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

Guidance Supplement

VMware Horizon Agent 8 2209 (Horizon 8.7)

Common Criteria (CC) Evaluated Configuration Guidance

Document Version: 1.0
Document Date: May 17, 2023

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	May 17, 2023

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose

This document describes the operational guidance and preparative procedures for VMware Horizon Agent (referred to throughout this document as “Horizon Agent”), 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 and Upgrade
- Horizon Overview and Deployment Planning

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

- 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 should be disabled as part of placing the product into its evaluated configuration:

- Tunnel Channel – The Horizon Agent for Windows supports an HTTPS channel that can be used for some communications with a remote Horizon Client. 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 for Windows. In the evaluated configuration, PCoIP is disabled on the Horizon Agent so only the Blast channel is used (Linux Agents only support Blast).
- 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 in the claimed Protection Profile 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.

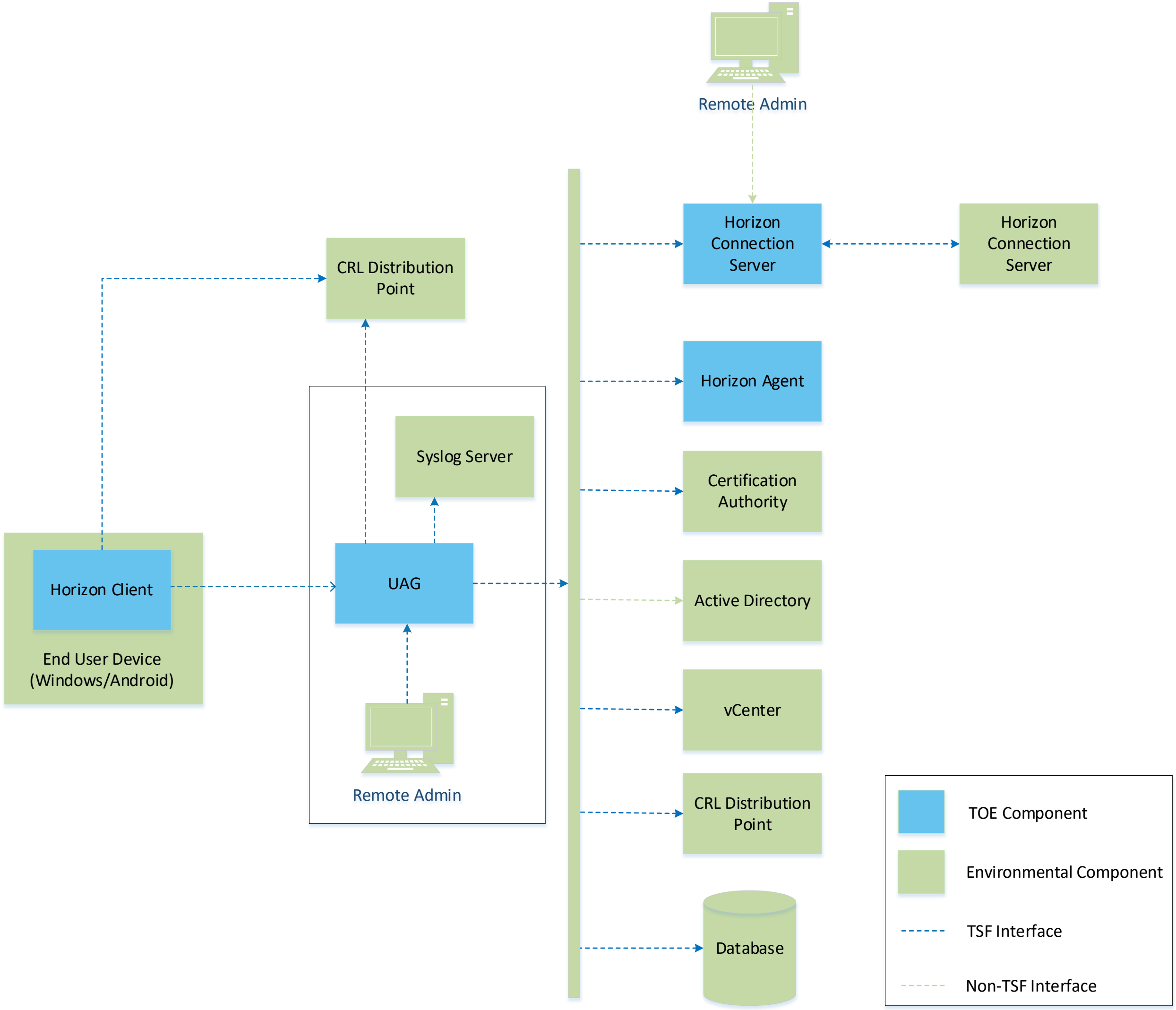

Figure 1: VMware Horizon Evaluated Configuration

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

- TCP/4001: Java Message Service (JMS) channel for communications with Connection Server
- TCP/22443: Blast connection from UAG (TLS server 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.

2.3 TOE Components

The TOE consists of the Horizon Agent application. In the evaluated configuration, the application is installed on any of the following:

- Windows
    - Windows 10
    - Windows Server 2019
- Linux
    - Red Hat Enterprise Linux 8.0 or higher

The tested configuration used for the evaluation is Windows Server 2019, Windows 10, and Red Hat Enterprise Linux 8.0, all virtualized on VMware ESXi 7.0.

Additionally, the underlying OS platform must be configured into FIPS mode. Microsoft guidance for configuration of this for Windows can be found at https://docs.microsoft.com/en-US/windows/security/threat-protection/fips-140-validation. VMware guidance for configuration of this for Linux can be found in the "Configure a FIPS-compliant Virtual Machine" section of Linux Desktops and Applications in Horizon.

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 Client	End user application that requests content to be served to it by VMware Horizon Agents.
