokens, which do not make use of an Enrollment Server.
- Replica Server – The claimed security requirements do not relate to availability so replica server functionality, which is used for high-availability/failover protection, is not included in the evaluation scope.
- Non-FIPS Mode of Operation – the evaluated configuration requires the use of the product's FIPS-compliant mode.

Refer to the Security Target for the product to see the functional claims made for the product that are considered to be security-relevant with respect to the claimed standard. Any product functionality that is not specifically related to addressing the claimed security functions and is not listed in the exclusions above is considered to be non-interfering with respect to security; that is, its presence or configuration does not affect the ability of the product to meet the claimed security requirements.

As a general example, external interfaces to the product that use TLS are evaluated for their secure implementation of the TLS protocol; the actual data transmitted over the TLS interface is not addressed by any specific security requirements. Similarly, the claimed standards do not define any access control requirements, so the specific virtual desktop content that is served to a user based on their assigned privileges was not tested as part of this evaluation.

2 INSTALLATION GUIDELINES AND PREPARATIVE PROCEDURES

2.1 Assumptions

The following assumptions are made with regards to the setup, installation, and ongoing operation of this product:

- The computing platform on which the product is installed is assumed to be trustworthy through appropriately hardened configuration and is assumed to have various services available that the product can make use of, including a system clock that can be presumed to be accurate.
- Application users are not willfully negligent or hostile and will operate the product in accordance with any organizational usage policies.
- Application administrators are not willfully negligent or hostile and will operate the product in accordance with any organizational usage policies.

2.2 Evaluated Configuration

The evaluated configuration of VMware Horizon consists of one or more Horizon Clients, a Horizon Connection Server, one or more Horizon Agents, and a VMware UAG. A second Connection Server instance is present in the operational environment to demonstrate connectivity between server instances that reside in separate cloud pods. In the tested configuration, all components except for the Horizon Clients are virtualized on VMware ESXi 7.0. The diagram below shows the evaluated configuration of the VMware Horizon Suite with tested components and interfaces highlighted in blue. VM hypervisors, network boundary/infrastructure devices (e.g., routers, switches, firewalls), and certificate infrastructure (e.g., CA, CRL distribution point, OCSP responder) are not shown for readability purposes.

