



HDX Framehawk Virtual Channel

Administrator Guide

XenApp and XenDesktop 7.6 Feature Pack 3

Contents

Introduction	1
Framehawk raises the bar on user experience	1
Design considerations using Thinwire and Framehawk	2
Required Framehawk Components	3
Network considerations.....	3
Installation	4
Install the VDA update	4
Install the GPO update package	4
Configuration.....	5
To configure Citrix policy for Framehawk.....	5
Configuring NetScaler Gateway for Framehawk support.....	12
About NetScaler Gateway support for Framehawk	17
Configuring Citrix Receiver 6.0.1 for iOS to support Framehawk.....	18
Monitoring Framehawk	20
Monitoring with Citrix Director	20
Known Issues.....	21
Appendix A	
Using Framehawk with XenApp and XenDesktop 7.6 FP2.....	23
Installation - XenApp and XenDesktop 7.6 FP2 only.....	24

Disclaimer

This document is furnished "AS IS". Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix Systems, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc.

About Citrix

Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of \$3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.

Copyright © 2015 Citrix Systems, Inc. All rights reserved. Citrix, Citrix Receiver, and StoreFront are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

Introduction

XenApp and XenDesktop 7.6 Feature Pack 3 integrates Framehawk, a new ICA virtual channel extending the Citrix HDX technologies. These technologies are a set of capabilities that work together to deliver a high definition in-session user experience of virtual desktops and applications for users running Citrix Receiver. The Framehawk virtual channel optimizes the delivery of virtual desktops and applications to users on broadband wireless connections, when high packet loss or congestion occurs.

You can use Citrix Policies to implement either Framehawk or Thinwire for a set of users in a way that is appropriate for your network characteristics and is aligned with overall scalability and performance expectations. This guide shows you how.

Framehawk raises the bar on user experience

Generally, user-experience has focused on frame rate and visual quality as a basis for a positive user experience. But with this addition to the HDX family, Citrix enhances the definition to account for linearity. Users need to enjoy the experience, not be distracted by it. Under degraded network circumstances, users struggle with the “rubber band” effect that plagues all protocols. This effect includes the tapping-waiting-tapping syndrome where a user isn’t sure if the screen will respond “this time” resulting in extra errant clicks by the user, creating more and more undesirable results. Framehawk smooths out those experiences, especially under strenuous network conditions.

High-speed home Internet connections frequently exhibit performance issues, whether due to collisions with neighboring Wi-Fi signals or spectral interference from cordless phones, baby monitors and vacuum cleaner motors, among others. More and more users are connecting to hosted apps and data via 3G or 4G/LTE cellular networks, or using inflight Internet services. Others like to take advantage of public Wi-Fi hotspots while stopping for a coffee break or at hotels where congestion is a common problem.

With Framehawk, users notice a more interactive experience (a more linear echoback of characters) compared to Thinwire at high latencies.

How Framehawk maintains a smooth user experience

Think of Framehawk as a software implementation of the human eye, looking at what’s in the frame buffer and discerning the different types of content on the screen. What’s important to the user? When it comes to areas of the screen that are changing rapidly, like video or moving graphics, it doesn’t matter to the human eye if some pixels are lost along the way because they will quickly be overwritten with new data.

But when it comes to static areas of the screen, like the icons in the systray or a toolbar, or text after scrolling to where the user wants to start reading, the human eye is very fussy; a user expects those areas to be pixel perfect. Unlike protocols that aim to be technically “accurate”

from a 1's and 0's perspective, Framehawk aims to be relevant to the human being who's using the technology.

Framehawk includes a next generation QoS signal amplifier plus a time-based heat map for a finer-grained and more efficient identification of workloads. It uses autonomic, self-healing transforms in addition to data compression, and avoids retransmission of data to maintain click response, linearity and a consistent cadence. On a lossy network connection, Framehawk can hide loss with interpolation, and the user still perceives good image quality while enjoying a more fluid experience. In addition, Framehawk algorithms intelligently distinguish between different types of packet loss; for example, random loss (send more data to compensate) versus congestion loss (don't send more data since the channel is already clogged).

Framehawk's Intent Engine distinguishes between scrolling up or down, zooming, moving to the left or right, reading, typing and other common actions, and manages the communication back to the Virtual Delivery Agent (VDA) using a shared dictionary. If the user is trying to read, the visual quality of the text needs to be excellent. If the user is scrolling, it needs to be quick and smooth. And it has to be interruptible, so that the user is always in control of the interaction with the application or desktop.

By measuring cadence on the network connection (which we call "gearing", analogous to the tension on a bicycle chain), the Framehawk logic can react more quickly, providing a superior experience over high latency connections. This unique and patented gearing system provides constant up-to-date feedback on network conditions, allowing Framehawk to react immediately to changes in bandwidth, latency and loss.

Design considerations using Thinwire and Framehawk

While Thinwire has led the industry in bandwidth efficiency and is well-suited to a broad range of access scenarios and network conditions, it is TCP-based for reliable data communications and therefore must retransmit packets on a lossy or overburdened network, leading to lag in the user experience.

Framehawk is UDP based, taking a "best effort" approach at data transmission. UDP is just a small part of how Framehawk overcomes lossiness, as can be seen when comparing the performance of Framehawk with other UDP-based protocols, but it provides an important foundation to the human-centric techniques that sets Framehawk apart.

How much bandwidth does Framehawk require?

What do we mean by "broadband" wireless? It is actually a difficult question to answer precisely because it depends on a number of factors, including how many users are sharing the connection, the quality of the connection, and apps being used. For optimal performance, Citrix suggests a base of 4 or 5 Mbps plus about 150 Kbps per concurrent user. Having said that, you may find that Framehawk greatly outperforms Thinwire on a 2 Mbps VSAT satellite connection because of the combination of packet loss and high latency.

Citrix's bandwidth recommendation for Thinwire is generally a base of 1.5 Mbps plus 150 Kbps per user (for more detail, refer to XenApp/XenDesktop bandwidth [blog](#)), but at 3% packet loss you'll find that Thinwire needs much more bandwidth than Framehawk to maintain a positive user experience.

Note: Thinwire remains the primary display remoting channel in the ICA protocol. Framehawk is off by default. Citrix recommends enabling it selectively using Studio policies to address the broadband wireless access scenarios in your organization.

Required Framehawk Components

Framehawk is available as a feature for the Virtual Delivery Agent (VDA) in XenApp and XenDesktop 7.6 Feature Pack 3 (FP3). To use Framehawk, download the following FP3 components from the [Citrix download site](#):

- Workstation OS VDA 7.6.300
- Server OS VDA 7.6.300
- Group Policy Management 7.6.300
 - CitrixGroupPolicyManagement_x86.msi (for x86 machines, 32-bit OS)
 - CitrixGroupPolicyManagement_x64.msi (for x64 machines, 64-bit OS)
- Citrix Director 7.6.300
- Citrix Receiver for Windows 4.3.100 (for updating the client endpoint)

On the endpoint, you need the latest version of Citrix Receiver for Windows and iOS to use Framehawk:

- Citrix Receiver for Windows 4.3.100
- Citrix Receiver for iOS 6.0.1

Note: Framehawk was originally delivered as a hotfix with XenApp and XenDesktop 7.6 Feature Pack 2. In FP3, it is now fully integrated in the standard VDA; the installation procedures have changed as a result.

