

App-V Security Operations Guide

White Paper Descriptor

The purpose of this whitepaper is to provide the App-V administrator with steps to configure security settings. Some of the security settings are well-known configurations within Windows and the appropriate links will be provided.

Copyright © 2008 MICROSOFT CORPORATION

[Introduction 4](#_Toc208823915)

[Audience 4](#_Toc208823916)

[Prior Knowledge 4](#_Toc208823917)

[App-V Components and Services 5](#_Toc208823918)

[List of APP-V Infrastructure Components 5](#_Toc208823919)

[Installing App-V Management Server or Streaming Server Securely 7](#_Toc208823920)

[Configuring Certificates to Support Secure Streaming 7](#_Toc208823921)

[Obtaining and Installing a Certificate 8](#_Toc208823922)

[Modifying Private Key Permissions to Support Management Server or Streaming Server 9](#_Toc208823923)

[Managing Private Keys on Windows 2003 9](#_Toc208823924)

[Use WinHttpCertCfg.exe to set the correct ACL on the private key 9](#_Toc208823925)

[Managing Private Keys on Windows 2008 11](#_Toc208823926)

[Installing App-V Management Server or Streaming Server 13](#_Toc208823927)

[Configuring Certificates for NLB environments 14](#_Toc208823928)

[Configuring Management or Streaming Server for Secure Communications Post-Installation 16](#_Toc208823929)

[Post-Installation Security for App-V Management Server 16](#_Toc208823930)

[Post-Installation Security for App-V Streaming Server 22](#_Toc208823931)

[Troubleshooting Certificate Permission issues 25](#_Toc208823932)

[Error Message 25](#_Toc208823933)

[Sft-server.log 26](#_Toc208823934)

[Configuring Windows Firewall for App-V 27](#_Toc208823935)

[Windows Server 2003 27](#_Toc208823936)

[Windows Server 2008 30](#_Toc208823937)

[Configuring App-V for Secure Administration 34](#_Toc208823938)

[Installing Management Service Securely 35](#_Toc208823939)

[Configuring Certificates to Support Secure Management Service 35](#_Toc208823940)

[Installing and Configuring APP-V MMC for Secure Environment 35](#_Toc208823941)

[Configuring App-V Administration for a Distributed Environment 37](#_Toc208823942)

[Configuring Active Directory (SQLService uses local system account) 38](#_Toc208823943)

[Trust the Computer Account(s) for Delegation 38](#_Toc208823944)

[Configuring Active Directory (SQLService uses domain-based account) 39](#_Toc208823945)

[Configuring IIS for Secure Streaming 40](#_Toc208823946)

[MIME Types 40](#_Toc208823947)

[Kerberos Authentication 40](#_Toc208823948)

[Configuring File Server for Secure Streaming 41](#_Toc208823949)

[App-V Client Security 42](#_Toc208823950)

[Installation/Upgrading 42](#_Toc208823951)

[Permissions 42](#_Toc208823952)

[Registry 42](#_Toc208823953)

[ADM Template 42](#_Toc208823954)

[Removing OSD File Type Associations 43](#_Toc208823955)

[Security when Sequencing 44](#_Toc208823956)

[Virus Scanning on the Sequencer 44](#_Toc208823957)

[Capturing ACLs on Files (NTFS) 45](#_Toc208823958)

[Sequencer Doesn’t Capture Registry ACLs 46](#_Toc208823959)

[Internet-Facing Setup 47](#_Toc208823960)

[Servers in the DMZ 48](#_Toc208823961)

[Servers in the Internal Network 49](#_Toc208823962)

[Traffic required from the Internet to the DMZ 49](#_Toc208823963)

[Client Internet-Facing Considerations 50](#_Toc208823964)

[Domain Joined Client 50](#_Toc208823965)

[Non-Domain Joined Client 50](#_Toc208823966)

[Windows XP 51](#_Toc208823967)

[Windows Vista 54](#_Toc208823968)

# Introduction

The App-V infrastructure can be configured with various security settings. These settings involve App-V components and the underlying infrastructure components to be configured for security. This document provides instructions for configuring security for the components of App-V and the underlying infrastructure.

This document does not provide guidance on choosing security options available in App-V. That information is provided in the App-V Security Best Practices Whitepaper available at <http://go.microsoft.com/fwlink/?LinkId=127120>.

## Audience

This document is created for the administrators responsible for configuring the security features that have been selected for deployment.