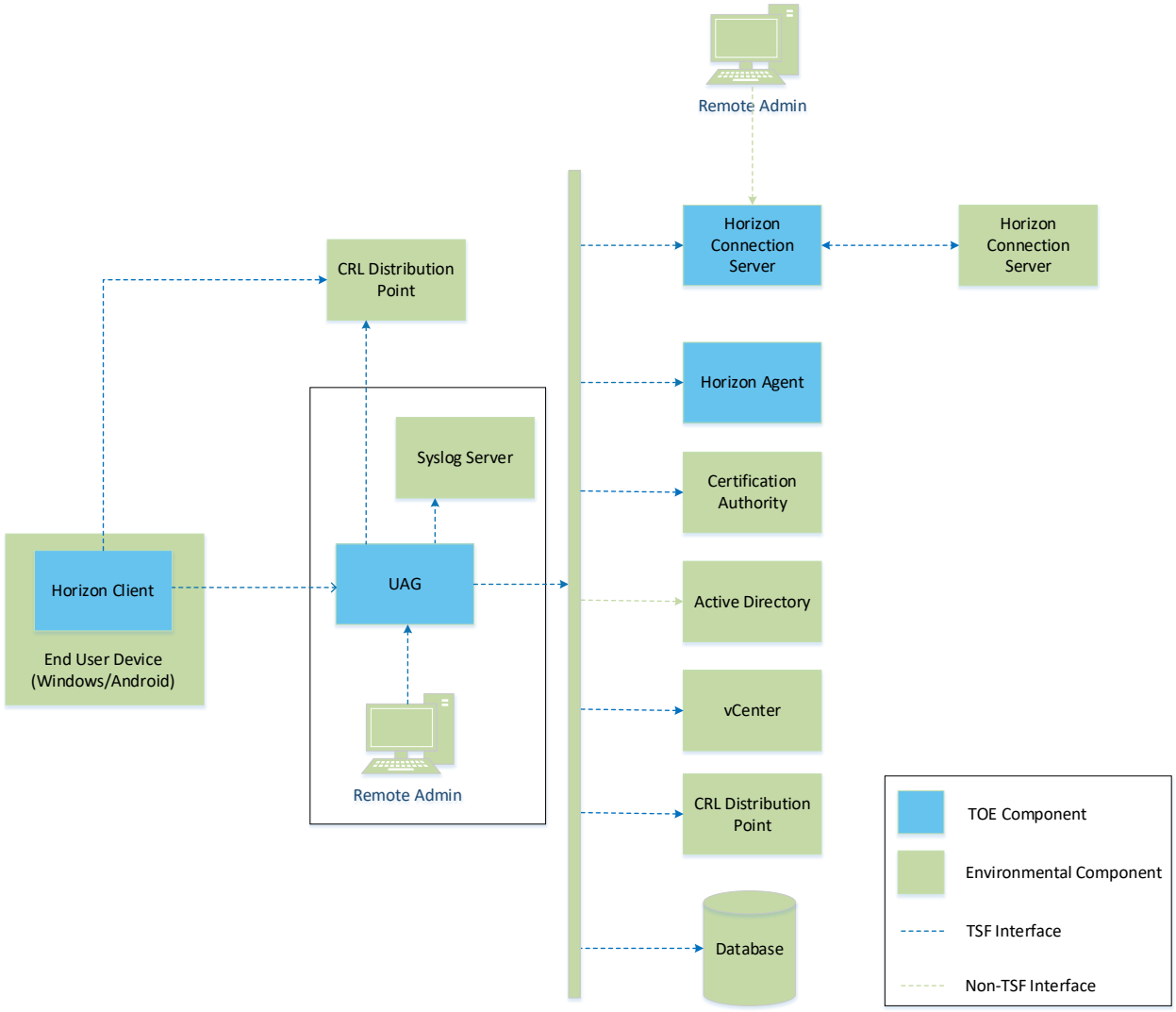


Figure 1: VMware Horizon Evaluated Configuration

The following external interfaces were tested in the evaluated configuration of the product:

- TCP/443: inbound remote administration (TLS server with or without mutual authentication)
- TCP/443: client user SAML token from UAG (TLS server without mutual authentication)
- TCP/8472: Connection Server cloud pod communications (TLS client or server with mutual authentication)
- TCP/variable (depends on database server configuration): outbound database connectivity (TLS client without mutual authentication)
- TCP/443: VMware vCenter connectivity (TLS client without mutual authentication)

Since Horizon consists of multiple components, it is expected that each component is configured in accordance with its own evaluated configuration guidance.

Additionally, the evaluated configuration is defined such that all certificates used within the Horizon deployment are issued by the same Certificate Authority. While not explicitly required for Horizon to function properly, it simplifies administration and reduces the likelihood of misconfiguration leading to error or vulnerability. This Certificate Authority will be used to issue valid smart card certificates to Horizon administrators.

2.3 TOE Components

The TOE consists of the Horizon Connection Server application. The application is compatible with Windows Server 2012 R2, 2016, 2019, or 2022. The tested configuration for the evaluation used Windows Server 2019, virtualized on VMware ESXi 7.0.

Table 1-1 "Horizon Connection Server Hardware Requirements" in Horizon Installation and Upgrade identifies the minimum and recommended hardware specifications for the host platform. Additionally, the underlying OS platform must be configured into FIPS mode. Microsoft guidance for this can be found at https://docs.microsoft.com/en-US/windows/security/threat-protection/fips-140-validation.

Environmental dependencies outside of the underlying host platform are listed in section 2.4 below.

2.4 Supporting Environmental Components

The following table lists the external components that are required for the product to function in its evaluated configuration.

Component	Description
VMware UAG	Used to control access between end user devices on external public networks and organizational resources on an internal private network.
VMware Horizon Connection Server	A secondary instance of a Connection Server that may be federated to grant Horizon Client users access to Horizon Agents in multiple environments.
VMware Horizon Agent	Used to serve content from a remote host to a VMware Horizon Client.
VMware Horizon Client	End user application that requests content to be served to it by VMware Horizon Agents.
Remote workstation	Used for remote administration of Connection Server settings.
External database	Used for recording of user and system activity.
VMware vCenter	Used by the Connection Server to create, start, and stop virtual machines running Horizon Agents on demand. These virtual machines are used to provide appropriate content to a Horizon Client user based on their authorizations.
Certificate Authority	Used to manage the generation, issuance, and revocation of X.509 certificates used for authentication and secure communications.

Table 2: Supporting Environmental Components

2.5 Installation of the TOE

2.5.1 Preparing the Operational Environment

Before installing Horizon Connection Server, the environment must be prepared in the manner specified below.

2.5.1.1 Configuring vSphere

The evaluated configuration is hosted on ESXi and uses vCenter server for VM management. Refer to section "Architecture Design Elements and Planning Guidelines for Remote Desktop Deployments" in Horizon Overview and Deployment Planning.

2.5.1.2 Configuring KMS

A Key Management Server is necessary for VM encryption. Refer to the section "vSphere Native Key Provider Process Flows" in the vSphere Security Guide.