Network considerations

By default, Framehawk uses UDP ports in the range 3224-3324 which can be customized in policy. Each concurrent connection between the client and the virtual desktop requires a unique port. For multi-user OS environments, such as XenApp servers, you need to define sufficient ports to support the maximum number of concurrent user sessions. For a single user OS, such as VDI desktops, it is sufficient to define a single UDP port. Framehawk attempts to use the first defined port, working up to the final port specified in the range. This applies both when passing through NetScaler Gateway, and internal connections directly to the StoreFront server.

For remote access, a NetScaler Gateway must be deployed. By default, NetScaler uses UDP port 443 for encrypted communication between the client Receivers and the gateway. This port must be open on any external firewalls to allow secure communication in both directions. The feature

is known as Datagram Transport Security (DTLS) and is currently offered only on NetScaler Gateway, not the NetScaler Unified Gateway. For additional information, see [Configuring NetScaler for Framehawk support](#) later in this document.

Consider the following best practices before implementing Framehawk virtual channels:

- Contact your Security administrator to confirm UDP ports defined for Framehawk are open on the firewall. The installation process does not automatically configure the firewall.
- In many cases, NetScaler Gateway might be installed in the DMZ, flanked by firewalls on both the external as well as the internal side. Ensure UDP port 443 is open on the external firewall, and UDP ports 3224-3324 are open on the internal firewall if the environment is using the default port ranges.

Installation

Use the information in this section to install Framehawk using XenApp and XenDesktop 7.6 FP3.

You must install the following components in this order:

1. Install or update the VDA to XenApp and XenDesktop 7.6 FP3.
2. Apply the Group Policy Object update.

Install the VDA update

Use the procedures in this section to install FP3:

1. Ensure the infrastructure servers with XenApp and XenDesktop 7.6 or later are installed and configured correctly.
2. Install the VDA update for release 7.6 Feature Pack 3 per your operating system.
3. After completing the installation, restart the VDA.

Install the GPO update package

New Citrix policy objects for Framehawk must be added to the Group Policy Management Console. The Group Policy Object (GPO) update package is installed on the system where you define and control policies, which is typically the system running Citrix Studio. Depending on your organization's practices, it could instead be the domain controller or the local system.

Note: XenApp and XenDesktop allow policies to be enforced using multiple methods, and Citrix policies in Studio is one of them. If you are using Active Directory for policy administration, you may install the GPO package on the domain controller. If policies are enforced locally on a particular VDA (for example, as client service extensions, or CSE), the GPO package may be installed on the local machine (VDA). Citrix recommends that you select one method and continue using that method.

To install the GPO update package

1. Select the appropriate MSI installer package from the download for your operating system (32-bit or 64-bit). See [Required Framehawk Components](#) for a list of options available for FP3.
2. Run the installer and follow the on-screen prompts to complete the installation.
3. Click **Finish** to exit the setup wizard.

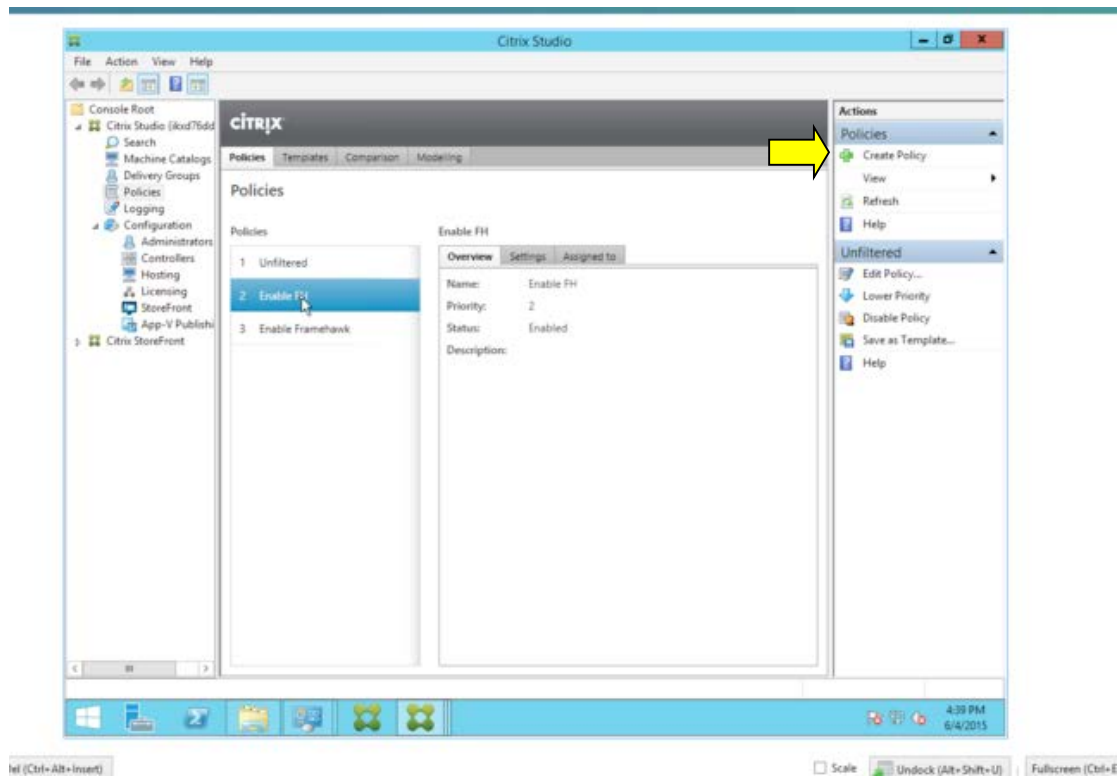
Configuration

To configure Citrix policy for Framehawk

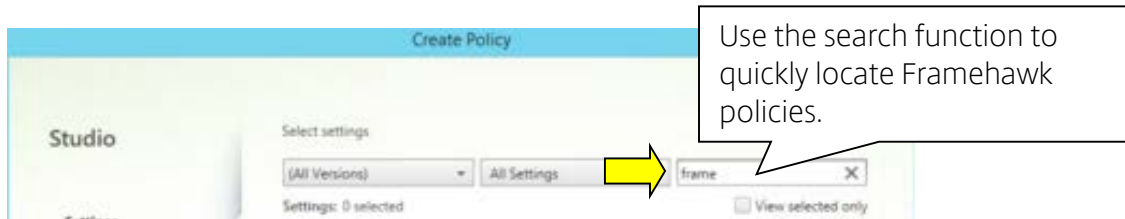
The Framehawk virtual channel is disabled by default. After completing the GPO installation update, you must configure policies to enable Framehawk for appropriate users. When enabled, the server attempts to use the Framehawk virtual channel for users' graphics and input. If the pre-requisites are not met for any reason, the connection is established using the default mode (Thinwire).

Note: The Framehawk virtual channel is disabled by default. Use policies to enable it, and assign to users on lossy, broadband wireless connections.

