Upload Portal Administrator's Guide

telestream

October 2018

265824

Administering the Upload Portal

Introduction

This guide provides instructions for administrators to set up the Vantage Upload Portal. The Upload Portal is a Web application that runs in most popular browsers and presents a simple interface to allow your customers or remote users to quickly and easily upload media and other files and metadata to your Vantage system via an HTTP connection or an Aspera server over the Internet.

TrafficManager administrators who have an Aspera server and the Aspera Connect Plug-in for their browser (required) can configure their portal for Aspera to achieve very fast data uploads to the Aspera server.

TrafficManager administrators who do not have an Aspera server can simply configure their portal for HTTP. This configuration uses the Windows IIS Web Server built into the Windows OS on their Vantage server to upload directly to Vantage workflows.

Before enabling your customers to upload files, you should configure Vantage workflows to receive and process the uploaded files.

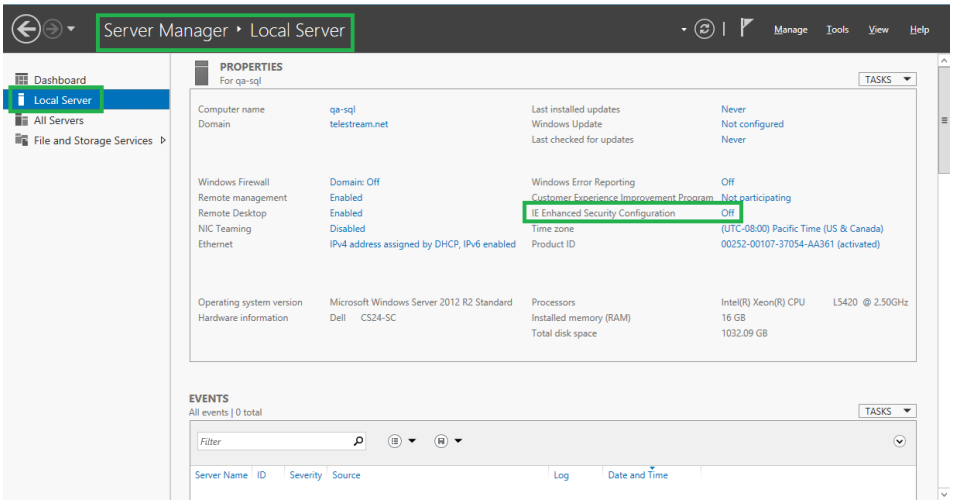
Once your portals and workflows are configured, your customers can upload in three simple steps:

(1) Select the files.
(2) Enter the metadata describing each file and the advertiser.
(3) Submit the files.

Administering the portal involves the following tasks:

Windows Server Preparation

If you are using Internet Explorer on a Windows Server operating system, disable *Enhanced Security Configuration (ESC)* using the Windows Server Manager. To do this select *Server Manager* > *Security Information* > *Configure Internet Explorer ESC*.



Updating the Upload Portal

If you already have the Vantage Upload Portal installed and would like to update to the latest version while retaining your current configuration, follow these steps:

1. Use the Windows Control Panel to remove the old Upload Portal.
2. Install the new portal as explained in *Installing the Upload Portal*.
3. When you run the new Web Upload Portal software, your previous configuration will be detected and restored.

- For details about administering and using the Upload Portal, refer to the built-in help system and the details later in this guide.

Installing the Upload Portal

The Vantage Upload Portal is a TrafficManager option that may be installed and removed separately without affecting other Vantage components.

One of the following Windows Server versions is required on the host machine:

- Windows Server 2012 R1 (64-bit only)
- Windows Server 2012 R2 (64-bit only)
- Windows Server 2016 (64-bit)

The following Microsoft components are required on the host machine:

- Microsoft IIS 8.0 or later
- .NET 4.7.2

Follow these steps to install the Upload Portal:

1. Verify that IIS 8.0 or later is installed prior to running the Upload Portal installer.

Note: To verify the IIS setup, select *Start>Programs* and enter *IIS* to see if the Internet Information Services Manager is listed among the programs on your computer.

---

2. Enable IIS roles as listed in the *IIS Role Service Requirements* table.
3. Download and unzip the Upload Portal file to access the Vantage_<version>_Upload_Portal_*Setup.exe* installers.
4. Run the Vantage_<version>_Upload_Portal_*Setup.exe* installer on the target server.
5. When the Welcome Window appears, click Next.
6. Read the license agreement. If you accept the terms, click *I Agree* and click Next.
7. When the Select Installation Address dialog appears, be sure to set the Application Pool selection to - *create Vantage Application Pool* - (or *Vantage ASP .NET*).

Note: On the Select Installation Address page, you can set the address used to access the portal by changing the Virtual directory field. The default value is UploadPortal (http://servername/UploadPortal/). If you change the value to MyPortal, for example, the URL becomes http://servername/MyPortal/.

When finished with the Select Installation Address page, click Next.

8. Click Install to start the installation.
9. When the Installation Complete dialog appears, click Finish.

Role Service Requirements

Select the following IIS roles on your Windows server in IIS Manager.

IIS Role Service Requirements

Service	Install/Select	Uninstall/Deselect
Common HTTP Features	Static Content Default Document Directory Browsing HTTP Errors	HTTP Redirection WebDAV Publishing
Application Development	.NET Extensibility 4.5/4.6 ASP.NET 4.5/4.6 ISAPI Extensions ISAPI Filters	.NET Extensibility 3.5 Application Initialization ASP ASP.NET 3.5 CGI Server Side Includes WebSocket Protocol
Health and Diagnostics	HTTP Logging Request Monitor	Logging Tools Tracing Custom Logging ODBC Logging Tracing (2016)
Security	Request Filtering	Basic Authentication Windows Authentication Digest Authentication Client Certificate Mapping Authentication IIS Client Certificate Mapping Authentication URL Authorization IP and Domain Restrictions
Performance	Static Content Compression	Dynamic Content Compression
Management Tools	IIS 6 Management Console IIS 6 Management Compatibility IIS 6 Metabase Compatibility IIS 6 WMI Compatibility IIS 6 Scripting Tools IIS 6 Mgmt. Console	IIS Management Scripts and Tools Management Service
FTP server		FTP server FTP Service FTP Extensibility
IIS Hostable Web Core		IIS Hostable Web Core

Configuring Your Network

A vital part of setting up the Vantage Upload Portal for your advertisers includes planning your Vantage server network to ensure safety from the possibility that your system could be hacked or compromised while also serving your advertisers effectively. The Vantage Web Upload Portal should be installed behind a firewall as described in this section. For best security, use two firewalls—one between the portal and the Internet and a second one between the portal and the Vantage domain and database.