2.5.1.3 Configuring Domains, PKI, Certificates, and User Accounts

Horizon integrates with Microsoft Active Directory and several configuration steps are needed for this. Refer to section "Preparing Active Directory" in Horizon Installation and Upgrade.

2.5.1.4 Configuring Platform Encryption

2.5.1.4.1 VM Encryption

The Horizon Connection Server must be deployed into an environment with full disk encryption to protect data at rest. Refer to "Create an Encrypted Virtual Machine" in the vSphere Security Guide.

2.5.1.4.2 Enabling FIPS Mode on Windows

All Horizon components need to be installed in FIPS mode to be able to be configured in the CC evaluated configuration. Windows OS must be configured to run in FIPS mode before Horizon can be installed in FIPS mode.

The evaluated configuration uses Windows Server 2019. Enable windows to use FIPS by configuring policy "Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options>System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing". More information can be found in Windows System Cryptography.

2.5.2 Obtaining Software

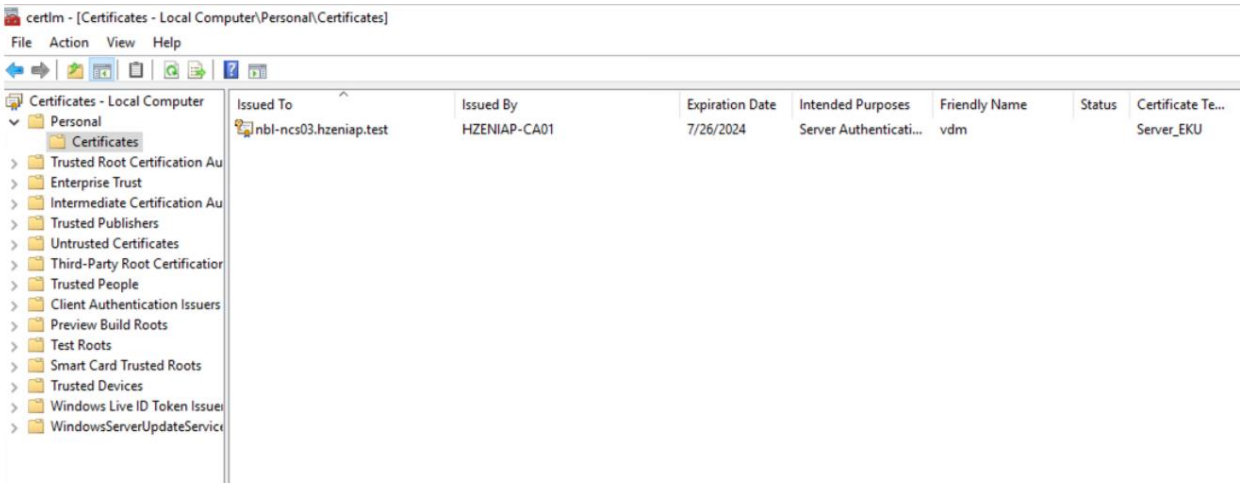
You can obtain software either from an OEM or from the "My VMware" download portal at: https://my.vmware.com/.

Note that there are multiple editions of the Horizon Connection Server software. Select the appropriate edition based on your license key. With respect to the CC configuration of the product, there are no differences in the security functionality and the remainder of this guidance applies to all editions.