1. Start Studio and create a new policy for the Framehawk virtual channel.

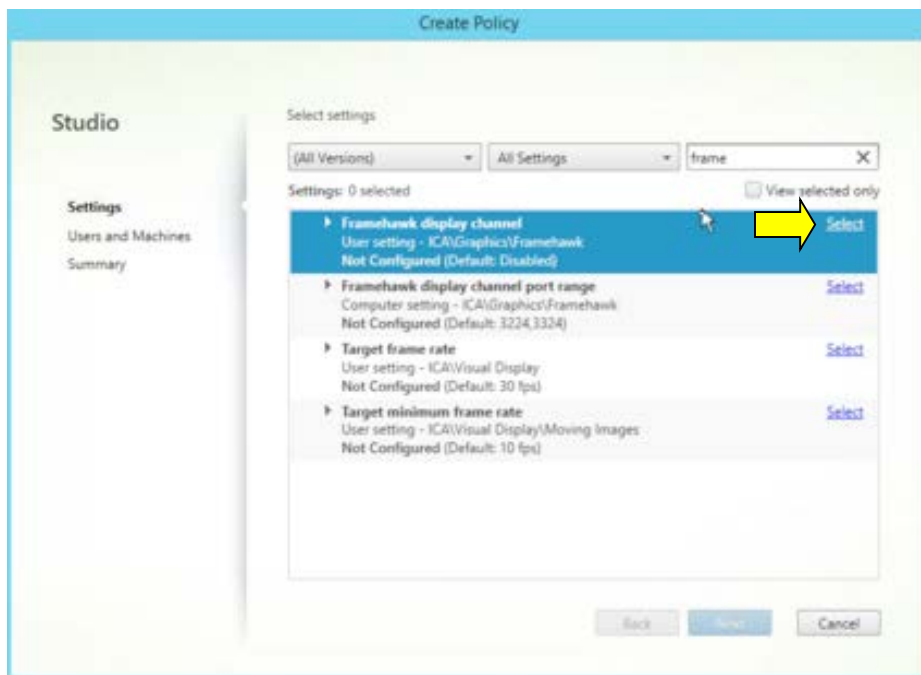


2. On the **Create Policy** screen, locate the new Framehawk policy; type *framehawk* in the search bar.

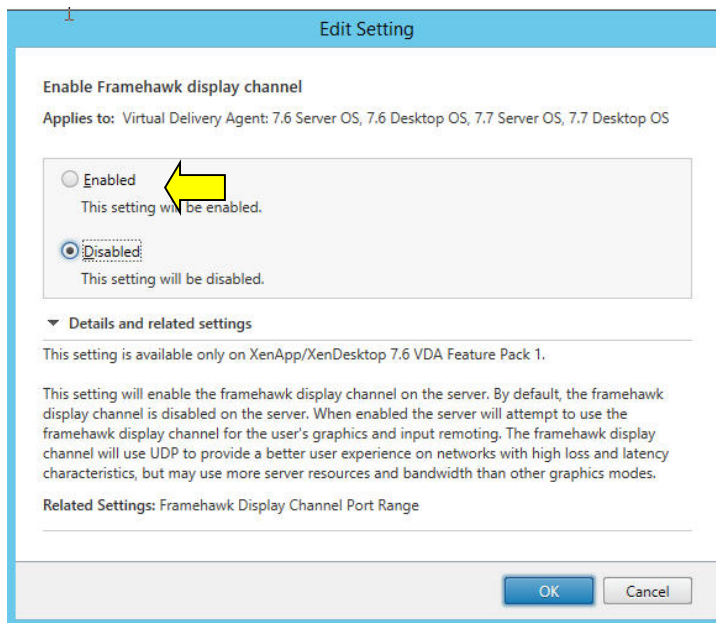


The **Create Policy** screen changes to display policies associated with the Framehawk virtual channel. These policies include:

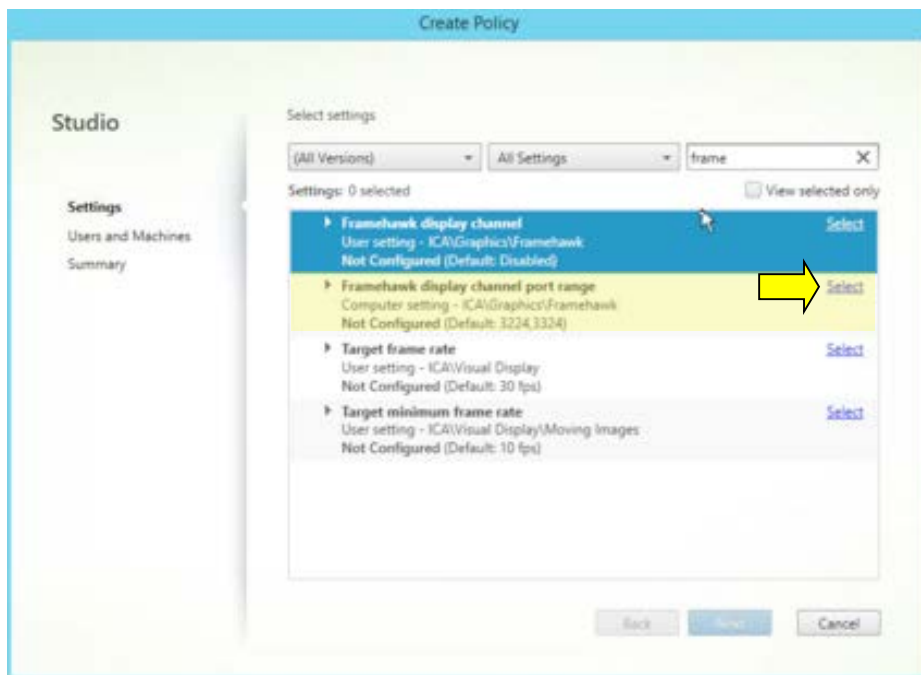
- **Framehawk display channel** – Use this policy to enable or disable the feature (see step 4 below).
 - **Framehawk display channel port range** – Use this policy to define the range of ports using the virtual channel (see step 6 below).
3. In Framehawk display channel, click **Select**.



4. On the **Edit Setting** screen, select **Enabled** and click **OK**.



- On the Create Policy screen, in Framehawk display channel port range, click Select.



This Framehawk policy setting specifies the range of UDP port numbers (lowest port number to highest port number) that the VDA uses to exchange Framehawk display channel data with the user device. The VDA attempts to use each port, starting with the lowest port number and incrementing for each subsequent attempt. The port handles inbound and outbound traffic.

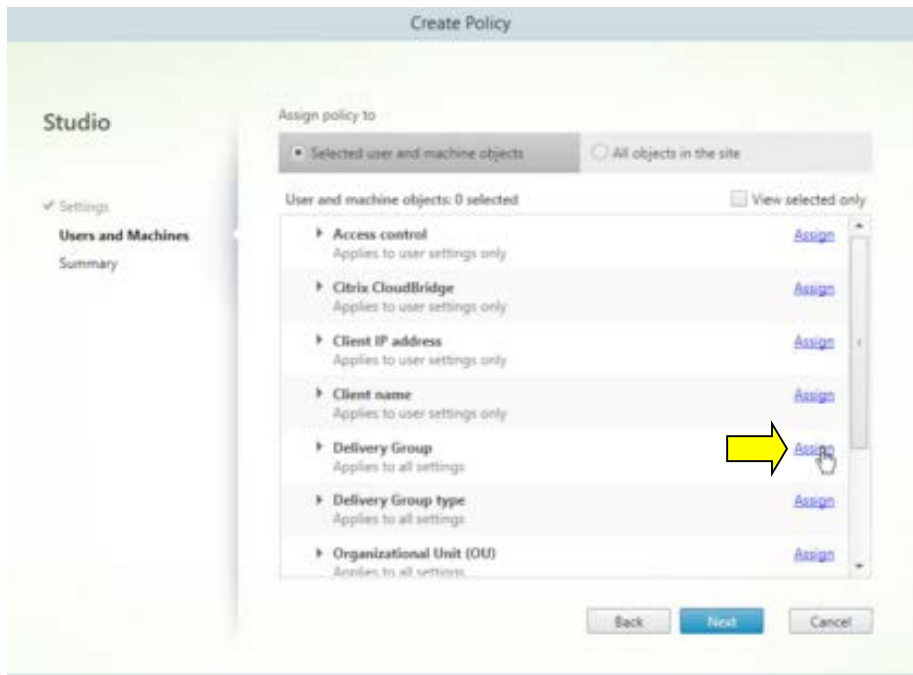
6. If required, enter the custom UDP port range and click **OK**.