Ports

For ports used by Aspera, refer to the *Aspera Connect PDF Guide*, which can be downloaded from: http://downloads.asperasoft.com/connect2/.

For the Upload Portal to be addressable over the Internet, port 80/TCP must be forwarded through the Internet firewall to the outside world using Network Address Translation (NAT).

Note: The Upload Portal communicates through the outside firewall to the Internet via port 80.

If an additional firewall separates the portal from the Vantage domain and storage, these ports must be forwarded through the embedded firewall:

Table 1. Port Numbers for Forwarding Through an Embedded Firewall

Port Name	Port Number	Port Type
NB-Name	137	UDP
NB-Datagram	138	UDP
NB-Session	139	TCP
SMB	445	TCP
Vantage SDK-1	8676	TCP

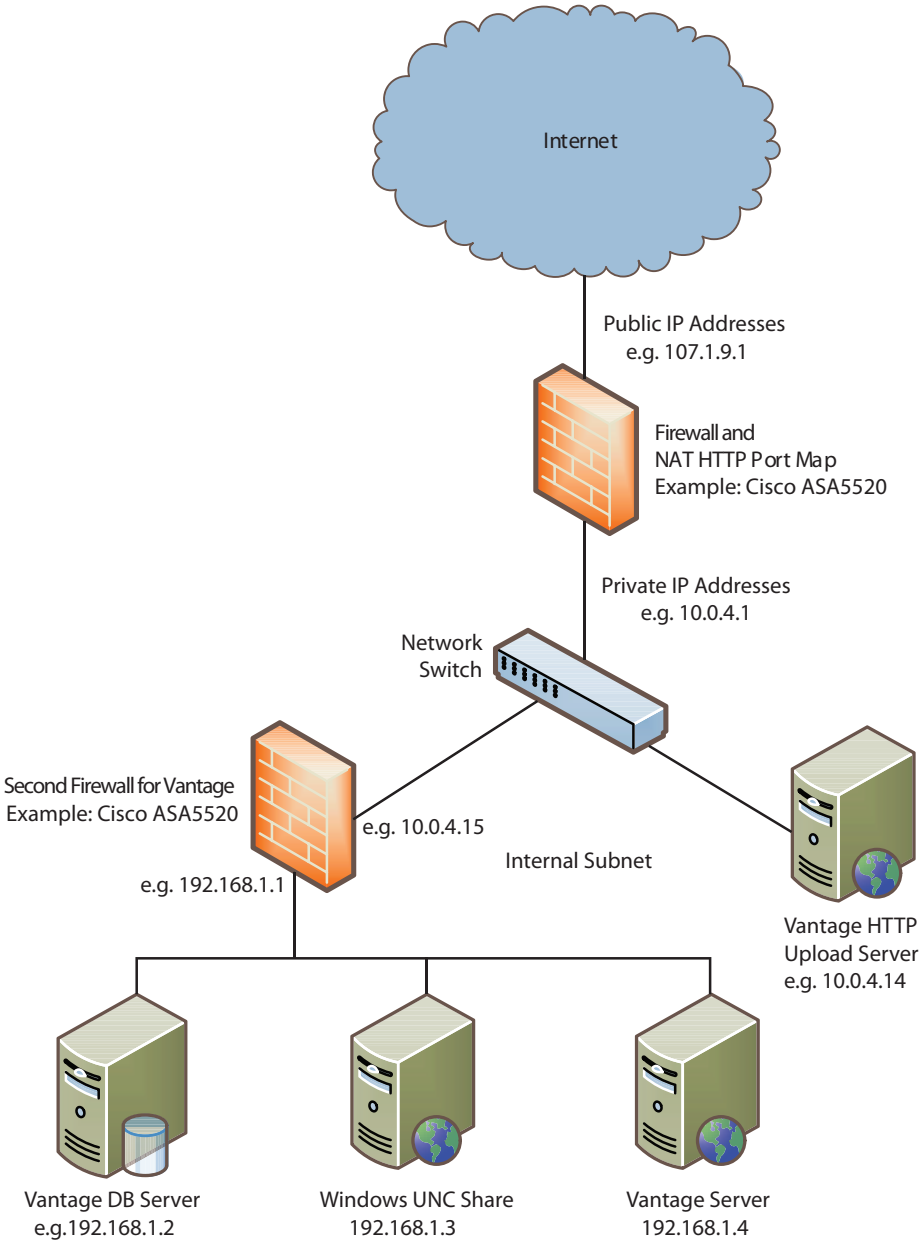
The following topics present network map examples:

- Network Map 1: Double Firewall
- Network Map 2: Double Firewall with Proxy Outside
- Network Map 3: Upload Server Outside Firewall
- Network Map 4: Server and Share Outside Firewall

Network Map 1: Double Firewall

In this highly-recommended network setup as depicted in the illustration below, a Cisco ASA5520 Security Appliance hardware firewall separates the entire Vantage network from the Internet. A second firewall separates the Vantage servers on the internal network. Network Address Translation (NAT) via an HTTP Port Map in the Cisco unit ensures that IP addresses used on the Internet are converted to different IP addresses internally, protecting internal servers from being directly addressed via the Internet. This double firewall approach maximizes protection against attacks.