2.5.3 Installing Software

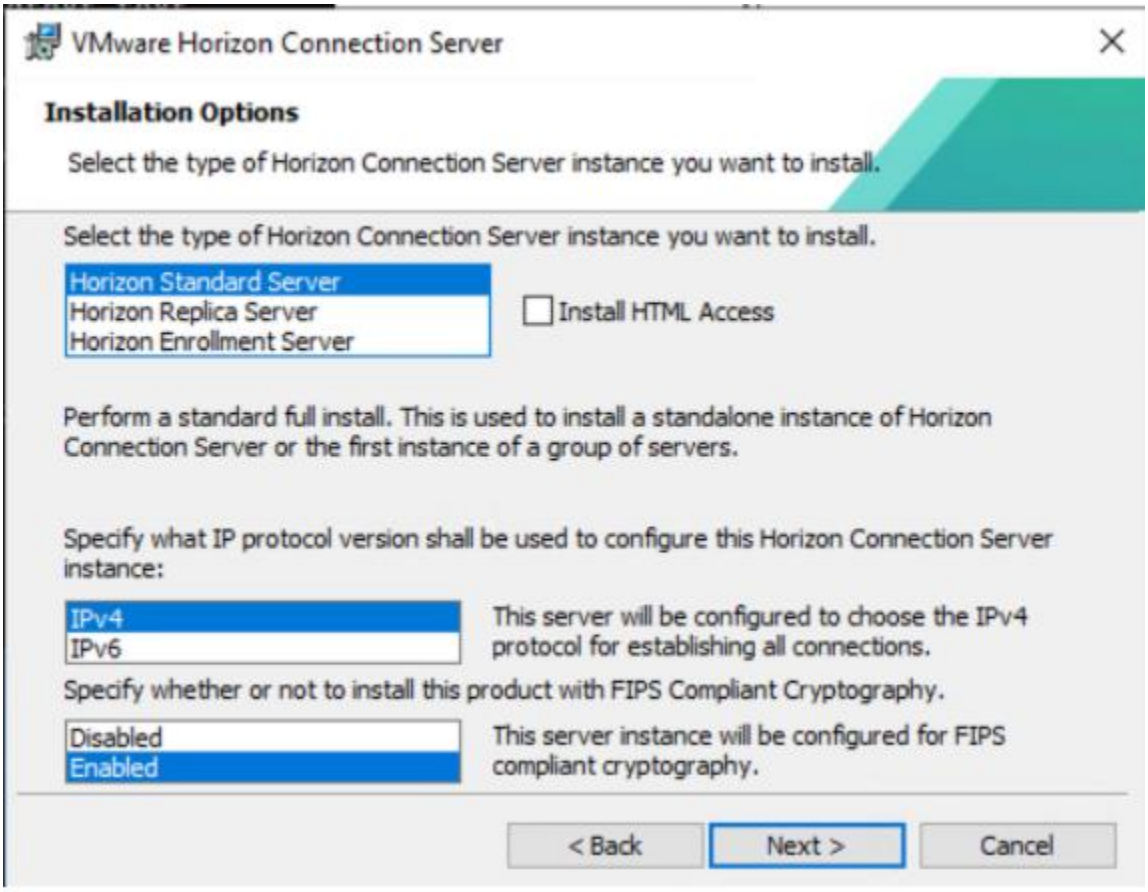
This section describes how to install the Connection Server software. For more information, refer to "Install Horizon Connection Server with a New Configuration" in the Horizon Installation and Upgrade guide.

1. Obtain and configure the Certificate Authority (CA) issued certificate for the Connection Server vdm certificate. This is the certificate that is presented to the UAG. If you have Microsoft Certificate Services in your AD environment, then follow the guidance in https://kb.vmware.com/s/article/80314. Otherwise, follow the guidance in https://kb.vmware.com/s/article/2032400.
2. Create the vdm certificate with the following characteristics:
   - Subject name: FQDN of Connection Server or wildcard matching FQDN
   - SAN: FQDN of Connection Server or wildcard
   - EKU: Server authentication
   - Set friendly name: vdm
   - Private key should be marked exportable
   - Signature Algorithm to use: SHA384
3. On the Connection Server host, use Certificate snap-in to place this certificate in "Certificates (Local Computer)>Personal>Certificates" store
4. Import the CA Root certificate to the Connection Server's "Trusted Root Certification Authorities" Local Computer store and import any intermediate CA certificates into the "Intermediate Certification Authorities Store."



5. Run Horizon Connection Server installer.
6. Select "Horizon Standard Server".

7. Ensure that “Install HTML Access” is deselected and that FIPS Compliant Cryptography is set to “Enabled.”



8. Complete the installation.

2.5.4 Verifying Software

The installer is signed by VMware. Integrity of the installer is checked at installation time; a failed integrity check will prevent installation of the application.

To verify the version of the installed Connection Server on the local system, navigate to Computer\HKEY_LOCAL MACHINE\SOFTWARE\VMware, Inc.\VMware VDM in the Windows Registry. The “Product Version” key will have the current version as its value.

2.6 Updating Software

Software updates are acquired from the VMware site in the same manner as the initial installation package. To install an update, refer to the “Upgrading Horizon Connection Server” section of the Horizon Installation and Upgrade guide. Ensure that all relevant configuration settings from the initial installation are applied.

2.7 Obtaining Support

In the event of software failure, customers should engage with VMware Global Support Services to make use of any purchased support contract(s). See the Support Contact Options for more information.

VMware also maintains comprehensive guidance for all VMware products in the VMware Knowledge Base, located at https://kb.vmware.com/s/. Consult the Knowledge Base for any issues that are not found in other guidance, as well as any product patches and associated documentation.

2.8 Security Issues and Mitigations

VMware maintains a Security Advisories page at https://www.vmware.com/security/advisories.html. Information regarding security issues and product workarounds or fixes for the issues are posted here as part of the timely security update process. Administrators can also sign up for notifications to be made aware of updated guidance and patches as they are released.

