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

Guidance Supplement

VMware Horizon Client 8 2209 (Horizon 8.7)

Common Criteria (CC) Evaluated Configuration Guidance

Document Version: 1.0
Document Date: April 4, 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 4, 2023

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose

This document describes the operational guidance and preparative procedures for VMware Horizon Client, 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 VMware Horizon 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 Horizon can found at the following links:

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

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

- VMware Horizon Client for Android Documentation
- VMware Horizon Client for Windows Documentation

Note that VMware Horizon Client is available on several additional OS platforms; these were not included in the scope of the evaluation so no assurance of their security functions can be made with respect to Common Criteria requirements. Similarly, 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 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 should be disabled or otherwise made unavailable as part of placing the product into its evaluated configuration:

- Direct Connection Server interface – The product supports the ability to communicate directly with a Connection Server as part of establishing a virtual desktop session. In the evaluated configuration, a UAG is expected to be present so no communications over this interface will occur. The application will be configured such that the destination server is a UAG.
- Tunnel Channel – The Horizon Client supports an HTTPS channel that can be used for some communications with a remote Horizon Agent running Windows, such as RDP. In the evaluated configuration, this channel is not used and all such communications are routed through the Blast channel.
- PCoIP – Virtual desktop connectivity supports both PC over IP (PCoIP) and Blast as a communications channel to remote Horizon Agents. In the evaluated configuration, PCoIP is disabled on the Horizon Agent so only the Blast channel is used.

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 secondary Horizon Connection Server was also used for the purpose of testing cloud pod communications. 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 VMware Horizon 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) are not shown for readability purposes.