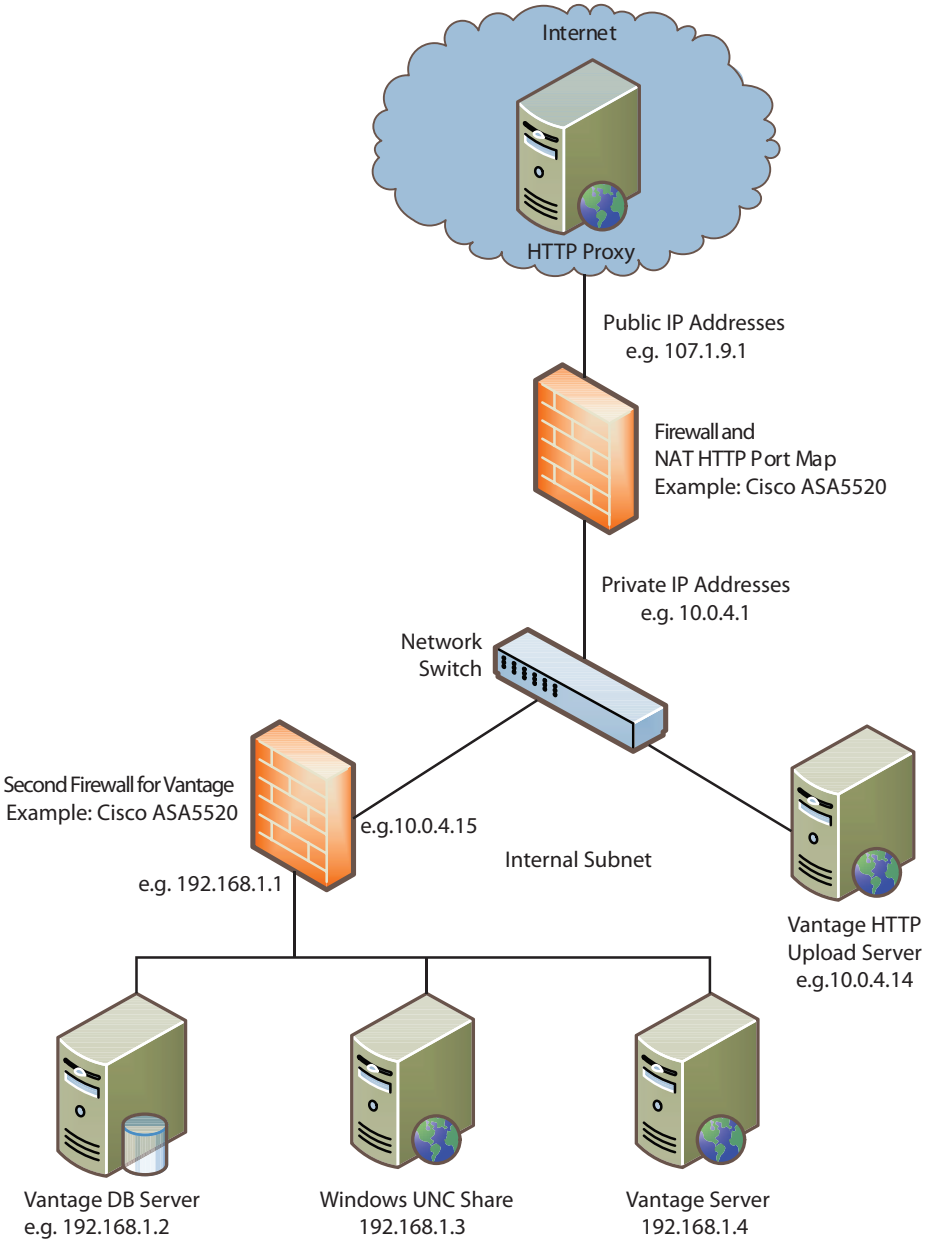
Figure 1. Network Map 1: Double Firewall



Network Map 2: Double Firewall with Proxy Outside

Another recommended network setup, as illustrated, uses an HTTP proxy server on the Internet outside the corporate firewall. This server passes appropriate Internet traffic through the Cisco ASA Security Appliance firewall to the Vantage HTTP Upload Server. The Vantage servers on the internal network are protected by another firewall. A NAT Port Map in the Cisco device remaps external IP addresses to a different set of internal IP addresses to prevent direct Vantage server access from the Internet. Again, this double firewall with IP remapping provides effective protection against attacks.

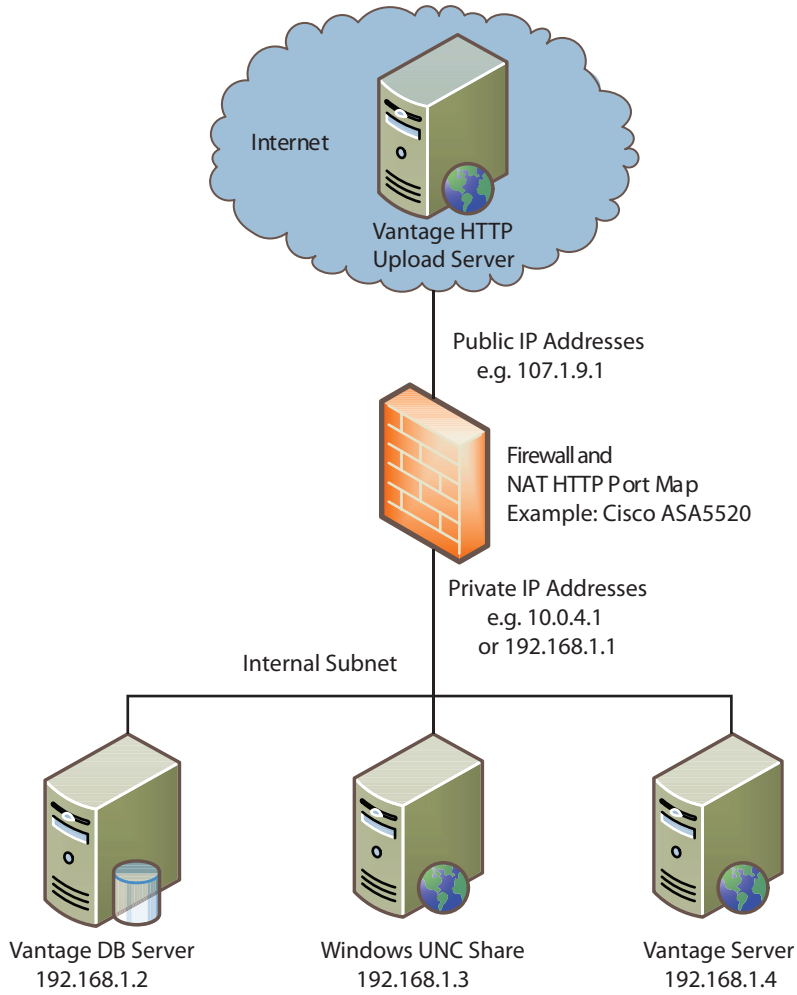
Figure 2. Network Map 2: Double Firewall with Proxy Outside



Network Map 3: Upload Server Outside Firewall

The network setup shown in this figure is **NOT RECOMMENDED** because it places the Vantage HTTP Upload Server outside the corporate firewall on the Internet. This arrangement leaves that server vulnerable. However, the firewall between that server and the other Vantage servers protects the general Vantage installation. A NAT Port Map deployed on the Cisco ASA5520 Security Appliance further protects Vantage by mapping external IP addresses to different internal IP addresses. This arrangement is not recommended because it provides only minimal security.

