PCoIP Zero Client Firmware Version 5.5.1

Release Notes

Current Version: 5.5.1
Release Date: 2017-10
Previous Version: 5.4.1

Contents

Release type and definition

PCoIP Zero Client Firmware v5.5.1 is a firmware for Tera2 PCoIP Zero Clients and not for PCoIP Remote Workstation Cards.

This release is a feature release with functional changes and bug fixes over release 5.4.1. These release notes provide a summary of key feature additions, compatibility notes, resolved issues, and known issues for this release.

Current Version

5.5.1

Previous version

5.4.1

What's new in this release

The following are the new features in this release:

Gemalto IDPrime MD smart card

The following Gemalto IDPrime MD smart cards are supported during VMware Horizon View session authentication:

- IDPrime MD 830
- IDPrime MD 840
- IDPrime MD 3810

PIVKEY smart card

PIVKEY C980 smart cards are supported on zero clients during VMware Horizon View authentication.

HID OMNIKEY 5421 smart card reader

HID OMNIKEY 5421 smart card reader is supported during VMware Horizon View pre-session authentication.

X.509 User name hint

Zero client supports VMware Horizon View smart card user name hint feature. This feature allows a user with multiple accounts to choose a user account to login using a smart card. The feature was implemented in VMware Horizon View v7.0.2. For more information, see http://pubs.vmware.com/Release_Notes/en/horizon-7-view/horizon-702-view-release-notes.html.

SNMP sysName

When you query the zero client using SNMP, the sysName.0 MIB object defined in SNMPv2-MIB returns the zero client's FQDN.

Updated time zones

The IANA time zone database included in the zero client firmware is updated to 2016j. This ensures that the time zones used on the zero client matches the current international standards.

Zero Clients does not send event logs to the management console

The zero client no longer pushes the event logs to the Endpoint Manager. You can see Management Console v2.4.0 and later version can view the static log information in the log viewer accessed from the Endpoint Details page.

Administrative Web Interface certificate is a 3072-bit RSA key

The certificate by the Administrative Web Interface uses a 3072-bit RSA key.

Important notes

Wyse Device Manager

- Wyse Device Manager v5.7.2 and v5.7.1 support 4.x, 5.2.2, 5.4.1, and 5.5.1 versions of firmware.
- Earlier versions of Wyse Device Manager support only 4.x. If you are using earlier versions of Wyse Device Manager, then upgrade the Wyse Device Manager to version 5.7.1, and proceed with the firmware update.

Teradici console

- PCoIP Management Console v2.x cannot detect or manage devices on firmware versions prior to v5.0. If you upgrade from firmware v4.x, then either the zero client AWI or PCoIP Management Console v1.10.3 - v1.10.8 must be used to upgrade the zero client to firmware v5.x.
- Zero clients on firmware v5.x can only be managed by PCoIP Management Console v2.0 or later. PCoIP Management Console v1.x cannot detect or manage devices on firmware v5.0 or later.
- Zero clients upgraded to firmware 5.x from a 4.x release must first be upgraded to firmware v4.7 or v4.8.
- The file contains .all extension for use by the Administrative Web Interface (AWI), and a file identified by the .pcoip extension for use by PCoIP Management Console v2.x.
- The .pcoip file contains zero client firmware v5.5.1 for Tera2 PCoIP Zero Clients only.

Support platforms

This release supports the following platforms:

- Wyse 5030 zero client for VMware and AWS
- Wyse 5050 AIO thin client for VMware and AWS
- Wyse 7030 zero client for VMware and AWS

Upgrade scenarios

The following are the different upgrade scenarios for this product:

- Upgrade path from 5.2.2 or 5.4.1 to 5.5.1 (ThreadX 5.x) using Wyse Device Manager.
- Upgrade path from 4.8 (ThreadX 4.x) to 5.5.1 (ThreadX 5.x) using Wyse Device Manager.
- Upgrade path using Teradici Console.

   Customers who are using Teradici Console need to follow the Teradici instructions available at Teradici Knowledge Base.