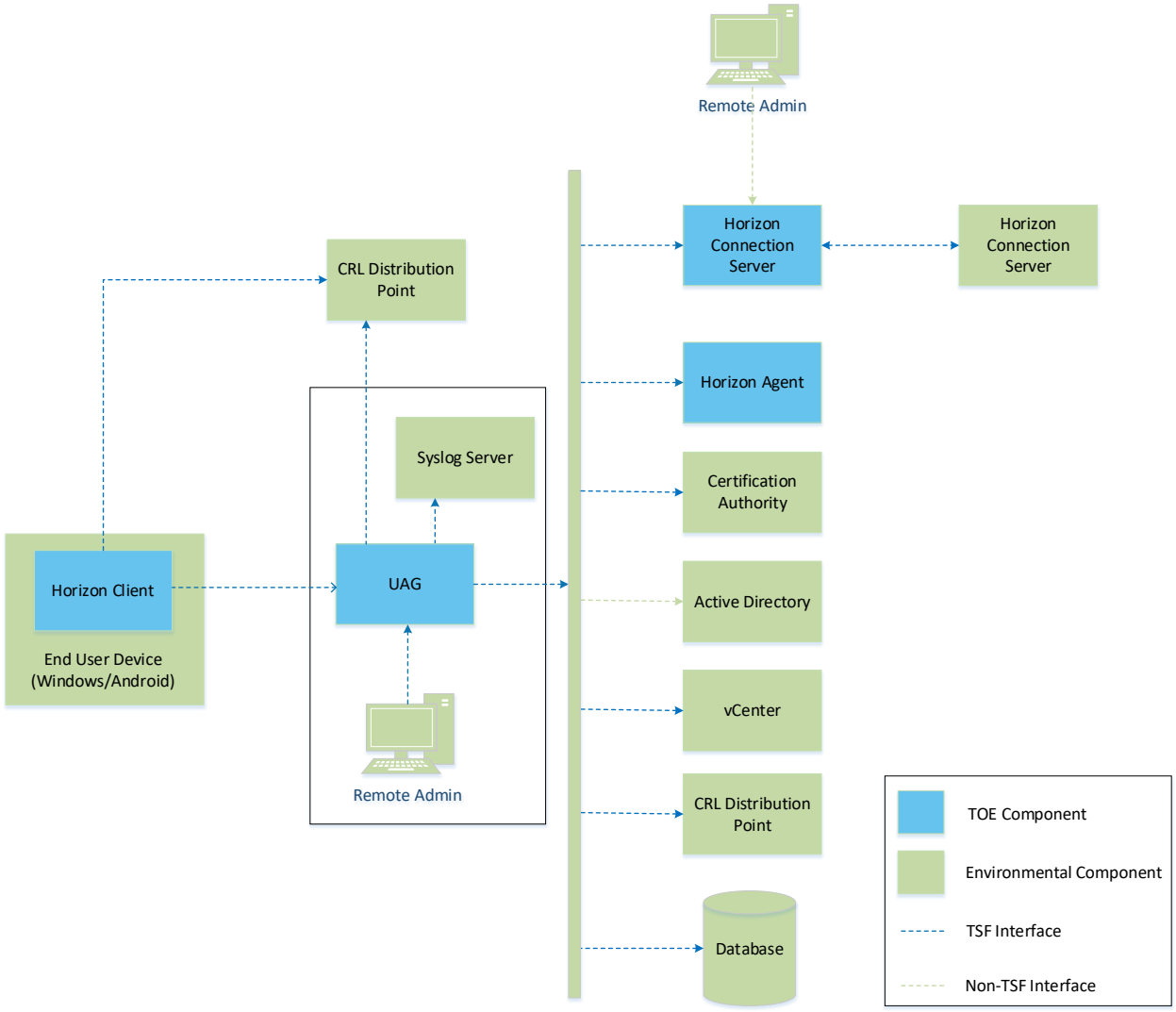

Figure 1: VMware Horizon Evaluated Configuration

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

- TCP/443: initial UAG connectivity (TLS client with mutual authentication)
- TCP/443: Blast connection to UAG (TLS client with 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 Client users.

2.3 TOE Components

The TOE consists of the Horizon Client application. In the evaluated configuration, the application is installed on 64-bit Windows 10 or higher, or Android 11. The tested configuration for the evaluation used Windows 10 and Android 11.

For Windows, other platform requirements are specified in the Horizon Client for Windows documentation under "System Requirements and Setup for Windows-Based Clients" at https://docs.vmware.com/en/VMware-Horizon-Client-for-Windows/2209/horizon-client-windows-installation.pdf. Note that this documentation references PCoIP and RDP, which are out of scope in favor of VMware Blast per section 1.3. Additionally, the underlying OS platform must be configured into FIPS mode. Guidance for this can be found under "Enabling FIPS Mode in the Windows Client Operating System" in https://docs.vmware.com/en/VMware-Horizon-Client-for-Windows/2209/horizon-client-windows-installation.pdf. Additionally, the evaluated configuration requires the use of smart cards for authentication, so the guidance referenced under "Smart Card Authentication Requirements" in the same document must also be followed.

For Android, system requirements can be found under "Setup and Installation" at https://docs.vmware.com/en/VMware-Horizon-Client-for-Android/2209/horizon-client-android-installation.pdf. Note that this documentation references PCoIP, which is out of scope in favor of VMware Blast per section 1.3. Additionally, the evaluated configuration requires the use of smart cards for authentication, so the "Smart Card Authentication Requirements" guidance in the referenced section must be followed.

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	Used for authentication and authorization of VMware Horizon Client users.
VMware Horizon Agent	Used to serve content from a remote host to a VMware Horizon Client.
Certificate Authority	Used to manage the generation, issuance, and revocation of X.509 certificates used for authentication and secure communications.

Table 1: Supporting Environmental Components

2.5 Installation of the TOE

2.5.1 Obtaining Software

2.5.1.1 Android

The Horizon Client software is downloaded from the Google Play store. The application is identified as “VMware Horizon Client” and uses the following icon:

2.5.1.2 Windows

The Horizon Client software can be downloaded directly from the VMware site at https://customerconnect.vmware.com/en/downloads/info/slug/desktop_end_user_computing/vmware_horizon_clients/horizon_8.

2.5.2 Installing or Updating Software

2.5.2.1 Android

The installation process for the Android version of the software is identical to that of other Android applications. Search for VMware Horizon on the Google Play store, download it, and simply tap the downloaded application.

Once installed, updates to the application are made automatically by the platform.

After the software has been installed, it is necessary to configure the client to be in Common Criteria Mode. The steps for doing this are as follows:

1. Tap the **Settings** (gear) icon in the upper right corner of the Horizon Client window.
2. Tap **Connection Settings** and then tap **Security Options > Advanced Security Options**.
3. Under **Advanced Security Options**, deselect Use Default Settings and select **Enable Common Criteria Mode**.
4. Click OK. The changes will take place on the next connection.

2.5.2.2 Windows

Note: prior to installation, the host operating system must be placed into a FIPS compliant mode of operation. Instructions for doing this can be found in section 2.3 of this guide. The option to enable FIPS-compliant cryptography when installing the product will not be selectable unless this has been done as a prerequisite step. The use of FIPS compliant cryptography is required for the product to be placed into its evaluated configuration; the use of other cryptographic settings was not evaluated or tested.

To install the Windows application, apply the guidance that is found under “Install Horizon Client for Windows” in https://docs.vmware.com/en/VMware-Horizon-Client-for-Windows/2209/horizon-client-windows-installation.pdf

Note that “Custom installation” must be selected so that the “Enable FIPS-compliant cryptography” option can be chosen during the installation process. Other installation options are non-interfering with respect to the claimed security functionality and can be chosen freely.