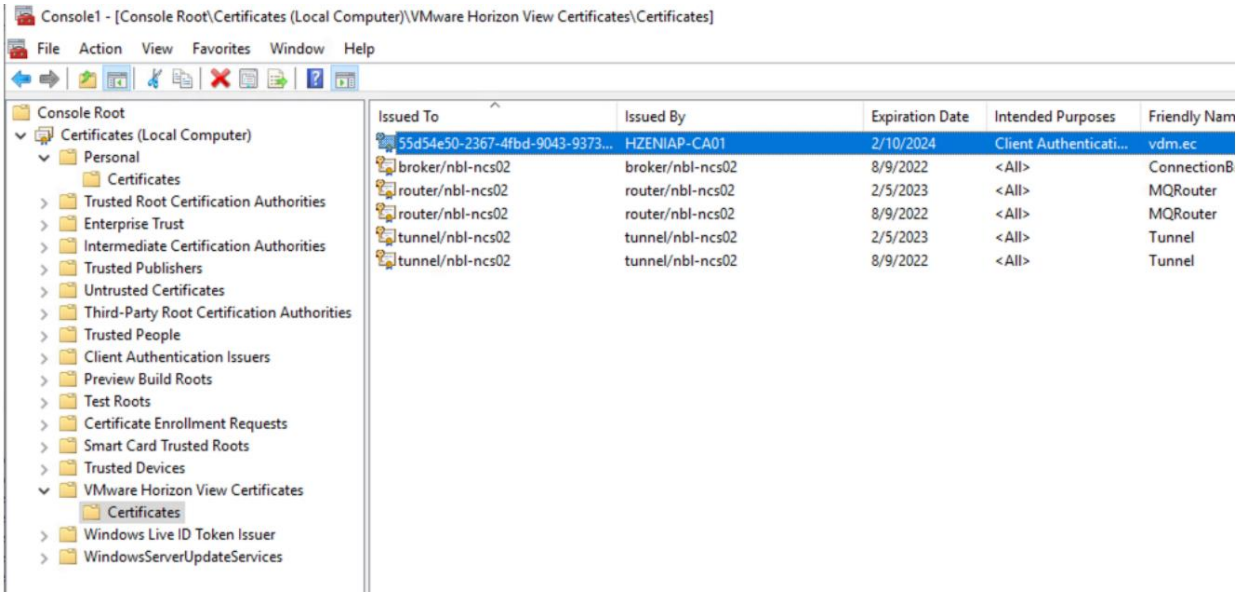
3 POST-INSTALLATION CONFIGURATION

The procedures in this section describe how to configure the installed Connection Server (and its cryptographic engines which include Bouncy Castle BC-FJA implemented within the Connection Server as well as Windows platform cryptography invoked from the Connection Server) for it to be in its evaluated configuration. No other cryptographic engines or configurations were used during the evaluation of the TOE.

3.1 Configure Cluster Certificate

1. Generate a CA signed cluster certificate meeting the following requirements:
    - Subject name: Any
    - SAN: Cluster GUID of Horizon POD as DNSName. Obtain cluster GUID using vdmadmin -C command or from 'Connection Server Cluster GUID' under HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager
    - EKU: Server authentication, Client authentication
    - Private key should be marked exportable
    - Signature Algorithm to use: SHA384
1. On the Connection Server host, use Certificate snap-in to place this certificate in “Certificates (Local Computer)>VMware Horizon View Certificates>Certificates” store.
2. Set the friendly name to:

```
vdm.ec.new
```



3.2 Disable Remote Log Download

To disable the transmission of log data between Horizon Agents and the Connection Server, connect to the local LDAP and set `pae-AgentLogCollectionDisabled` to `1` under `CN=Common,OU=Global,OU=Properties,DC=vdi,DC=vmware,DC=int`

3.3 Change Security Mode of Message Bus

In the evaluated configuration it is necessary to use sender verification for Horizon Agent message bus communications. This operation uses 128-bit AES-CTR keys to encrypt data transmitted between Horizon Connection Server and Horizon Agents. This is configured by doing the following:

1. Set `pae-DisallowEnhancedSecurityMode` to "`1`" under `CN=Common,OU=Global,OU=Properties,DC=vdi,DC=vmware,DC=int` in LDAP.
2. Use vdmutil command-line tool to monitor the message bus security level. Procced to next step only when it reports 'waiting for bus restarts'. Do not restart the service at this point.

   ›vdmutil --getMsgSecLevel --authAs administrator --authDomain yourdomain --authPassword password
   MsgSecLevel: WAITING_FOR_BUS_RESTARTS

No separate configuration beyond this is needed for key establishment and distribution as this is handled automatically by vSphere.