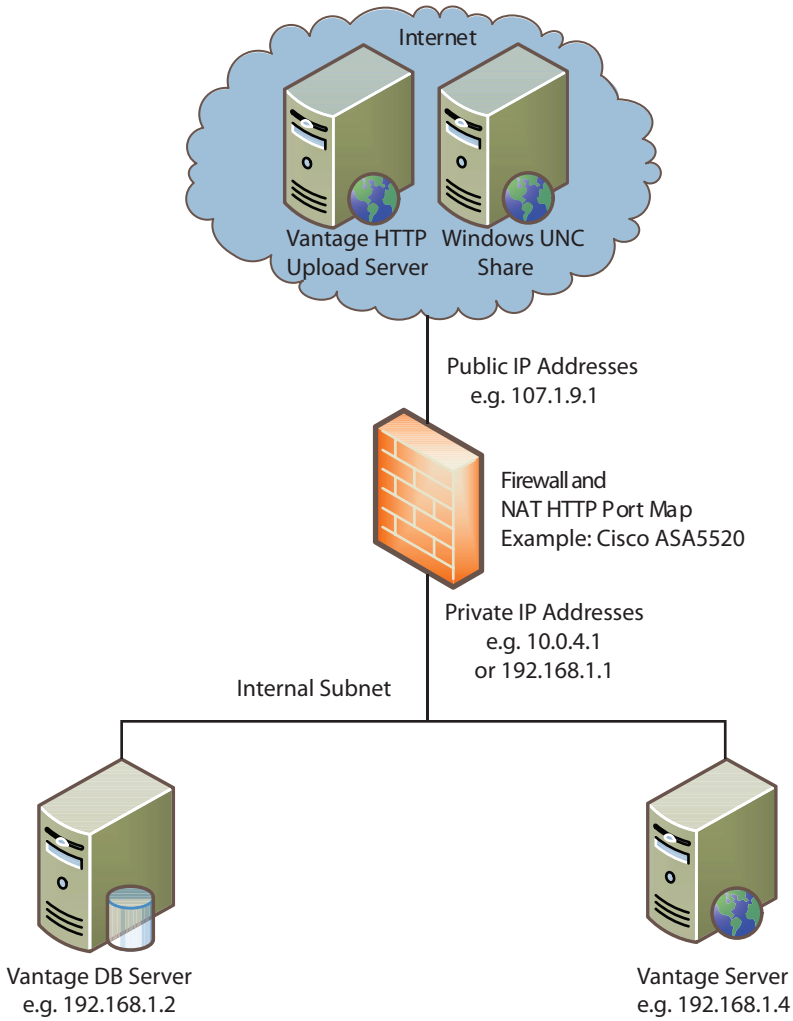
Figure 3. Network Map 3: Outside Firewall NAT Port UNC



Network Map 4: Server and Share Outside Firewall

A fourth network setup shown here is also **NOT RECOMMENDED** because it places the Vantage HTTP Upload Server and the Windows UNC share outside the corporate firewall on the Internet. This arrangement leaves those servers vulnerable. However, the firewall between those servers and the other Vantage servers protects the general Vantage installation. This arrangement is not recommended because it provides only minimal security.

Figure 4. Network Map 4: Outside Firewall



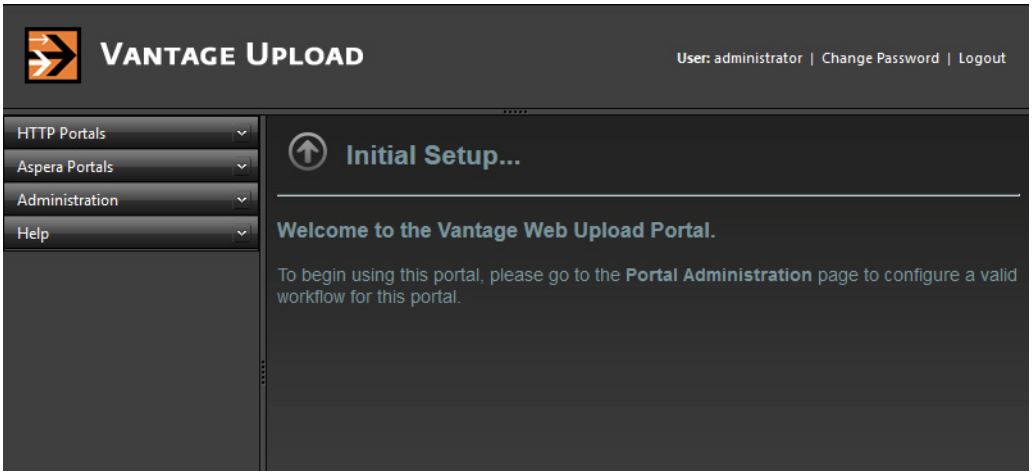
Logging Into the Upload Portal

To log into the Vantage Upload Portal as an administrator:

1. Open a Web browser and enter the following address in the browser's address field:

   http://<servername>/UploadPortal/

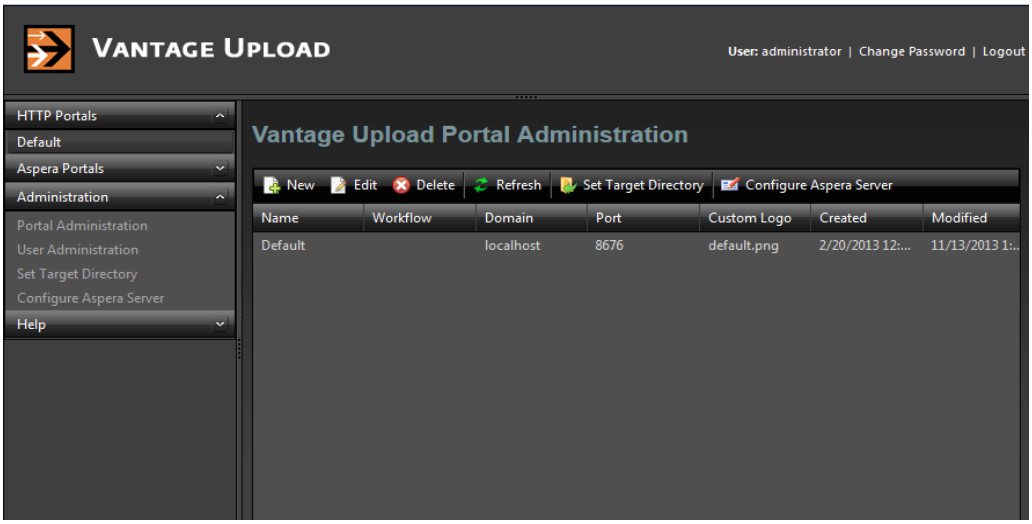
   In place of *servername*, insert the name of the server running the Upload Portal. Also, if you changed the portal name during installation, use that name instead of UploadPortal.
2. Press Enter. The Vantage Upload Login window opens.
3. Enter *administrator* in the User Name field and leave the password field blank. (Note that you may want to change the administrator's User Name and password once you have logged in—see Configuring User Accounts and be sure to check the Administrator check box to make your new user the administrator.) If you want Windows to remember your login and auto-fill the fields, leave *Remember me next time* checked. To turn off auto-fill, uncheck it.
4. Click *Log In* to complete the login. The portal opens to the Initial Setup window.