Once installed, the application can be configured to check for updates to itself at a specified location. Refer to VMware guidance under “Update Horizon Client Online” at https://docs.vmware.com/en/VMware-Horizon-Client-for-Windows/2209/horizon-client-windows-installation.pdf for instructions on configuring the update process.

2.5.3 Verifying Software

2.5.3.1 Android

The Android installer, when downloaded from the Google Play Store, is signed by Google. Integrity of the installer is checked by the mobile device at installation time; a failed integrity check will prevent installation of the application.

To check the version of the currently installed application, select the “About VMware Horizon Client” option under the gear dropdown menu.

2.5.3.2 Windows

The Windows 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 check the version of the currently installed application, select the “About VMware Horizon Client” option under the horizontal dots dropdown.

2.5.4 Initial Connectivity

Initial connectivity to a remote server is performed by following the steps outlined in the Connect to a Remote Desktop or Published Application section of the VMware Horizon Client User Guide (this section exists in both Windows and Android documentation). The only user configuration that may be necessary for this is to specify the server host to connect to. Other settings are configured administratively on the server side and cannot be modified using the client.

2.6 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.

2.7 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 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.

3.1 General Application Usage

3.1.1 Required System Resources

To make full use of Horizon Client features, the application requires use of the following system resources and hardware devices, if applicable to the system on which the application is installed:

- Network connectivity
- Camera
- Microphone
- Location services
- USB devices
- Smartcard (physical or virtual)
- Scanner
- Serial port devices
- Printer
- Speaker
- Input devices
- Monitor
- File system
- Clipboard
- System information

Access to these resources are needed because the Horizon Client is used to facilitate virtual desktop sessions, which means that a user may be authorized to access anything from individual applications to a full-fledged desktop experience on enterprise resources. File system and device access is needed to take full advantage of the resources accessed through the Horizon Client. Network access is a prerequisite to using the Horizon Client since its purpose is to access external systems. System information is used for logging purposes.

The Android version of the client requests explicit user approval to access files on the device and any connected storage volumes, camera, microphone, and location services. This approval is requested on first use of the application before any attempt to use it can be made.

The Windows version of the client requires explicit authorization for file system, location, and screen capture data. File system access is enabled under **Drive & Folder Sharing**, location service access is enabled under **Geolocation**, and screen capture access is enabled under **Calls and Sharing**, specifically the **Allow screen sharing for published applications** option.

3.1.2 Cryptographic Functionality

The cryptographic engine used by Horizon Client is OpenSSL. The installation steps described in section 2.5.2 above are necessary to place this cryptographic engine into the state required by the evaluated configuration. No other cryptographic engines or configuration was used during the evaluation of the TOE.

3.2 TLS Configuration

3.2.1 Configuring Client Authentication

The evaluated configuration for the Horizon Client requires connections to the UAG to use mutual authentication. It is therefore necessary to configure TLS client authentication, which uses a smart card as the source of the X.509 client certificate. Instructions for doing this for each platform version of the application are listed below.

Note that the evaluated configuration requires the use of RSA client certificates with key size of 2048 bits or greater.

3.2.1.1 Android

The Android client supports the use of virtual smart cards so that a physical card reader or token does not need to be connected to the Android device. To create a virtual smart card on an Android device, follow the steps outlined in VMware guidance under "Create a Virtual Smart Card" at https://docs.vmware.com/en/VMware-Horizon-Client-for-Android/2209/horizon-client-android-installation.pdf.

After the virtual smart card is created, an administrator must pair it with smart card middleware through Active Directory configuration. To do this, follow the steps outlined under "Pair a Virtual Smart Card with Smart Card Middleware" at https://docs.vmware.com/en/VMware-Horizon-Client-for-Android/2209/horizon-client-android-installation.pdf. Note that this is configured on the Active Directory system; no configuration of the Horizon Client or the system on which it is installed is required for this step.

3.2.1.2 Windows

VMware Horizon Client supports both physical and virtual smart card authentication. All smart card configuration is done external to the application; the Horizon Client will support the authentication mechanism configured on its host system.

Sample Microsoft guidance for configuration of a virtual smart card can be found at https://docs.microsoft.com/en-us/windows/security/identity-protection/virtual-smart-cards/virtual-smart-card-get-started.

3.2.2 Configuring TLS Settings

The evaluated configuration for the Horizon Client uses only TLS 1.2 with only one cipher suite, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. The default configuration of the application supports a more permissive set of TLS connection settings, so it is necessary to configure a restriction of this in order for the product to be in its evaluated configuration. Note

that the supported cryptographic algorithms and key strengths are configured implicitly by defining the supported TLS cipher suite.