For more information about vdmutil, reference "Using the vdmutil Utility to Configure the JMS Message Security Mode for VMware Horizon 8" in the Horizon Security guide.

3.4 Disable Incompatible Services

In the evaluated configuration, all Horizon Client services are provided through UAG and the Connection Server is not responsible for acting as a gateway for any services.

Review the VMware Knowledge Base and download the script attached to the linked KB reference. Temporarily copy this script to any location on the Connection Server system and proceed as follows.

1. Launch the PowerShell console as an administrator and switch to the directory location where you saved the script.
2. Execute the script by typing "./ManageSecureGatewayService.ps1" in the console.
3. Press '3' to disable both PCoIP and BLAST Secure Gateways.
4. When the script completes it displays "Secure Gateway Configuration Completed", Press 'N' to quit without starting the Connection Server service.

3.5 Configure TLS Parameters

It is necessary to edit the Horizon LDAP attributes that define global acceptance and proposal policies for TLS configuration to ensure that appropriately secure TLS connections are negotiated.

Note that TLS 1.2 is enabled by default; no separate configuration is needed for this.

Security-related settings are provided in Horizon LDAP under the object path `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`

Use the Microsoft ADSI Edit tool to connect to Horizon LDAP instance and modify the values below as follows:

- Server cipher suites are defined by the `pae-ServerSSLCipherSuites` LDAP attribute. Modify the attribute with the following supported values:
  ```
  pae-ServerSSLCipherSuites =
  \LIST:TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_
  SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM
  _SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_25
  6_GCM_SHA384
  ```
- Client cipher suites are defined by the `pae-ClientSSLCipherSuites` LDAP attribute. Modify the attribute with the following supported values:
  ```
  pae-ClientSSLCipherSuites =
  \LIST:TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_
  SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM
  _SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  ```
- Named groups are defined by the `pae-SSLNamedGroups` LDAP attribute. Modify the attribute with the following supported values:
  ```
  pae-SSLNamedGroups =
  \LIST:secp256r1,secp384r1,secp521r1,ffdhe2048(256),ffdhe3072(257),ffdhe
  4096(258),ffdhe6144(259),ffdhe8192(260)
  ```
- Client Signature schemes are defined by the `pae-SSLClientSignatureSchemes` attribute. Modify the attribute with the following supported values:
  ```
  pae-SSLClienSignatureSchemes =
  \LIST:RSA_PSS_RSAE_SHA256,RSA_PSS_RSAE_SHA384,RSA_PSS_PSS_SHA256,RSA_PS
  S_PSS_SHA384,RSA_PKCS1_SHA256,RSA_PKCS1_SHA384
  ```
- Server Signature schemes are defined by the `pae-SSLServerSignatureSchemes` attribute. Modify the attribute with the following supported values:
  ```
  pae-SSLServerSignatureSchemes =
  \LIST:RSA_PSS_RSAE_SHA256,RSA_PSS_RSAE_SHA384,RSA_PSS_PSS_SHA256,RSA_PS
  S_PSS_SHA384,RSA_PKCS1_SHA256,RSA_PKCS1_SHA384
  ```
- To enable TLS to the Event DB set the “pae-enableDbSsl” attribute to “1” under CN=Common,OU=Global,OU=Properties,DC=vdi,DC=vmware,DC=int

Check character cases carefully and ensure that there are no trailing spaces.

3.6 Configure Smart Card Authentication for Admin Console

To configure administrator smart card authentication to the Connection Server, it is first necessary to obtain all applicable CA certificates for all trusted user certificates on the smart cards presented by Horizon administrators. Note that for remote administration, only certificate chains with a path length of two are supported.

1. On the Connection Server host, use the keytool utility to import the root certificate into the server trust store. Note that the 'alias' parameter is a unique friendly name for the certificate.