Support matrix

Compatibility Notes	Workstation	VMware Horizon	Amazon WorkSpaces	Teradici Cloud Access Platform
This release is compatible with VMware Horizon 7.1. It is also compatible with one major release of Horizon prior to this. Other versions of Horizon may also be compatible, but will need to be verified in your specific deployment environment.		✓		
PCoIP Connection Manager for Amazon WorkSpaces 1.0.2 or higher is required in order to connect to Amazon WorkSpaces. Use of Amazon WorkSpaces with hourly billing requires the PCoIP Connection Manager for Amazon WorkSpaces 1.0.5 or later.			✓	
Management requires a compatible endpoint manager such as PCoIP Management Console release 2.0 or later.				
While mixed firmware release operation is not generally supported, this firmware release has been tested to work with Remote Workstation Cards on Remote Workstation Card firmware 4.9.0. **Note:** Using zero clients on this firmware release to connect to Remote Workstation Cards may require you to use both versions of PCoIP Management Console: version 2 to manage the zero clients, and version 1.x to manage Remote Workstation Cards until such time as there is a Remote Workstation Card firmware release that is supported by PCoIP Management Console 2.0 or higher.	✓	✓		
This release has been tested against Imprivata OneSign 5.2 with VMware Horizon 7.1.		✓		
This release has been tested with the Leostream Connection Broker version 8. It is not compatible with earlier versions of the Leostream Connection Broker. **Note:** After upgrading from PCoIP Zero Client Firmware 4.x to 5.x, the session connection type for the zero client must be	✓	✓		✓

changed to PCoIP Connection Manager, with the address of the Leostream Connection Broker. Also ensure the Leostream Connection Broker has had 'Enable TLSv1.1 protocol' enabled in the Connection Broker Security Options section of the **Connection Broker > System > Settings** page.

Supported browsers are Firefox, Chrome, Internet Explorer 11, and Microsoft Edge. Versions of the browsers tested are those that were available prior to release.

Web browsers must support TLS 1.1 or higher to connect to the administrative web interface (AWI).

Known issues

SIPR token authentication fails with multiple certificates on smart card

The zero client fails to complete SIPR token smart card authentication against VMware Horizon View when the smart card contains more than two certificates.

Workaround: Ensure that the card only two certificates.

Change in button timing for entering manual recovery

With the firmware v5.2.1, the power button sequence to boot a zero client from powered down into the recovery image is:

1. Press power button once to turn on the client and wait for one second
2. Press the power button three times.
3. Zero client boots into the recovery image

From firmware v5.0.0 to v5.2.0 it was possible to press the power button three times immediately after turning on the zero client. This is no longer supported.

Mouse cursor does not work after zero client reboots

The On-Screen Display's mouse cursor does not work for a few seconds after a zero client reboot when a web browser is connected to the zero client's Administrative Web Interface.

Zero Client is not able to connect using IPv6 VMware Horizon View when DHCPv6 is not available

If the zero client is configured for IPv6, and it cannot connect a DHCPv6 server, it will be unable to connect to a desktop when brokered by an IPv6 VMware Horizon View Connection Server. The zero client displays the message **'CONFIGURATION_ERROR - IPv6 capability required: Your VMware Horizon View Client addressing configuration is not compatible with this View Server...**'

Security scanners may report zero client to be susceptible to CVE-2004-0230

Security scanners may report that the zero client is susceptible to CVE-2004-0230. This CVE exists in TCP stacks in devices that implement the Border Gateway Protocol. While this is a significant issue for routers that implement the Border Gateway Protocol, it is not a significant issue for zero clients.

Mouse wheel problem occurs with Belkin Advanced Secure Keyboard/Mouse Switch

Mouse wheel scroll-down does not work while in a PCoIP session. This occurs when the mouse is connected to a zero client through a Belkin Advanced Secure Keyboard/Mouse (KM) Switch. This problem has been observed while using KM models F1DN102K, F1DN104K, and F1DN108K.

Workaround: On Tera2 Zero Clients, bridge the KM and enable the Force Local Cursor Visible on the zero client **Configuration > USB Administrative Web Interface**.