The screenshot shows a Windows-style dialog box titled "Edit Setting". The main heading is "Framehawk display channel port range". Below it, it says "Applies to: Virtual Delivery Agent: 7.6 Server OS, 7.6 Desktop OS". There is a text input field labeled "Value:" containing the text "3224,3324". Below the input field is a checkbox labeled "Use default value: 3224,3324", which is currently unchecked. A section titled "Details and related settings" is expanded, showing a scrollable area with the following text: "Please enter a range in the format (Low port),(High port).", "This setting is available only on VDA versions XenApp and XenDesktop 7.6 Feature Pack 2 and later.", "This setting specifies the range of port numbers (in the form lowest port number,highest port number) used by the VDA to exchange Framehawk display channel data with the user device. The VDA attempts to use each UDP port to exchange data with the user device, starting with the lowest and incrementing for each subsequent attempt. The port handles both inbound and outbound traffic.", and "By default, this is set to 3224,3324." At the bottom right of the dialog are "OK" and "Cancel" buttons.

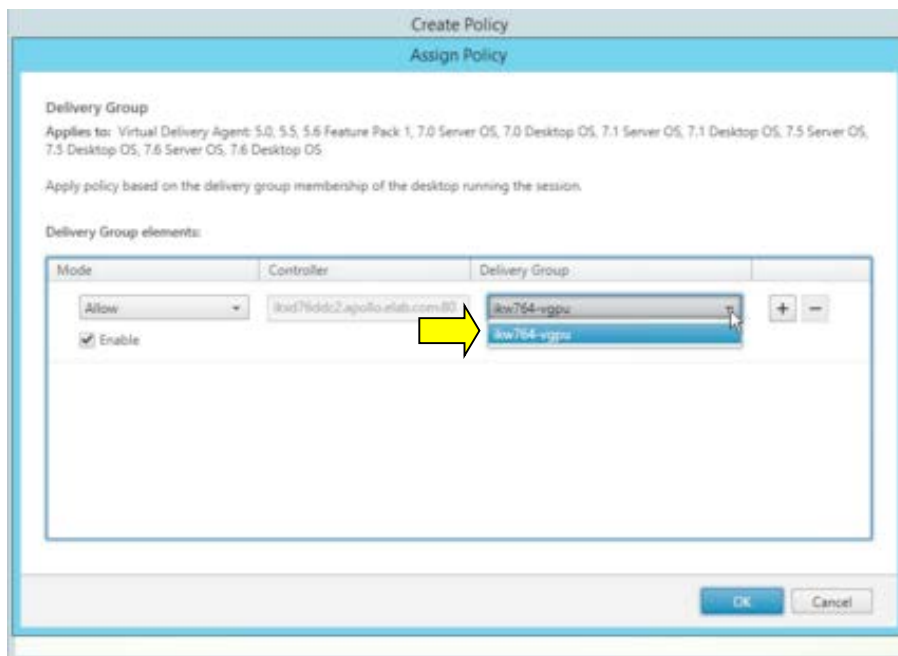
7. Click **Next** to continue with the configuration process and then assign the policy to users, Delivery Group, or virtual machines on broadband wireless connections experiencing high packet loss.

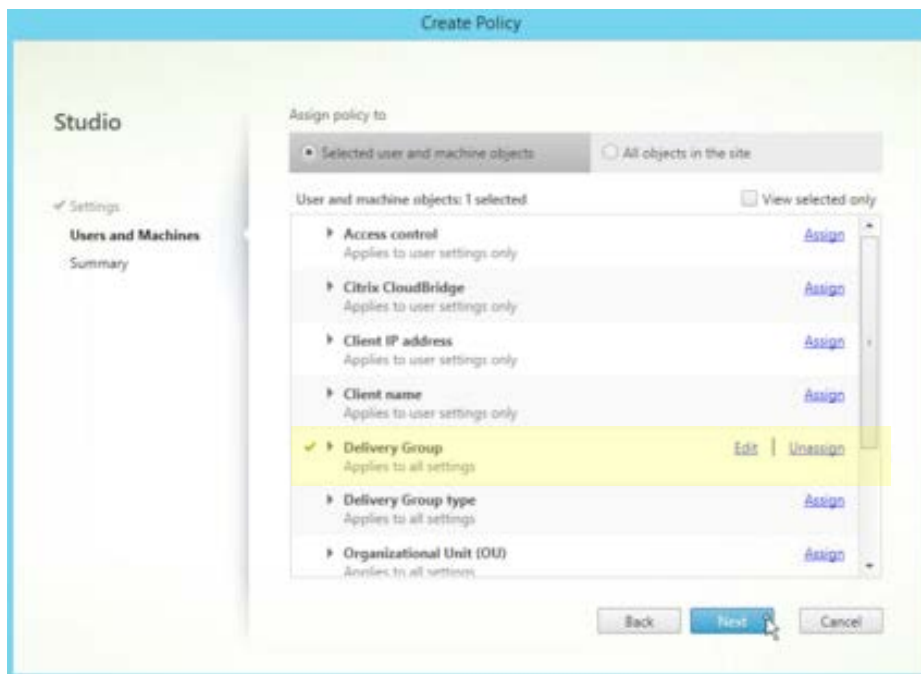
Caution: Citrix recommends that you enable Framehawk only for users experiencing high packet loss. It is also recommended that you **do not** deploy Framehawk as a universal policy for all objects in the Site.

This example associates the Framehawk policy to a Delivery Group. Click **Assign**.

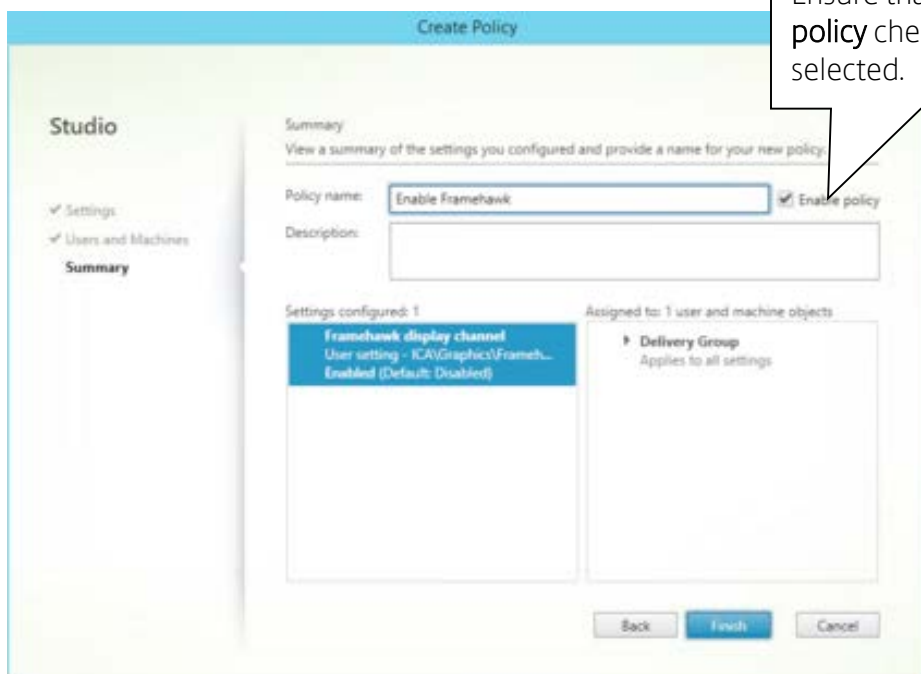


8. On the **Assign Policy** screen, in the **Delivery Group** list, click the appropriate Delivery Group, click **OK** and then **Next**.