    - `keytool -import -alias` *`alias`* `-file` *`root_certificate`* `-keystore` *`truststorefile.key`* `-storetype` *`JKS`*
2. Copy the truststorefile.key to the SSL gateway configuration folder `'`*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\'` on the Connection Server host
3. Create the locked.properties file in the same folder on the Connection Server host and enter the following configuration data

    ```
    trustKeyfile=truststorefile.key

    trustStoretype=jks

    useCertAuth=true

    enableRevocationChecking=true
    ```

    Check character cases carefully and there are no trailing spaces.
4. Connect to the Horizon LDAP instance and modify the `pae-CertAuthAdmin` attribute under `CN=CS_Name,OU=Server,OU=Properties,DC=vdi,DC=vmware,DC=int` and set its value to `2`.
1.

3.7 Confirm successful logon to Horizon Console

1. Start Horizon connection server services and wait for a few minutes.
2. Open a browser on the Remote Admin system.
3. Insert smartcard with a valid certificate for the Horizon Administrator and connect to https://connectionserverfqdn>/admin/
4. Configure the license key.
5. Verify '**Horizon Console >Settings>Global Settings>Security Settings>Message Security Status' shows Enabled.**
6. Leave the Horizon Console open to complete the remaining steps.

3.8 Disable Automatic Certificate Management

Automatic certificate management is an optional feature that relies on the issuance of self-signed certificates. Since the CC evaluated configuration of Horizon Connection Server requires PKI certificates to be used, this functionality should be disabled. To do this:

2. Set `pae-NoManagedCertificate` to "`1`" under `CN=Common,OU=Global,OU=Properties,DC=vdi,DC=vmware,DC=int` in LDAP.

3.9 Add Event Database Server

Event Database connectivity requires TLS in the evaluated configuration. To enable this, follow the steps outlined in "SSL Connection to Event Database" in the Horizon Installation and Upgrade guide. These steps are summarized below.

1. Configure the database server with a CA issued certificate that has the following properties:
   - Subject name: FQDN of DB Server or wildcard
   - SAN: FQDN of DB Server or wildcard
   - EKU: Server authentication
   - Signature Algorithm to use SHA384, SHA512
2. Import the CA Root certificate to the Connection Server's "Trusted Root Certification Authorities" Local Computer store. Import any intermediate CA certificate to the Connection Server's "Intermediate Certification Authorities" Local Computer Store. These steps may not be necessary if certificate is from a well-known CA or If it is issued by same CA as Connection Server Certificate.
3. Add the database server using **Horizon Console > Settings > Event Configuration**.

3.10 Add vCenter Server

To configure a TLS connection to vCenter, perform the following steps:

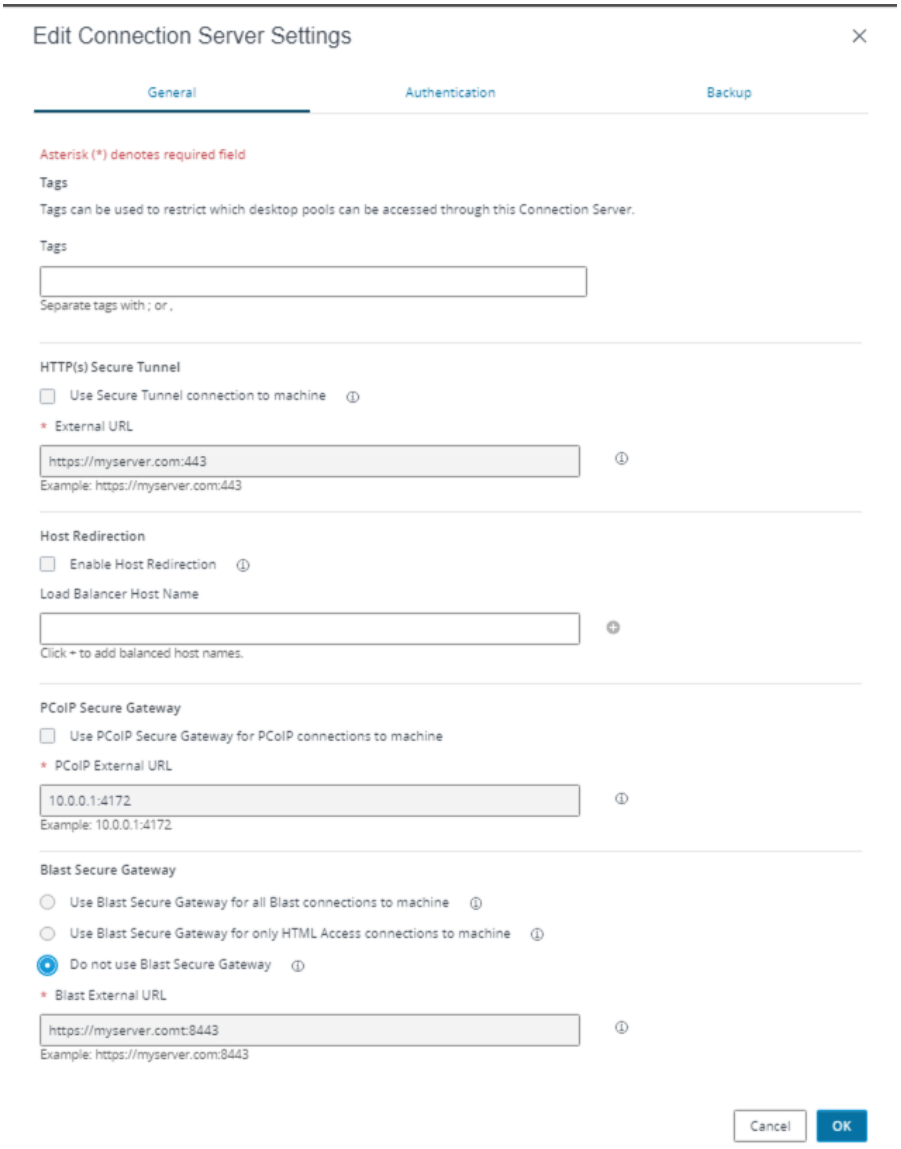
1. Configure the vCenter Server with a CA issued certificate with the following properties:
   - Subject name: FQDN of vCenter or wildcard
   - SAN: FQDN of vCenter or wildcard
   - EKU: Server authentication
   - Signature Algorithm to used: SHA384, SHA512
2. Import the CA Root certificate to the Connection Server's "Trusted Root Certification Authorities" Local Computer store. Import any intermediate CA certificate to the Connection Server's "Intermediate Certification Authorities" Local Computer Store. These steps may not be necessary if the certificate is from a well-known CA or if it is issued by same CA as Connection Server Certificate.
3. Add vCenter server using **Horizon Console > Servers > vCenter Servers - Add**.

3.11 Disable Tunnel

In the evaluated configuration, all Horizon Client services are provided through UAG and the Connection Server is not responsible for acting as a gateway for any services. In the Horizon