3.2.2.1 Android

To configure the supported TLS versions and cipher suites on Android, refer to the guidance under "Configure Advanced Security Options" at https://docs.vmware.com/en/VMware-Horizon-Client-for-Android/2209/horizon-client-android-installation.pdf to do the following:

- Disable TLS 1.1: ensure TLS 1.1 is deselected and TLS 1.2 is selected in the security protocol list
- Configure the cipher control string to be ECDHE-RSA-AES256-GCM-SHA384
- Set the signature algorithms to RSA+SHA384
- Set the supported groups to P-384

3.2.2.2 Windows

The supported TLS versions and cipher suites on Windows can be configured via group policy or the Windows registry.

To apply TLS configuration settings via group policy, download the Horizon GPO Bundle from the VMware Customer Connect site at https://customerconnect.vmware.com/downloads/details?downloadGroup=HZ-2212-STD&productId=1392&rPId=99630. Then, configure the following GPOs:

- Configure SSL protocols and cryptographic algorithms
    - Set SSL protocols and ciphersuite to TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384
    - Set SSLSignatureAlgorithms to RSA-SHA384
    - Set SSLSupportedGroups to P-384

Alternatively, these settings may be applied directly through registry configuration. Information on configuring Horizon Client settings through the registry is found under "Using the Windows Registry to Configure Horizon Client" under https://docs.vmware.com/en/VMware-Horizon-Client-for-Windows/2209/horizon-client-windows-installation.pdf. The following registry settings are applicable to TLS configuration:

- HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Client\Security\SSLCipherList
    - TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384
- HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Client\Security\SSLSignatureAlgorithms
    - RSA+SHA384
- HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Client\Security\SSLSupportedGroups
    - P-384

3.2.3 Configuring X.509 Validity Settings

The evaluated configuration of the Horizon Client requires server certificates to be validated against a certificate chain terminating with a trusted root CA, having the certificate identity be validated through thumbprint verification, and through configuring whether or not a certificate with an undetermined revocation status is assessed as valid. Guidance for configuration of this behavior is as follows:

3.2.3.1 Android

To install a CA certificate on the Android device, do the following:

- Download the certificate
- Tap Settings > Biometrics and Security > Other Security Settings
- Tap Install Device Storage
- Tap CA Certificate
- Tap through the warning and select Install Anyway
- Navigate to the storage location of the downloaded certificate, select it, and tap Done

The handling of certificates with undetermined revocation status is configured through Security Settings > Security Options. In Common Criteria mode, the available options are "Will not connect to servers when the server certificate is revoked or unable to determine revocation status" and "Will not connect to servers when the server certificate is revoked." In the latter case, certificates with undetermined revocation status are accepted if they are otherwise valid.

The validation of certificate chains and identity data is also configured through Security Settings > Security Options. Select "PKI and Thumbprint Verification" to validate both the certificate chain and reference identifier. The reference identifier is the DNS name of the server contained in the SAN of the certificate; this is checked automatically when PKI and Thumbprint Verification is enabled.

3.2.3.2 Windows

Configuring the Horizon Client into FIPS mode ensures that the identity of server certificates is always checked to validate that the certificate issuer is a trusted CA. This setting is not configurable. To ensure that any server certificate is recognized as valid, ensure that the Windows Certificate Store is configured to have the signing CA of the server certificate be recognized as a trust anchor.

To configure the restrictive manner to handle certificates with undetermined revocation status, an administrator may configure the group policy setting for "Strict certificate revocation check," which is documented in Table 3-5 of https://docs.vmware.com/en/VMware-Horizon-Client-for-Windows/2209/horizon-client-windows-installation.pdf. When disabled, a certificate with undetermined revocation status that is otherwise valid is accepted. When enabled, a certificate with undetermined revocation status is presumed to be invalid.

To apply X.509 configuration settings, download the Horizon GPO Bundle from the VMware Customer Connect site at https://customerconnect.vmware.com/downloads/details?downloadGroup=HZ-2212-STD&productId=1392&rPId=99630. Then, configure the following GPOs:

- Do not check certificate revocation status
    - Set to disabled (note that this is the default setting)
- Strict certificate revocation check
    - Set to either Enabled or Disabled, based on desired behavior as described above
- Protocol connection certificate verification mode
    - PKI & Thumbprint. The reference identifier is the DNS name of the server contained in the SAN of the certificate; this is checked automatically when PKI and Thumbprint Verification is enabled.

The strict certificate revocation check setting can also be configured in the registry, using the Boolean HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Client\Security\StrictCertRevocationCheck setting.

Within the application itself, the certificate checking mode can also be configured through the Settings (gear icon) > SSL Configuration. Specify “Never connect to untrusted servers” as the certificate checking mode, and the “Thumbprint Verification” and “PKI Verification” options in the protocol connection certificate checking mode.