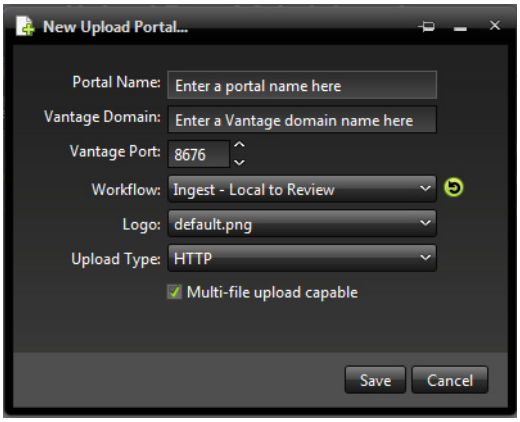
Configuring a Portal

The Upload Portal allows you to configure multiple portals so that each of your customers can have their own customized portal. You can even configure multiple portals per customer if it makes sense to do so. To create a portal, follow these steps:

1. Click Administration and then Portal Administration in the left panel of the Upload Portal window. The Vantage Upload Portal Administration window opens.

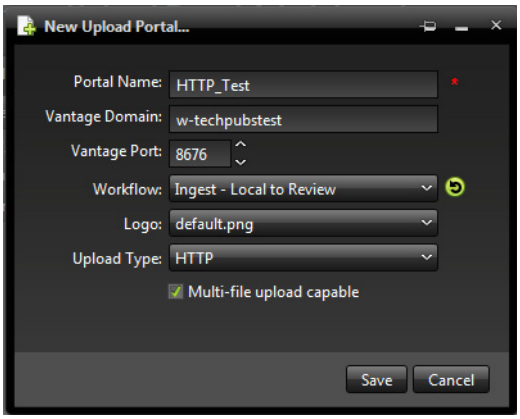


2. Click New in the Vantage Upload Portal Administration window. The New Upload Portal window opens.

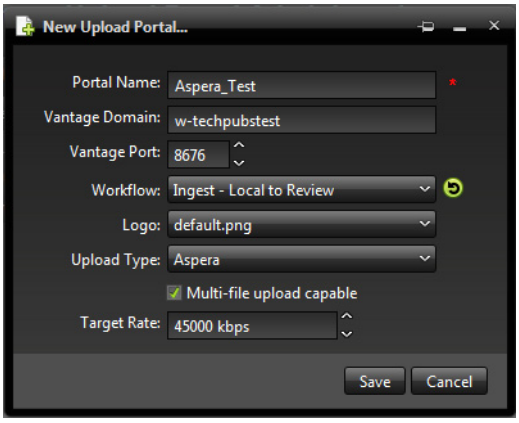


3. Select the Upload Type drop-down menu near the bottom of the window, and set this portal to be an HTTP portal or an Aspera portal.
4. Enter a Portal Name. Typically, you might use the client's company name in the Portal Name to help you identify who will be using this portal.
5. Enter the Vantage Domain server name. This is the name of the server where the Vantage SDK service is installed.

6. Use the Workflow drop-down menu to select the Vantage workflow to which you want to submit uploaded files. Be sure to click the refresh button ( ) to see all available workflows. Workflows can be designed to immediately act upon files submitted via the portal.
7. Use the Logo drop-down menu to select and install your own custom logos, if you wish. You can apply your logo to both HTTP and Aspera portals, as selected by the Upload Type menu. For detailed instructions about changing the top left and center right logos and the favicon, see *Customizing Logos*.
8. Check Multi-file upload capable to grant the user the ability to upload multiple files. (**Note:** Browsers can select multiple files at a time, except for Internet Explorer 9, which can select only one file at a time.) Leave this unchecked if you want the user to upload only one file at a time.
9. For Aspera portals, set the Target Rate for data transfer, usually 45000 kbps or greater.



New HTTP Portal



New Aspera Portal

10. Click Save to save the new portal. The new portal appears in the Vantage Upload Portal Administration list.
11. For HTTP portals, select the new portal in the list, and select *Set Target Directory*. Enter a path in the *Edit Target Path* window to specify the folder that will receive the uploaded files. The path must be in UNC format (include the server name/IP and complete path), and it must be accessible to both Vantage and the IIS web server running the portal.

    For Aspera Portals, see *Configuring an Aspera Server Connection* to configure the Aspera-Vantage connection and the folder that will receive uploaded files.

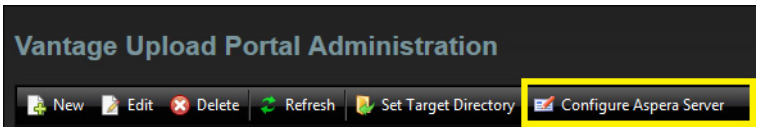
Note the other buttons for future use:

- *Edit*—allows you to edit the details of an existing portal in the list.
- *Delete*—lets you delete a portal from the list.
- *Variables*—lets you add or remover user variables.
- *Refresh*—refreshes the list of portals after you make changes.

Configuring an Aspera Server Connection

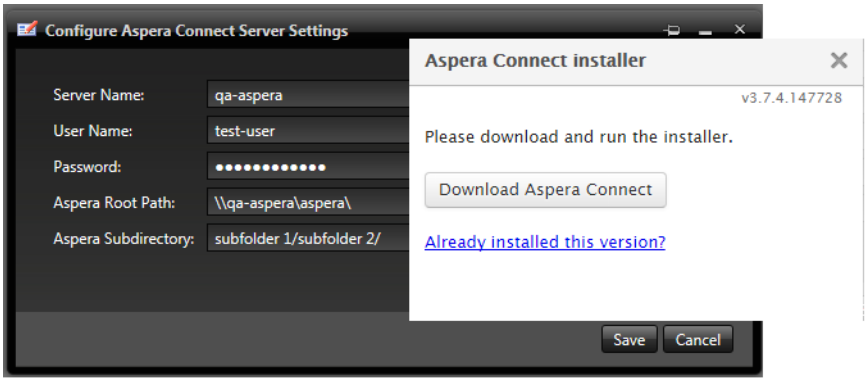
Follow these steps if you are configuring an Aspera Portal. Skip this topic if you are configuring an HTTP Portal.