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 Preparing the Operational Environment

The Horizon Agent runs on a virtual machine within a VMware vSphere environment. Protection of data at rest is addressed through the use of Virtual Machine Encryption, which is documented in vSphere guidance at https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-E6C5CE29-CD1D-4555-859C-A0492E7CB45D.html.

2.5.1.1 Linux

Configuration of the underlying OS platform is performed by following the procedures listed under "Create a Virtual Machine and Install Linux" and "Prepare a Linux Machine for Remote Desktop Deployment" in the Linux Desktops and Applications in Horizon guide. Additionally, ensure that the `libappindicator-gtk3` package is installed on the platform. Specific configuration for resource pooling (instant-clone vs full-clone vs manual) is dependent on individual customer deployment and does not affect the behavior of the Horizon Agent software.

Note: since the evaluated configuration of the Horizon Agent is for deployment in the same vSphere instance as the Connection Server, settings for "managed mode" should be applied.

2.5.1.2 Windows

Configuration of the underlying OS platform is performed by following the procedure listed under "Creating and Preparing a Virtual Machine for Cloning" in the Windows Desktops and Applications in Horizon guide. If using a Windows Server platform, ensure that the "Install Desktop Experience on Windows Server" guidance is followed.

Additionally, the following configuration steps are needed to disable unused services on ports 32111, 4172, and 9427:

- Set registry key HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager\EnableSocketListener to 'false'
- Remove the following registry keys:
  - HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration\Listeners\FRAMEWORKCHANNEL
  - HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration\Listeners\VDPSERVICECHANNEL
  - HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\PCoIP\AgentDLL
- Disable the 'VMware Horizon View PCoIP Secure Gateway' service
- Remove or disable the following firewall rules:
  - VMware Horizon View Device and Multimedia
  - VMware Horizon View Framework
  - VMware PCoIP Server (both UDP and TCP)
  - VMware Horizon Agent (Ext-PCoIP-TCP-In)
  - VMware Horizon Agent (Ext-PCoIP-UDP-In)
  - VMware Horizon Agent (Int-PCoIP-UDP-In)
- Reboot the system

2.5.2 Obtaining Software

The Horizon Agent software can be obtained from https://my.vmware.com/web/vmware/downloads. Both the Windows and Linux versions of the software can be found here. To download the software, it is necessary to create an account on VMware Customer Connect.