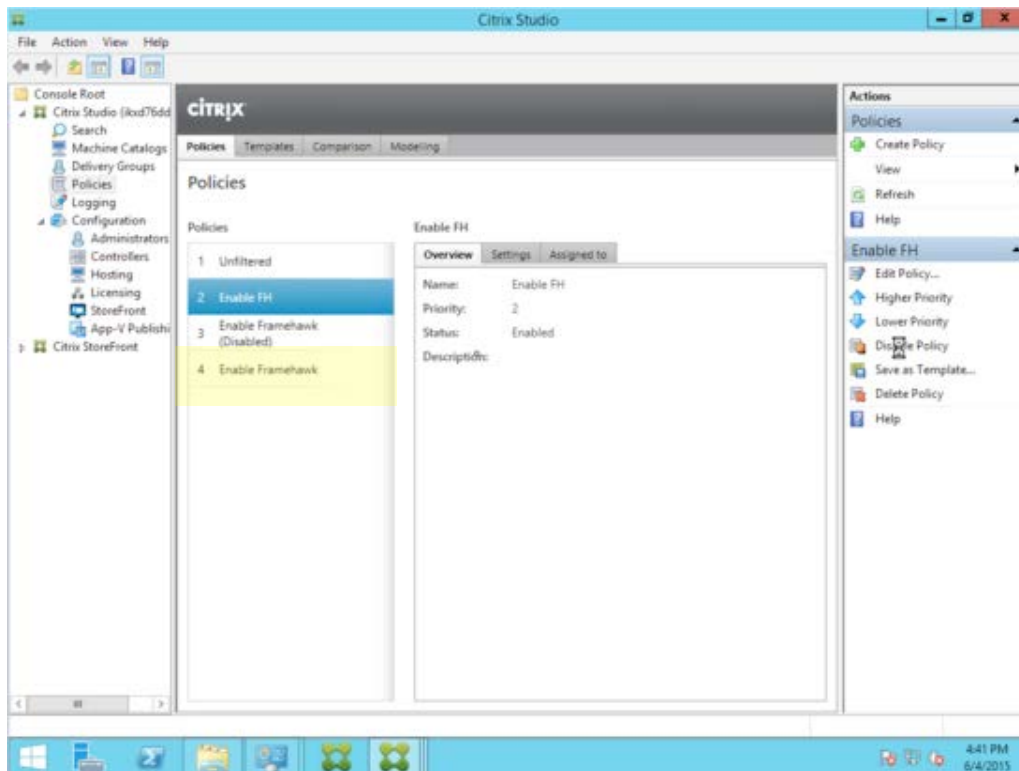




9. Specify a name for the new policy (for example, Enable Framehawk). Make sure the **Enable policy** check box is selected and then click **Finish**.



Ensure that the **Enable policy** check box is selected.

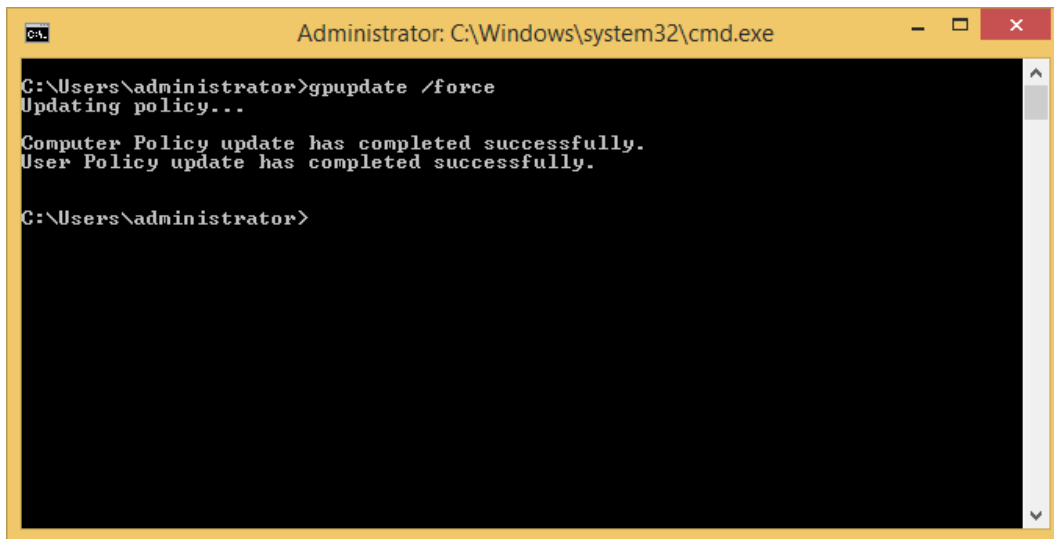


The Framehawk display channel policy is displayed, enabled and assigned to a Delivery Group. The policy will take effect when the user reconnects to the server.

10. Apply the policy through a GPO update. This takes effect when users reconnect to the server. You can also use the command prompt in Administrator mode to immediately apply the policy using the following command:

C:\>gpupdate /force

For example:



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\administrator>
```

Configuring NetScaler Gateway for Framehawk support

This configuration is required if you are enabling UDP encryption on NetScaler Gateway for remote access. This feature, delivered using Datagram Transport Layer Security (DTLS), is not available on NetScaler Unified Gateway at this release.

When configuring NetScaler for Framehawk support, you must:

- ensure UDP port 443 is open on any external firewalls
- enable DTLS in the settings for the VPN virtual server
- unbind and rebind the SSL cert-key pair

To configure NetScaler for Framehawk support:

1. Deploy and configure NetScaler Gateway to communicate with StoreFront, as per standard operating practices, and correctly authenticate users for XenApp and XenDesktop.
2. In the NetScaler Configuration tab, expand **NetScaler Gateway**, and select **Virtual Servers**:

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

Buttons: Add, Edit, Delete, Statistics, Visualizer, Action

Name	State	IP Address	Port	Protocol
FHNSION	Up	10.15.242.97	443	SSL

Left Sidebar (Red Box):

- + System
- + AppExpert
- + Traffic Management
- + Optimization
- + Security
- NetScaler Gateway
 - Global Settings
 - Virtual Servers**
 - Portal Themes
- + User Administration
- + KCD Accounts

- Click **Edit** to display Basic Settings for the VPN Virtual Server; verify the state of the DTLS setting:

VPN Virtual Server

Basic Settings

Name	FHNSION
IPAddress	1.26.52.147
Port	-
State	-
RDP Server Profile	-
Login Once	false
Double Hop	false
Down State Flush	false
DTLS	false
AppFlow Logging	false

- Click **More** to display additional configuration options:

Name
FHNSION

IP Address Type
IP Address

IP Address*
1 . 26 . 52 . 147 ☐ IPv6

Port
443

► More

OK Cancel

SSL Parameters

5. Select **DTLS**, to provide communications security for datagram protocols such as Framenhawk. Click **OK**:

Windows EPA Plugin Upgrade

Linux EPA Plugin Upgrade

Mac EPA Plugin Upgrade

☐ Login Once

☐ ICA Only

☐ Double Hop

☒ DTLS

☐ ICA Proxy Session Migration

☐ Enable Device Certificate

☒ Enable Authentication

☐ Down State Flush

☐ AppFlow Logging

☒ State

Comments

▲ Less

OK Cancel

- The Basic Settings area for the VPN Virtual Server is updated to show that the DTLS flag is set to **True**. Next, we must edit the server certificate.

VPN Virtual Server

Basic Settings			
Name	FHNSION	Maximum Users	500
IPAddress	1.26.52.147	Max Login Attempts	-
Port	-	Failed Login Timeout	-
State	-	ICA Only	false
RDP Server Profile	-	Enable Authentication	true
Login Once	false	Windows EPA Plugin Upgrade	-
Double Hop	false	Linux EPA Plugin Upgrade	-
Down State Flush	false	Mac EPA Plugin Upgrade	-
DTLS	true	ICA Proxy Session Migration	false
AppFlow Logging	false	Enable Device Certificate	false

Certificates	
1 Server Certificate	>
No CA Certificate	>

6. In the **Certificates** section of the VPN Server screen, select the server certificate (refer to the image above) to re-bind the certificate for DTLS handshake.
7. On this screen, select the certificate keypair (remember the name, we need it later). Click **Unbind**:

SSL Virtual Server Server Certificate Binding	
SSL Virtual Server Server Certificate Binding	
<div> Add Binding Unbind Details Update Certificate </div>	
Certificate	Server Certificate for SNI
FHNSION-Keypair	
<div>Close</div>	

8. Click **Save**. After unbinding the certificate, the Certificates portion of the screen shows that no certificates are bound to the server:

Down State Flush	raise	MAC EPA F
DTLS	true	ICA Proxy
AppFlow Logging	false	Enable De

Certificates

No Server Certificate

No CA Certificate

Continue

- Reopen the **Server Certificate Binding** screen, and click + to bind the certificate key pair:

Server Certificate Binding

Server Certificate Binding

Select Server Certificate*

Click to select

>

+

☐ Server Certificate for SNI

Bind Close

- Choose the certificate key pair from earlier, click **Select**:

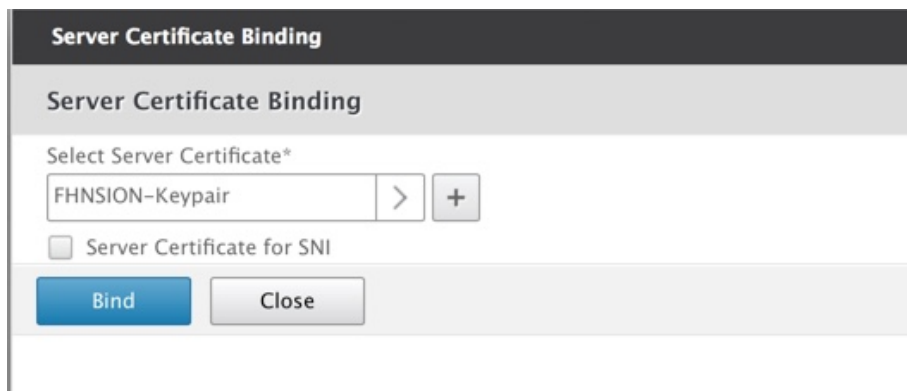
Server Certificate Binding > SSL Certificates

SSL Certificates

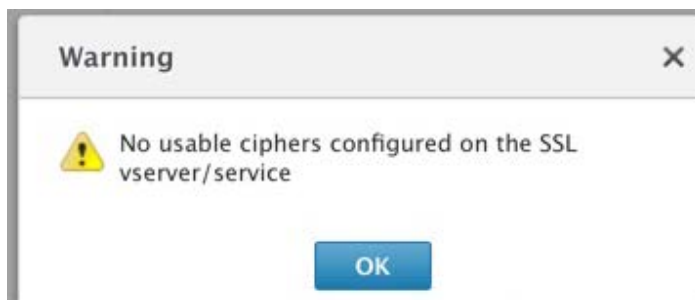