1. Select Portal Administration, and select the Aspera portal you wish to configure in the Portal Administration list.
2. Click *Configure Aspera Server* in the menu bar at the top of the right panel.



The *Configure Aspera Connect Server Settings* window opens.

If Aspera Connect has not already been installed, an installer window appears over the Configure window. Download Aspera Connect and run the .msi installer. Then open the browser and Upload Portal again and return to these steps.

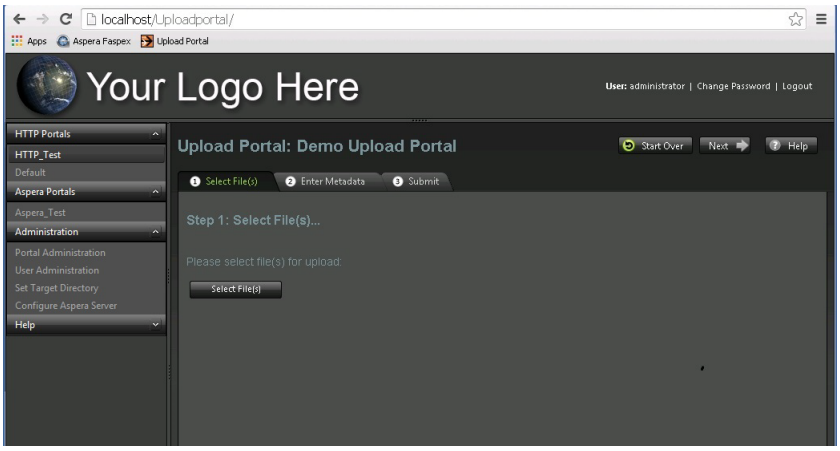


3. Enter the Aspera server name in the Server Name field.
4. Enter the user name the Upload Portal will use for logging into the Aspera server.
5. Enter the password for the user specified in the previous step.
6. Enter the Aspera Directory for uploaded files. Typically, this path looks similar to this: `\\hostname\root share\`.
7. Enter the Aspera Subdirectory, which is the subfolder within the folder where uploads will be placed. This might be called, `subfolder1/subfolder2/`. Therefore, the full path looks similar to this: `\\hostname\root share\subfolder1/subfolder2/`.

   The subdirectory permissions must allow access to both Aspera and Vantage.

Customizing Logos

You can change the logos in the upper left corner and the top middle of the portal user interface (shown below). Additionally, you can change the favicon—the icon shown in the browser address bar.



To change the logo or favicon, follow these instructions:

Top Left Logo

To change the logo displayed at the top left of an Upload Portal page:

1. On the web host, use Windows Explorer to browse to *C:\inetpub\wwwroot\UploadPortal\CustomLogos*.
2. Copy an image file to the *CustomLogos* folder.

   Note: The image file can be PNG, JPEG, or GIF. A PNG with a transparent background looks best. The size of the logo must be 468 x 80 pixels; if a larger icon is used, the links for Change Password and Logout may be pushed off the screen.
3. Use a web browser to browse to *http://<hostname>/UploadPortal/*.
4. Log in as the administrator.
5. Select Portal Administration.
6. Create a new Upload Portal configuration or edit an existing one.
7. Expand the Upload Type drop-down menu and select whether the logo is for your HTTP or Aspera system.
8. Expand the Logo drop-down-menu and select your image file by filename.

Top Center Logo

To change the logo displayed at the top center of the Upload Portal login page:

1. On the web host, use Windows Explorer to browse to *C:\inetpub\wwwroot\UploadPortal\App_Themes\Default\images.*
2. Replace the *upload_loginLogo.png* file with your own image file.

   Note: The file name of the login image must be *upload_loginLogo.png* and must be a PNG file. A PNG with a transparent background looks best.

Favicon

To change the Upload Portal favicon (icon used in browser bookmarks):

1. On the web host, use Windows Explorer to browse to *C:\inetpub\wwwroot\UploadPortal\App_Themes\Default\images.*
2. Replace the *favicon.ico* file with your own icon file.

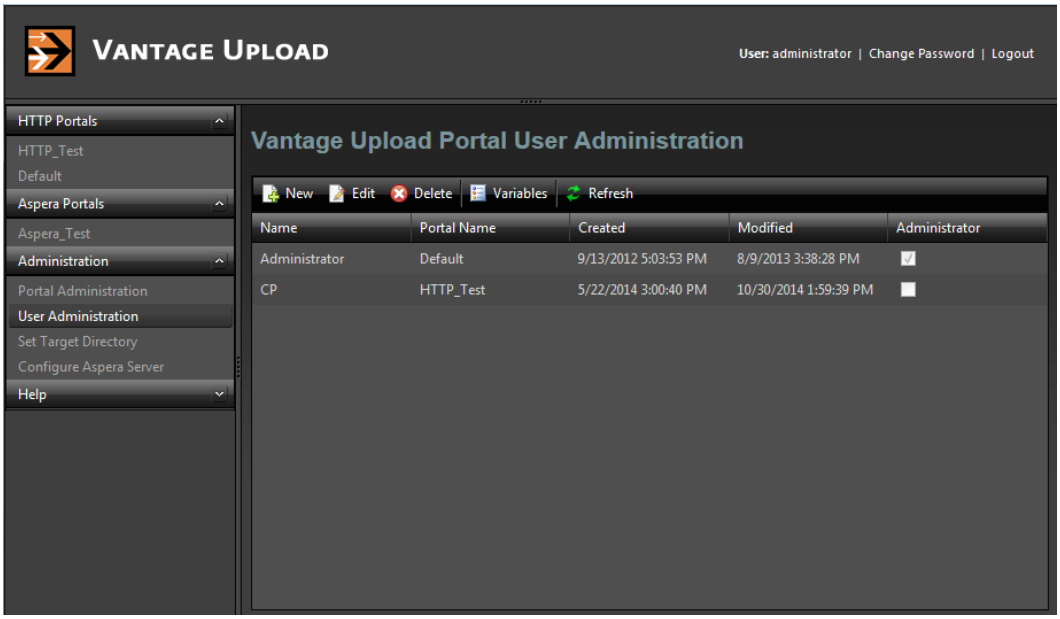
   Note: The file name of the icon image must be *favicon.ico* and must be an ICO file.