Zero client fails to resolve FQDN with a label that starts or ends with an underscore

A zero client will not resolve an FQDN that begins or ends with the underscore character (for example, **_myhost.teradici.local).**

Restrict Proximity Card setting does not work with VMware Horizon RDSH

The Restrict Proximity Card setting does not work with VMware Horizon RDSH sessions when set to disabled.

Enumeration failures with Western Digital portable hard drives

Western Digital Passport external portable hard drives connected to a zero client internal hub may fail to enumerate.

Workaround: Connect the drive to a zero client root hub port, or connect the drive to an external hub that is connected to the zero client, then restart the PCoIP session and disconnect/reconnect the drive.

Manual IPv6 gateway address is overwritten on reset

Although the IPv6 Gateway address is displayed as an editable field on the zero client Administrative Web Interface (AWI), changes to this field are not respected by the zero client firmware. Instead, the IPv6 gateway is determined using IPv6 Router Advertisement.

Zero client AWI cannot be accessed when IPv6 Link Local Address is entered in the IPv6 Manual address field

Configuring a zero client in IPv6 mode to manual addresses and setting the IPv6 Manual Address to the same value as the Link Local Address will make the zero client Administrative Web Interface (AWI) unreachable.

Workaround: Use the On-Screen Display (OSD) to reconfigure the IPv6 address settings.

Evoluent VerticalMouse 4 does not work when connected behind a hub during active session

The Evoluent VerticalMouse 4 device does not work if the device is bridged and the user connects the device to a zero client behind a hub (external or built-in hub port) while a session is active.

Workaround: Avoid plugging the device into a hub port while a session is active or connect the device to a zero client root port. Alternatively, disconnect and reconnect the session after plugging the mouse into a zero client behind a hub.

Elo Touch monitor may lose calibration in OSD after used in bridged mode with certain Elo Multi-Touch drivers

An Elo Touch monitor connected to a zero client may lose its calibration settings and be unstable in the On-Screen Display (OSD) when the zero client connects to a PCoIP host running certain versions of the Elo Multi-Touch driver, and when the monitor is calibrated using Elo Multi-Touch driver on the host.

Workaround: Use version 5.5.3 of the Elo Multi-Touch driver. This issue has not been observed with this driver version.

Disconnecting one display resets Preferred Resolution Override on all displays

When multiple displays have Preferred Resolution Override applied to them, disconnecting one display will clear the override for all displays.

RDR-7L82AKU smart card reader does not work with OneSign 4.9 SP1 HF11 and latest version

RFIDeas RDR-7L82AKU proximity card readers do not detect cards after logging in to a virtual desktop running Imprivata OneSign 4.9 SP1 HF11 or latest version.

Workaround: Revert Imprivata OneSign installation to a version older than 4.9 SP1 HF11.

Gemalto IDCore 3020 smart cards is missing correct driver in Windows 7

By default, Gemalto IDCore 3020 smart cards work in pre-session. However, the card does not work while in-session for Windows 7 virtual desktops.

Workaround: Install the correct driver from a default Windows 7 installation:

1. From the zero client administrative web interface, bridge the smart card reader.
2. Without the smart card inserted, log in to the virtual desktop with username/password.

3. Insert the smart card. Windows 7 should recognize the smart card and reader and automatically install the correct drivers.

4. Log off Windows to disconnect the session.

5. From the zero client administrative web interface, remove the bridge configuration for the smart card reader.

6. Log in with the smart card. The smart card should be fully accessible.

OneSign cannot authenticate after changing Session Connection Type

After changing a zero client's Session Connection Type from View Connection Server + Kiosk to View Connection Server + OneSign, the Zero Client is unable to negotiate a PCoIP session with VMware View using OneSign authentication.

Workaround: Restart the zero client.

After display is turned off, screen does not wake up by pushing zero client button

When the On-Screen Display (OSD) Screensaver timeout expires, it will turn off the display after the end of a PCoIP session brokered by a PCoIP Connection Manager. Clicking the zero client's physical button does not wake the display.

OSD cursor briefly stops responding to mouse input

The On-Screen Display (OSD) cursor stops responding to mouse input for a few seconds after pressing the Apply button on the AWI USB Permissions page, or while loading the AWI Attached Devices page. It will behave as expected shortly after.