Select Install Update Delete Action

Name
<div> <div></div> <div>FHNSION-Keypair</div> </div>

- Save the changes to the server certificate binding.
- After saving, the certificate key pair appears. Click **Bind**:



13. Ignore the following warning message, if it appears after binding the certificate:



About NetScaler Gateway support for Framehawk

HDX Framehawk virtual channel is not available if NetScaler Gateway is deployed with Unified Gateway. It is supported on NetScaler Gateway 11.0 build 62.10.

NetScaler Gateway refers to the deployment architecture where the Gateway VPN vServer is directly accessible from the end-user device; that is, the VPN vServer has a public IP address assigned and the user connects to this IP directly.

On the other hand, NetScaler with Unified Gateway refers to the deployment where the Gateway VPN vServer is bound as a target to the Content Switching vServer (CS). In this deployment, CS vServer will have the public IP and the Gateway VPN vServer will have a dummy IP.

To enable Framehawk support on NetScaler Gateway, the “DTLS” parameter on the Gateway VPN vServer level must be enabled. Once the parameter is enabled and the components on XenApp/XenDesktop are updated correctly, Framehawk audio, video, and interactive traffic is encrypted between the Gateway VPN vServer and the user device. See [Configuring NetScaler for Framehawk support](#) earlier in this document for information on setting the DTLS parameter.

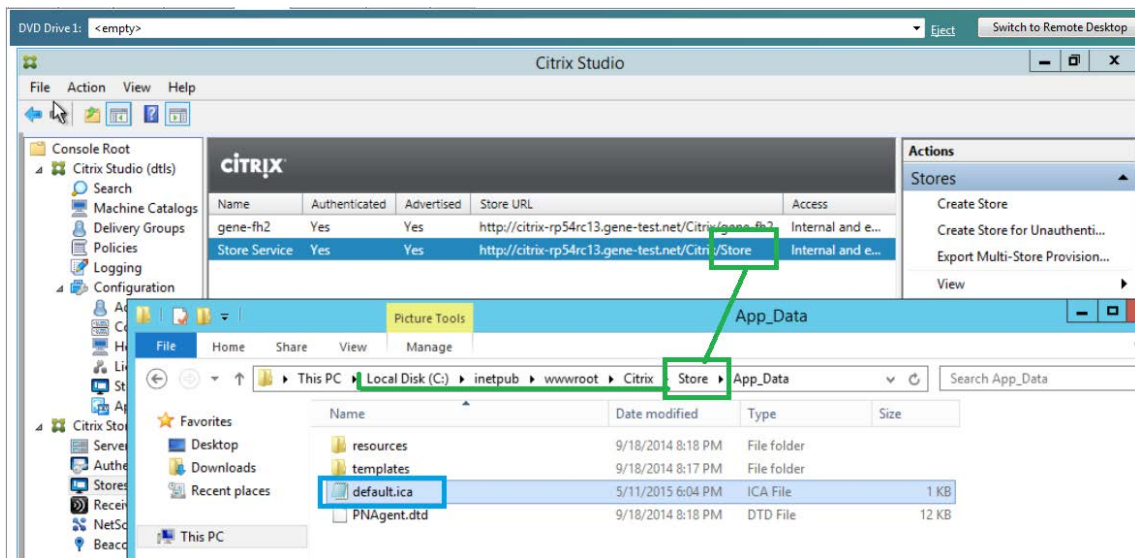
The following table summarizes Framehawk support for different use cases:

Scenario	Framehawk support
NetScaler Gateway	Yes
NetScaler Gateway + Global Server Load Balancing	Yes
NetScaler with Unified Gateway	No
HDX Insight	No
NetScaler Gateway in IPv6 mode	No
NetScaler Gateway Double Hop	No
Multiple Secure Ticket Authority (STA) on NetScaler Gateway	No
NetScaler Gateway with High Availability (HA)	No
NetScaler Gateway with Cluster setup	No

Configuring Citrix Receiver 6.0.1 for iOS to support Framehawk

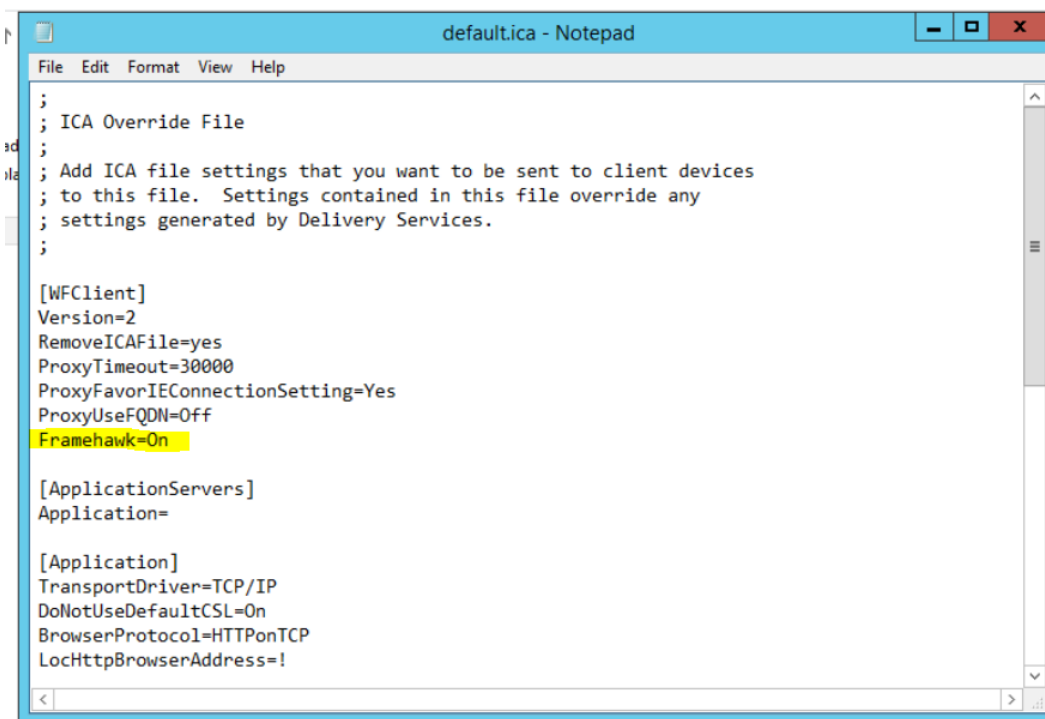
To configure Citrix Receiver for iOS to support Framehawk, you must manually edit the **default.ica**

1. On the StoreFront server, access the **App_Data** directory of your store in **c:\inetpub\wwwroot**.



2. Open the default.ica file and add the following line in the **WFClient** section:

Framehawk=On



3. Save the changes.

This will allow Framehawk sessions to be established from a compatible Receiver on iOS devices.

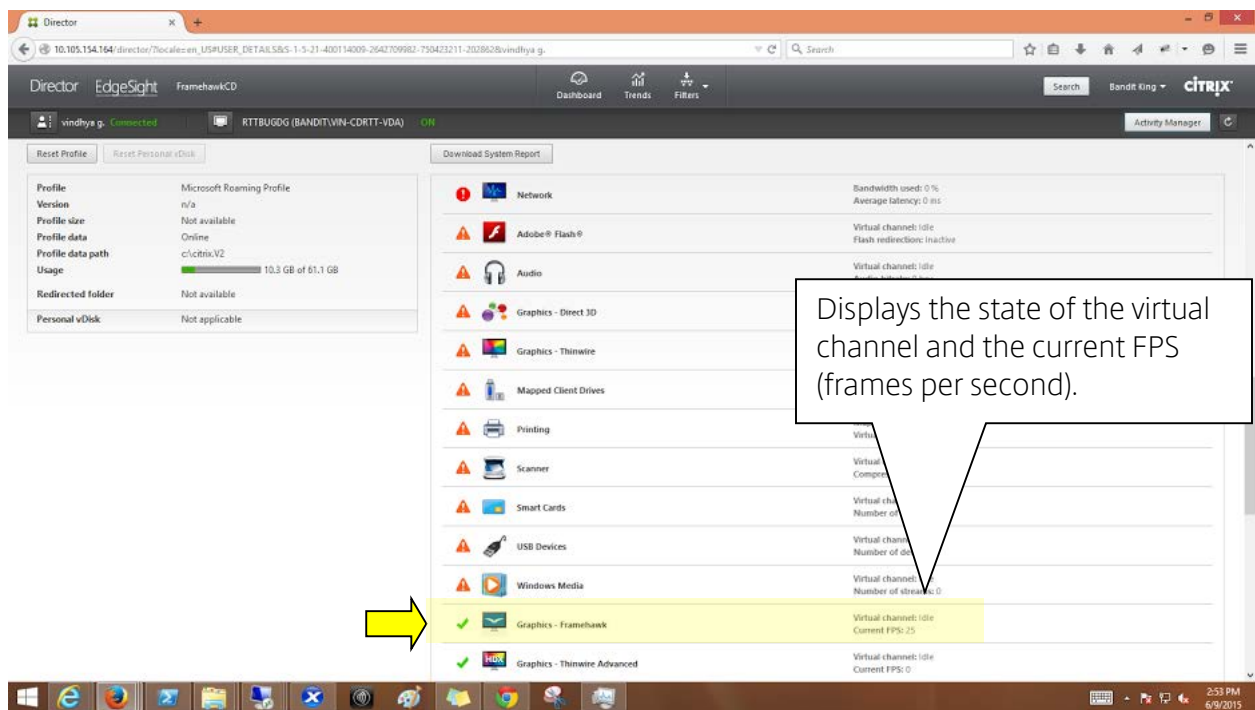
Monitoring Framehawk

You can easily monitor the use and performance of Framehawk using the new statistics in Citrix Director.

Monitoring with Citrix Director

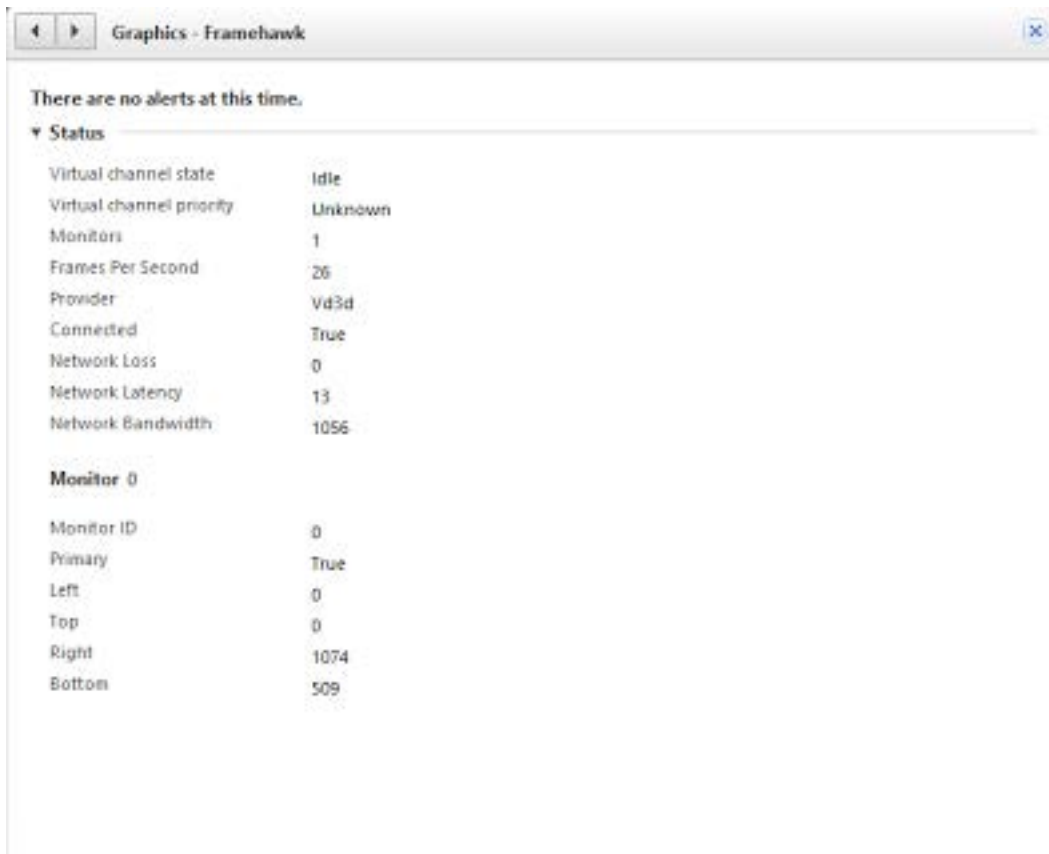
Citrix Director 7.6.300 displays HDX graphics information for the Framehawk virtual channel. The **HDX Virtual Channel Details** view contains useful information for troubleshooting and monitoring the Framehawk virtual channel in any session.

The following figure illustrates the **HDX** panel, under the Detailed connection view in Director. To view Framehawk-related metrics, select **Graphics-Framehawk**.



If the Framehawk connection is established, you will see the **Provider = VD3D** and **Connected = True** in the details page that is displayed. It is normal for the virtual channel state to be idle, because it monitors the signalling channel which is only used during the initial handshake.

This page also provides other useful statistics about the connection:



Known Issues

The following issues are known as this release; refer to the Framehawk [troubleshooting blog](#) for useful tips and tricks when conducting successful evaluations of this new technology:

- Session Recording/Smart Auditor are not supported with Framehawk.
- This release of Framehawk is not supported with high-end graphic intensive environments. It is tested for standard XenApp and XenDesktop workloads, such as knowledge worker and office apps.
- Multi-monitor clients are not supported at this time.