Console, go to **Settings > Servers > Connection Servers**, select the Connection Server instance, and click **Edit**. Under Edit Connection Server Settings, ensure that "Use Secure Tunnel connection to machine" and "PCoIP Secure Gateway" are unchecked, and that the **Do not use Blast Secure Gateway** radio button is selected.

Ensure that any necessary changes to the external URL of the Connection Server (e.g. DNS name) are applied to the "External URL" field under "Use Secure Tunnel connection to machine" prior to unchecking the box.



4 OPERATIONAL PROCEDURES FOR ADMINISTRATORS

This section describes additional steps, clarifications, and exclusions that might not be documented in the public documentation for this product. The assumption is that the TOE and its environment have already been successfully set up and working before these next steps are performed.

4.1 System Resources Used

Horizon Connection Server requires the use of the underlying operating system's network connectivity to process incoming connection requests, to set up and configure virtual machines running Horizon Agents, and to connect to external federated instances. It also requires the use of the underlying platform's log functionality to record its own behavior for diagnostic purposes.

4.2 Management Functions

The TOE is managed through its web GUI. Some management functions relate to the configuration of the TOE itself, but most relate to the configuration of environmental components. Specifically, the primary purpose of the TOE is to facilitate connectivity between Horizon Clients and Horizon Agents. Configuration then largely revolves around the access that individual Horizon Client users are granted to resources that are managed by Horizon Agents. The following management functions are configurable via the GUI:

- Log bundle collection – Setting log levels, initiating/cancelling requests to collect logs, downloading log bundles to the local file system, and deleting logs. Collection of Agent Logs is not supported from Horizon console in the evaluated configuration.

  Collect Logs in Horizon Console

  VMware Horizon Log Files

- Administer policy, including idle session policy – configuring the types of resources that clients are globally allowed/not allowed to interact with and how long an active client session can remain idle before termination.

  Entitling Users and Groups

  Global Settings for Client and Console Sessions

- Allocate roles to administrative users – configuring the administrative levels of privilege used to interact with the TOE's management functionality.

  Understanding Roles and Privileges

- Administer entitlements to resources – Configuring the Horizon Client users that are authorized to launch a particular resource on a Horizon Agent system.

  Entitling Users and Groups

- Helpdesk functions – Used to perform various support activities for users who may be having difficulty accessing their authorized resources.

  Using Horizon Help Desk Tool in Horizon Console
  - View status of desktop or application sessions – covered under Session Details for Horizon Help Desk Tool
  - Administration of helpdesk access to desktop resources – covered under Privileges for Horizon Help Desk Tool Tasks
  - Perform remote assistance to TOE users on connected desktops – covered under Troubleshooting Users in Horizon Help Desk Tool and under Troubleshoot Desktop or Application Sessions in Horizon Help Desk Tool (under Remote Assistance)
  - Disconnect and log off desktop or application sessions – covered under Troubleshoot Desktop or Application Sessions in Horizon Help Desk Tool (under Disconnect)
  - Restart virtual desktop infrastructure VM – covered under Troubleshoot Desktop or Application Sessions in Horizon Help Desk Tool (under Restart
  - Send notification to published desktop or application – covered under Troubleshoot Desktop or Application Sessions in Horizon Help Desk Tool (under Send Message)