Disconnecting a session with auto-reconnect enabled causes an alert dialog

With the auto-reconnect feature enabled, users may see an alert dialog briefly on screen before the PCoIP session is reconnected. The message shown is "Unable to connect (0x1001). Please contact your IT administrator." This message can be safely ignored.

Switching between DVI and DisplayPort connectors may cause screen to go blank on HP Z27i displays

HP Z27i displays connected to a zero client's DisplayPort connectors may not show the remote desktop content when the zero client starts a PCoIP session to a workstation access card, and the card's previous session was from a zero client with displays attached to its DVI ports.

Temporary IPv6 addressing causes failure when connecting zero clients to any soft host

Zero clients cannot establish a connection to any soft host that has temporary IPv6 addressing enabled.

Resolved Issues

The following are the resolved issues in this release:

Zero Client connect VMware Horizon View Connection Server after resolution of VMSA-2017-0008.2

VMware changes to Horizon View to resolve VMware Security Advisory ID VMSA-2017-0008.2 resulted in a "View Connection Server error" when the zero client attempted to connect to a desktop. Zero client firmware has been updated to support the changes introduced by VMware into Horizon View 6.2.4 and latest version.

Upgrading firmware 5.4.x with AWI open no longer causes zero client to freeze

The zero client will no longer freeze if upgrading from firmware 5.5 or higher. The issue was present only in firmware 5.4.x.

In OneSign mode the zero client will abort pre-session authentication when the View Connection Server session times out

A zero client in OneSign mode may receive more than one View Connection Server address from the OneSign server. When a zero client is left at the desktop selection dialog for longer than the View Connection Server's Forcibly Disconnect User setting value (default 600 minutes) and then a desktop selection is made, the zero client will abort to the Connect dialog.

Increased smart card transaction timeout

The zero client smart card remoting feature's idle timeout has been increased from five to 20 seconds to improve compatibility with versions of Windows older than Windows 8.

Zero client event log flooded with messages in 802.1x and PoE environments

The zero client event log may have become flooded with messages that began with "RDMA2 :src_mac" when the zero client is operating in PoE (Power over Ethernet) mode or is configured to use 802.1x. This is now resolved.

SNMP disabled by default

SNMP is now disabled by default. Zero clients where the Enable SNMP setting is not explicitly configured will now have SNMP disabled and must have SNMP re-enabled by the administrator if it is to be used after firmware upgrade.

Enabled USB audio no longer causes zero client reboots

Previously, a zero client with USB audio enabled may infrequently reboot, even when audio was not playing. This issue has been fixed.

Useful links

- Tera Dell Wyse site:
  https://appservices.wyse.com/pages/serviceandsupport/support/dlOraFW.asp?which=161&model=P25/P45

  NOTE: Currently, the firmware version 5.4.1 is available on the website.

- 5.2.2 Dell Release notes:
  https://appservices.wyse.com/supportdownload/WyseZeroClients/Dell%20Wyse%20PCoIP%20Firmware%205.2.2%20Release%20Notes.pdf

- Wyse Device Manager links: http://downloads.dell.com/wyse/wdm/

- Teradici 5.4 Administrator's Guide: http://www.teradici.com/web-help/TER1504003/5.4/default.htm

- Teradici 5.3 Release notes:
  https://techsupport.teradici.com/link/portal/15134/15164/Article/2942/PCoIP-Zero-Client-Firmware-5-3-Release-Notes-15134-2942

- Teradici 5.4 Release notes:
  https://techsupport.teradici.com/link/portal/15134/15164/Article/2984/Tera2-PCoIP-Zero-Client-Firmware-5-4-Release-Notes-15134-2984

- Teradici 5.5.1 Release notes:
  https://techsupport.teradici.com/link/portal/15134/15164/Article/3150/Tera2-PCoIP-Zero-Client-Firmware-5-5-1-Release-Notes-15134-3150

- PCoIP® Management Console 2.2:
  https://techsupport.teradici.com/link/portal/15134/15164/Article/2915/PCoIP-Management-Console-2-2