- The Vd3dn.dll may crash on the client under test conditions, such as modifying bandwidth and latency on a WAN emulator in-session. Disconnect the session before making any changes to WAN emulator settings, then reconnect; Framehawk recalibrates during session handshake.
- If policies to enable both Framehawk and legacy mode are enabled, for the same user the behavior changes as follows:
 - On Workstation OS (such as Windows 7 and Windows 10), Framehawk policy takes precedence.
 - On Server OS such as Windows Server 2012 R2, legacy mode policy takes precedence.

- Secure UDP transport using DTLS is not supported for Framehawk on NetScaler with Unified Gateway.
- In some instances, a Framehawk session may experience session reliability issues due to a number of factors, including unplugging and reattaching a network cable while a session is active. [0592502]

Appendix A

Using Framehawk with XenApp and XenDesktop 7.6 FP2

Citrix strongly recommends using XenApp and XenDesktop Feature Pack 3, as per the instructions in the previous sections.

If you are using Framehawk with the older version of XenApp and XenDesktop 7.6 Feature Pack 2, these instructions are required. The components required for Framehawk are not integrated in the VDA, and packaged in the Framehawk_76_FP2.zip compressed file on the [Citrix download site](#).

The ZIP file contains the following components:

Update on the Virtual Delivery Agent

- VDA hotfix for XenApp and XenDesktop Version 7.6 or later (one .MSI file for the workstation, and one for the server OS):
 - ICAWS760WX86026.msp for x86 machines , 32-bit Desktop OS
 - ICAWS760WX64026.msp for x64 machines, 64-bit Desktop OS
 - ICATS760WX64032.msp for x64 machines, 64-bit Server OS
- Citrix monitoring (WMI Proxy) plug-in
 - WMIProxy_x86(x64).msi
- Citrix HDX WMI Provider hotfix (only for XenApp VDA, Server OS):
 - HDXWMIPROV220WX64001.msi

Update on the Delivery Controller

- Group Policy Objects (GPO) update. This is installed on the delivery controller for Citrix Studio integration:
 - GPMx240WX86002.msi for x86 machines, 32-bit OS
 - GPMx240WX64002.msi for x64 machines, 64-bit OS

Update on Citrix Director

- Citrix Director 7.6.300
 - DesktopDirector.msi for x32 machines, 32-bit OS
 - DesktopDirector_x64.msi for x64 machines, 64-bit OS

And, for monitoring power-shell modules

- XDPoshModule760WX86002.msi
- XDPoshModule760WX64002.ms

Update on client end point

- Citrix Receiver for Windows 4.3
- Citrix Receiver for iOS Classic 6.0

Note: In order to use Framehawk on iOS Receiver, you must modify the default.ica file for the store. See [Configuring iOS Citrix Receiver for Framehawk support](#) in this guide.

Installation - XenApp and XenDesktop 7.6 FP2 only

If you are installing XenApp and XenDesktop 7.6 FP2, perform the following additional installation procedures.

To install the VDA hotfix

Use the procedures in this section if you plan to install FP2; **these procedures are not required for Framehawk installations used with XenApp and Desktop 7.6 FP3.**

4. Ensure the infrastructure servers with XenApp and XenDesktop 7.6 or later are installed and configured correctly.
5. Install the appropriate VDA hotfix for release 7.6 Feature Pack 2 per your operating system.
6. After completing the installation, restart the VDA.

To install the Citrix HDX WMI Provider feature pack

This section is only applicable if you are updating a XenApp VDA, running a server operating system. For a desktop operating system, the Citrix HDX WMI Provider feature pack is updated automatically with the VDA feature pack. **These procedures are not required for Framehawk installations used with XenApp and Desktop 7.6 FP3.**

The WMI Proxy plug-in on the VDA to Director 7.6.300 must also be updated, using *WMIProxy_x86(x64).msi*.

To install the HDX WMI provider hotfix on Server OS:

1. Select the 64-bit server feature pack installer for the WMI Provider feature pack (labeled HDXWMIPROV220WX64001.msi).
2. A security warning may appear. Click **Run**.



3. The Setup Wizard appears. Follow the on-screen prompts to complete the installation.



4. After installation completes, restart the VDA.