Configuring User Accounts

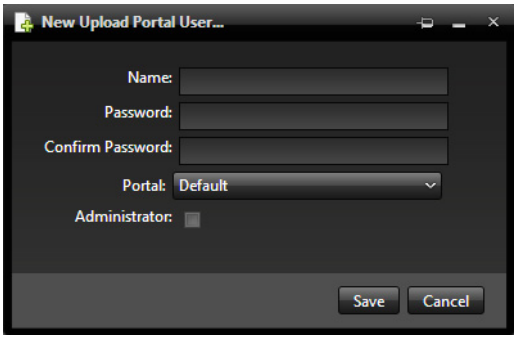
The Upload Portal allows you to configure user accounts and assign them to the custom portals you have created for each customer.

To create a user account, follow these steps:

1. Click Administration and then User Administration in the left panel of the Upload Portal window. The Vantage Upload User Administration window opens.



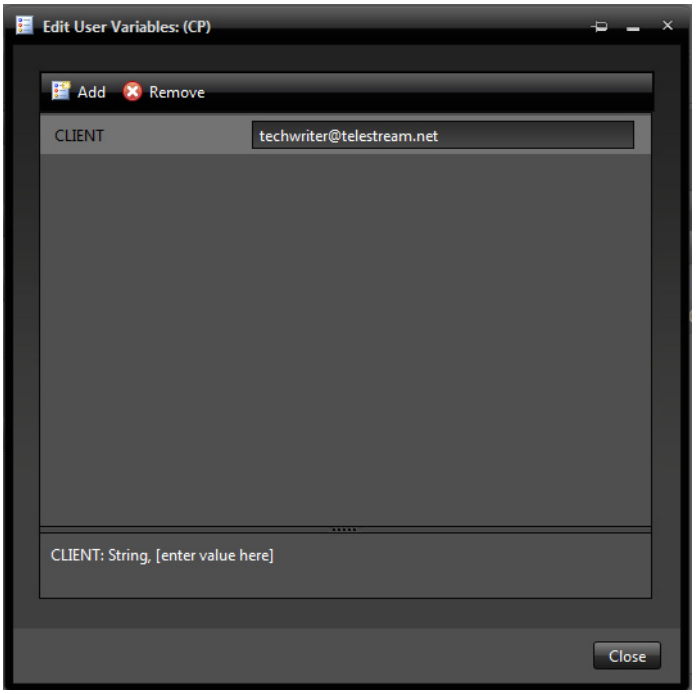
2. Click New in the Vantage Upload User Administration window. The New Upload Portal User window opens.



3. Enter a user name. Typically, you might use the client's company name to help you identify who will be using that account.
4. Enter a password and enter it again in the Confirm Password field.
5. Use the Portal drop-down menu to select the portal that the new account will be assigned to use. Check the Administrator box if you want the user to have administrative privileges.

6. Click to place a check mark in the Administrator box if you want the user to be an administrator.
7. Click Save to save the new user account. The new user name appears in the Vantage Upload User Administration list.
8. Click the new user in the list, and click Variables in the list tool bar if you wish to define any variables for the user. Click Add to Choose a Variable from a list, and then fill in the blank field with a text string to populate the variable.

   For example, you might add a CLIENT variable as shown below and enter an email address. You could then use that variable in your workflows to automatically send an email acknowledgment to the client upon receiving uploaded files.



Note the other user administration buttons for future use:

- Edit—allows you to edit the details of an existing user in the list.
- Delete—lets you delete a user from the list.
- Refresh—refreshes the list of users after you make changes.

User Authentication Setup

For HTTP portals, the target directory for uploaded files in the UNC share may require authentication of a specific Windows user. If so, follow this procedure for each user account:

1. On the Upload Portal web host server, launch Internet Information Services (IIS) Manager.
2. In the left-side navigation tree, expand the hostname for the server and select Application Pools.
3. In the main panel of the IIS Manager under Application Pools, select ASP.NET v4.5 for Windows Server 2012 OS.
4. On the right side of IIS Manager under Actions, Edit Application Pool, click Advanced Settings...
5. In the Advanced Settings window, select Identify under Process Model and click the (...) Browse button.
6. Select the Custom account radio button, and then click the Set... button.
7. Enter the username and password required for authentication to the Target Directory UNC share and click OK.
8. Click OK again to close the Application Pool Identity window.
9. Click OK again to close the Advanced Settings window.
10. On the right side under Actions, click the Stop button.
11. Also under Actions, click the Start button.
12. Close the IIS Manager window. Authentication setup is complete.

Notifying the Customer

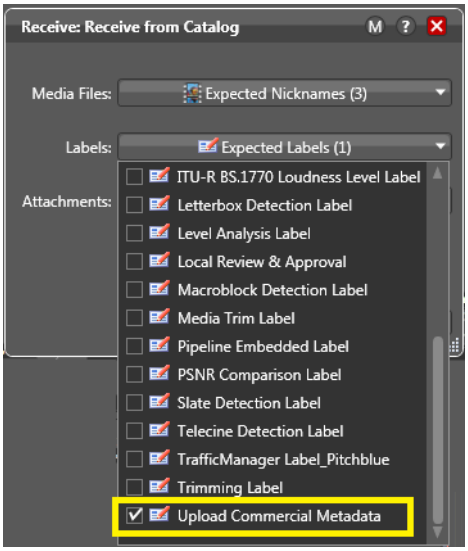
Once the portal and user account have been created for a customer, be sure to send them the URL, user name, and password for the portal and the account. Refer them to the built-in Help menu if they need help using the portal.

Designing Workflows for the Portal

When you create a new Upload Portal, you select a Vantage workflow in the Workflow Designer to receive the media file and metadata inputs from the portal. The workflow must include the appropriate Vantage workflow actions described below in order to automatically create the metadata fields in the portal and to accept the portal inputs for processing.