Note that there are multiple editions of the Horizon Agent 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 or Updating Software

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 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.

2.5.3.1 Linux

Installation of the Linux Agent is done by following the procedure listed in the "Install Horizon Agent for Linux using the digitally signed RPM installer" section of the Linux Desktops and Applications in Horizon guide. Note that the optional features in step d of this procedure are not within the scope of the evaluated configuration. The application must be installed with root privileges in order to function properly.

Following initial installation, ensure that FIPS mode is enabled using the `ViewSetup.sh` script with the "-f yes" flag set and that a PKI certificate is installed for the agent by following the procedure listed in the "Configure a FIPS-compliant Linux Virtual Machine" section of the Linux Desktops and Applications in Horizon guide.

2.5.3.2 Windows

Installation of the application can be performed by following the procedures in the "Install Horizon Agent on a Virtual Machine" section of the Windows Desktops and Applications in Horizon guide. Note specifically that the option to enable FIPS mode must be selected.

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 check the version of the installed application, the following steps should be performed:

- Linux: run the command `cat /usr/lib/vmware/viewagent/Product.txt` (assuming the default installation folder was used; modify this command as needed if it was not).
- Windows: navigate to Apps and Features in Windows; the product and its version will appear in the list of installed applications.

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

Regardless of whether the Windows or Linux Agent is being used, the communications channel from the Agent is configured using the Connection Server and UAG. These configurations ensure the use of Blast TCP to carry traffic to and from Horizon Clients.

3.1.1 Required System Resources

To make full use of Horizon Agent 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
- Audio/video interface
- System logs
- File system
- Clipboard

System logs are used by Horizon Windows Agent to record status and usage information to the local operating system. Other system functionality is used as needed to allow a Horizon Client user to interact with the functionality of the Horizon Agent system as part of the virtual desktop functionality that is served to the Horizon Client.

3.1.2 JMS Connectivity

JMS connectivity between the Horizon Agent and the Horizon Connection Server is configured through the Connection Server itself. No separate configuration steps are needed for the Horizon Agent. As part of JMS, the Horizon Agent generates 3072-bit RSA keys; no separate configuration is needed for this.

3.1.3 Cryptographic Functionality

The cryptographic engines used by Horizon Agent are OpenSSL and Bouncy Castle. The installation steps described in section 2.5.3 above are necessary to place these cryptographic engines into the state required by the evaluated configuration. No other cryptographic engines or configuration was used during the evaluation of the TOE.

3.1.4 Remote Management

The Horizon Agent has several security-relevant management functions. Note that no direct management interface exists for the Horizon Agent; this functionality is managed through the environmental Horizon Connection Server.

- Activation of certificate: Sets a new TLS certificate for the Agent (e.g. in the case where its existing certificate is about to expire)
    - This is done through the vdmutil utility, specifically through the `--refreshDesktopCertificates` command option.
    - For more information on the use of vdmutil, refer to “Using the vdmutil Utility to Configure the JMS Message Security Mode for VMware Horizon 8” in Horizon Security.
- Enabling/disabling Horizon Agent: Sets whether or not the Horizon Agent is running.
    - This is done through the Horizon Console management interface of the Horizon Connection Server.
    - In the Horizon Console, select **Inventory** > **Desktops**.
    - Select a desktop pool and change the status of the pool using the dropdown menu.
    - Click **OK**.
    - If the Horizon Agent is assigned to affected desktop pool, it will be disabled or enabled based on the setting that was applied.
- Termination of active session: Logs a connected Horizon Client user out of their Agent session.
    - This is done through the Horizon Console management interface of the Horizon Connection Server.
    - In the Horizon Console, navigate to where the active session is located. This can be done through the following ways:
        - By system: Select **Inventory** > **Desktops** or **Inventory** > **Farms** and click the **Sessions** tab for the desktop pool or farm, or select **Settings** > **Registered Machines** and view the **Sessions** column for the individual machine on which the Agent is running.
        - By session: Select **Monitor** > **Sessions**.
        - By user: Select **Users and Groups**, select the user or a group to which that user belongs, and click on the **Sessions** tab.
    - Select a session.
    - Select **Logoff Session**.
    - Click **OK**.
- Generation of message box prompt: Generating a pop-up notification with predetermined text that the TOE will display to the Horizon Client user who has an active session on the Agent system.
    - This is done through the Horizon Console management interface of the Horizon Connection Server.
    - In the Horizon Console, navigate to where the active session is located. This can be done through the following ways:
        - By system: Select **Inventory** > **Desktops** or **Inventory** > **Farms** and click the **Sessions** tab for the desktop pool or farm, or select **Settings** > **Registered Machines** and view the **Sessions** column for the individual machine on which the Agent is running.
        - By session: Select **Monitor** > **Sessions**.

        - By user: Select **Users and Groups**, select the user or a group to which that user belongs, and click on the **Sessions** tab.
    - Select a session.
    - Select **Send Message**.
    - Enter the message along with its label (Info, Warning, or Error).
    - Click **OK**.
- Configuration of log level: setting the log level to determine which events get audited (Windows Agent only).
    - The log level is configured using the vdmadmin command on the Connection Server.
    - This is done by following the steps listed under "Configuring Logging in Horizon Agent Using the -A Option" in Horizon Administration.

3.2 TLS Configuration

3.2.1 Configuring TLS Settings

The evaluated configuration for the Horizon Agent uses only TLS 1.2 with two cipher suites, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and 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 suites. Additionally, no separate configuration is required to ensure that the supported curves used for key generation (P-256/384/521) are used.

Note that the Windows Agent supports TLS session resumption based on both session IDs and session tickets; this behavior is enforced by default and no configuration is used for this. The Linux Agent does not support TLS session resumption.

3.2.1.1 Linux

TLS version and cipher suite information are configured through the /etc/vmware/viewagent-custom.conf configuration file. The following settings must be applied:

- SSLCiphers: !kECDH+AESGCM:RSA
- SSLProtocols: TLSv1_2

3.2.1.2 Windows

TLS version and cipher suite information are configured through the Windows Registry. The following keys must be configured:

- HKLM\Software\VMware, Inc.\VMware VDM\Agent\Configuration\ClientSSLSecureProtocols: TLSv1.2
- HKLM\Software\VMware, Inc.\VMware VDM\Agent\Configuration\ClientSSLCipherSuites:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

3.2.2 Configuring X.509 Certificates

X.509 certificates are used for inbound TLS connectivity. Listed below are the instructions for configuring this functionality.

Note that VMware Blast needs to use a CA-signed certificate. The root signing certificate must be deployed on the Unified Access Gateway used to access the Horizon Agent.

Note that in the evaluated configuration, RSA certificates with a minimum key size of 2048 bits must be used.

3.2.2.1 Linux

The certificate and private key files must be in PEM format. Once this has been done, the **DeployBlastCert.sh** script must be run with root permissions to place these materials into the Java Keystore. For example:

```
sudo /path/to/DeployBlastCert.sh -c /path/to/xxx.crt -k
/path/to/xxx.key
```

To enable protection of stored credentials, run the ViewSetup.sh script using the -j flag with the desired password. Refer to Table 5-1 of Linux Desktops and Applications in Horizon.

3.2.2.2 Windows

Any root or intermediate CAs used to sign the certificate are installed into the Windows Certificate Store using the Windows OS.