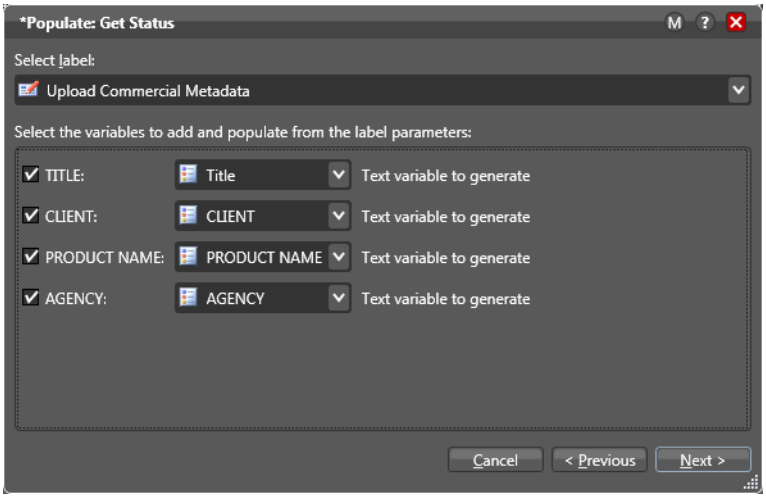
Receive Action

Workflows designed to accept metadata input from Upload Portals begin with Receive actions that use the Upload Commercial Metadata label as shown below. This label receives the metadata that users enter when submitting their commercial via the Upload Portal - Step 2 - Enter Metadata.



Populate Action

A Populate action following the Receive action binds variables to the label parameters. The variables carry the metadata on through the workflow with the media. Select *Variables From Label Parameters* in the Populate action. Next, select the parameters and variables you want to use, as shown below.



The parameters you select using the check boxes (above) are fed back to the Upload Portal to create the fields users see (below) when filling out the Enter Metadata form in Step 2 of the upload process.

Only the actions described above are needed to ensure the Upload Portal and the workflow can operate interactively. The remainder of the workflow can be designed as you desire to manipulate the media and metadata according to the needs of your organization.

Copyrights and Trademark Notices

Explorer, SQL Server 2005|2008|Server 2012, and Windows Media Technologies are trademarks of Microsoft Corporation.

SharpSSH2. SharpSSH2 Copyright (c) 2008, Ryan Faircloth. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Diversified Sales and Service, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Telerik. RadControls for ASP.NET AJAX copyright Telerik All rights reserved.

VoiceAge. This product is manufactured by Telestream under license from VoiceAge Corporation.

x264 LLC. The product is manufactured by Telestream under license from x264 LLC.

Xceed. The Software is Copyright ©1994-2012 Xceed Software Inc., all rights reserved.

ZLIB. Copyright (C) 1995-2013 Jean-loup Gailly and Mark Adler.



Other brands, product names, and company names are trademarks of their respective holders, and are used for identification purpose only.

MPEG Disclaimers

MPEGLA MPEG2 Patent

ANY USE OF THIS PRODUCT IN ANY MANNER OTHER THAN PERSONAL USE THAT COMPLIES WITH THE MPEG-2 STANDARD FOR ENCODING VIDEO INFORMATION FOR PACKAGED MEDIA IS EXPRESSLY PROHIBITED WITHOUT A LICENSE UNDER APPLICABLE PATENTS IN THE MPEG-2 PATENT PORTFOLIO, WHICH LICENSE IS AVAILABLE FROM MPEG LA, LLC, 4600 S. Ulster Street, Suite 400, Denver, Colorado 80237 U.S.A.

MPEGLA MPEG4 VISUAL

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. SEE HTTP://WWW.MPEGLA.COM.

MPEGLA AVC

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

MPEG4 SYSTEMS

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 SYSTEMS PATENT PORTFOLIO LICENSE FOR ENCODING IN COMPLIANCE WITH THE MPEG-4 SYSTEMS STANDARD, EXCEPT THAT AN ADDITIONAL LICENSE AND PAYMENT OF ROYALTIES ARE NECESSARY FOR ENCODING IN CONNECTION WITH (i) DATA STORED OR REPLICATED IN PHYSICAL MEDIA WHICH IS PAID FOR ON A TITLE BY TITLE BASIS AND/OR (ii) DATA WHICH IS PAID FOR ON A TITLE BY TITLE BASIS AND IS TRANSMITTED TO AN END USER FOR PERMANENT STORAGE AND/OR USE. SUCH ADDITIONAL LICENSE MAY BE OBTAINED FROM MPEG LA, LLC. SEE HTTP://WWW.MPEGLA.COM FOR ADDITIONAL DETAILS.

Limited Warranty and Disclaimers

Telestream, LLC. (the Company) warrants to the original registered end user that the product will perform as stated below for a period of one (1) year from the date of shipment from factory:

Hardware and Media—The Product hardware components, if any, including equipment supplied but not manufactured by the Company but NOT including any third party equipment that has been substituted by the Distributor for such equipment (the "Hardware"), will be free from defects in materials and workmanship under normal operating conditions and use.

Warranty Remedies

Your sole remedies under this limited warranty are as follows:

Hardware and Media—The Company will either repair or replace (at its option) any defective Hardware component or part, or Software Media, with new or like new Hardware components or Software Media. Components may not be necessarily the same, but will be of equivalent operation and quality.

Software Updates

Except as may be provided in a separate agreement between Telestream and You, if any, Telestream is under no obligation to maintain or support the Software and Telestream has no obligation to furnish you with any further assistance, technical support, documentation, software, update, upgrades, or information of any nature or kind.

Restrictions and Conditions of Limited Warranty

This Limited Warranty will be void and of no force and effect if (i) Product Hardware or Software Media, or any part thereof, is damaged due to abuse, misuse, alteration, neglect, or shipping, or as a result of service or modification by a party other than the Company, or (ii) Software is modified without the written consent of the Company.

Limitations of Warranties

THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. No oral or written information or advice given by the Company, its distributors, dealers or agents, shall increase the scope of this Limited Warranty or create any new warranties.

Geographical Limitation of Warranty—This limited warranty is valid only within the country in which the Product is purchased/licensed.

Limitations on Remedies—YOUR EXCLUSIVE REMEDIES, AND THE ENTIRE LIABILITY OF TELESTREAM, INC. WITH RESPECT TO THE PRODUCT, SHALL BE AS STATED IN THIS LIMITED WARRANTY. Your sole and exclusive remedy for any and all breaches of any Limited Warranty by the Company shall be the recovery of reasonable damages which, in the aggregate, shall not exceed the total amount of the combined license fee and purchase price paid by you for the Product.

Damages

TELESTREAM, INC. SHALL NOT BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF YOUR USE OR INABILITY TO USE THE PRODUCT, OR THE BREACH OF ANY EXPRESS OR IMPLIED WARRANTY, EVEN IF THE COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES, OR ANY REMEDY PROVIDED FAILS OF ITS ESSENTIAL PURPOSE.

Further information regarding this limited warranty may be obtained by writing:
Telestream, Inc.
848 Gold Flat Road
Nevada City, CA 95959 USA

You can call Telestream, Inc. via telephone at (530) 470-1300.

Part number: 265824

Publication Date: October 2018