## Prior Knowledge

The administrator using this guide should have previous knowledge of the following security-related technologies:

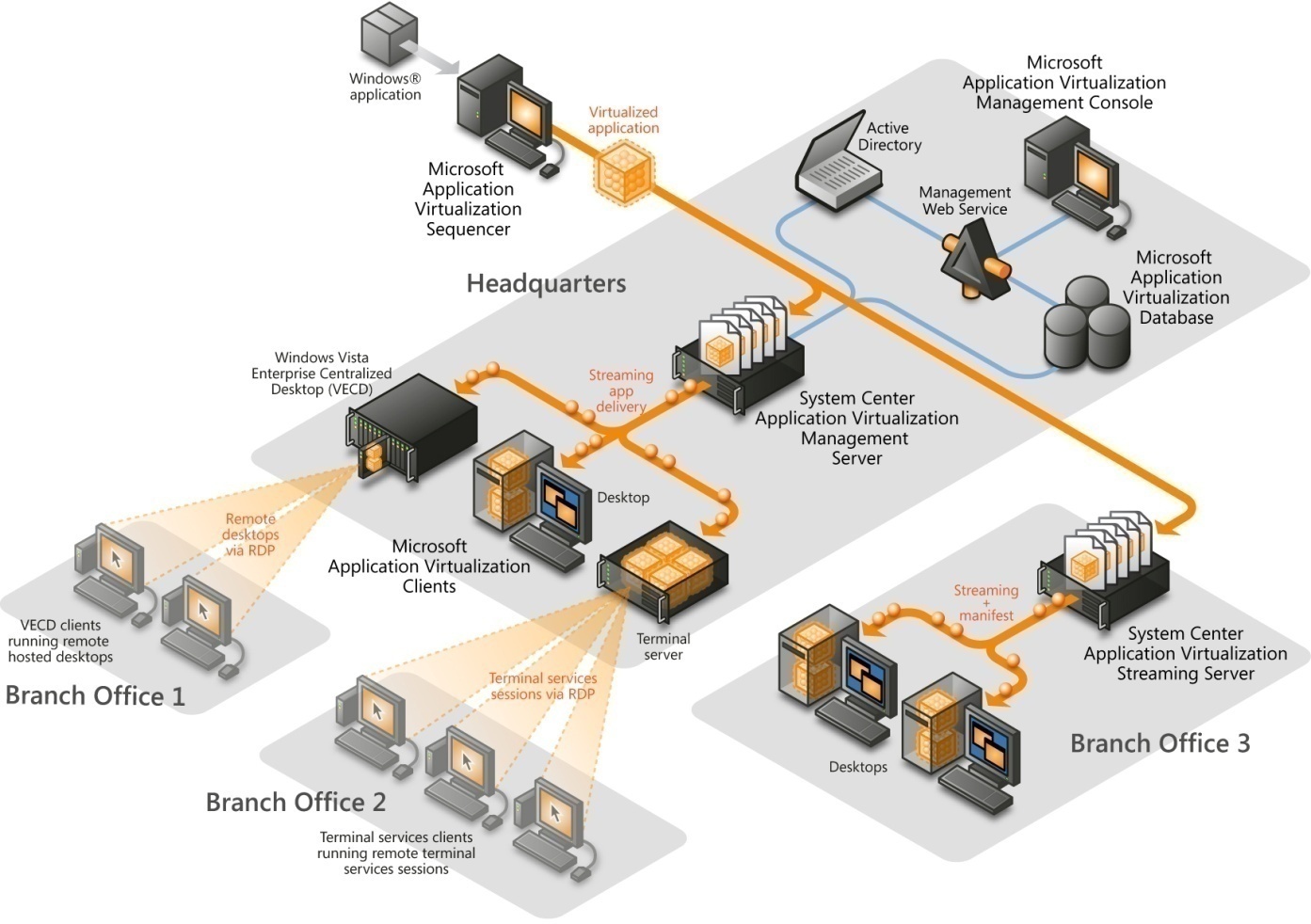
* Active Directory
* Public Key Infrastructure (PKI)
* Internet Protocol Security (IPSec)
* Group Policies
* Internet Information Server (IIS)

Many of the security features are well-known and well-documented elsewhere. This guide will provide external links where the instructions are already available. This document will provide specific instructions for App-V specific settings or other settings that are rarely used or are undocumented.

## App-V Components and Services

Securing a Microsoft Application Virtualization infrastructure requires an understanding of the components which make up the environment. With this new version of App-V, many of the names have changed for previously known components and services, and an additional streaming only server has been added to the App-V infrastructure. The following is a diagram and description of the components that will be discussed in this whitepaper.

Figure 1: Diagram of App-V Infrastructure



### List of APP-V Infrastructure Components

#### App-V Management Server (formerly Virtual Application Server)

This component is responsible for streaming the package content and publishing the shortcuts and file-type associations to the App-V Client.

The App-V Management Server supports active upgrade, License Management, and a database that can be used for reporting.

#### App-V Streaming Server (New!)

This component is responsible for hosting the packages for streaming to clients, such as in a branch office, where the link back to the Management Server is considered unacceptable for streaming package content to clients.

This server contains streaming functionality only and provides neither the Application Virtualization Management Console nor the Application Virtualization Management Web Service.

#### App-V Data Store

This component is stored in the SQL database and retains information related to the Application Virtualization infrastructure.

The information in this store includes all application records, application assignments, and which groups have responsibility for managing the Application Virtualization environment.

#### App-V Management Service (formerly Management Web Service)

This component is responsible for communicating any read/write requests to the Application Virtualization Data Store.

This component can be installed alongside the App-V Management Server or on a separate computer with IIS installed.

#### App-V Management Console

This is a MMC 3.0 snap-in management utility for App-V Server administration.

This component can be installed alongside the App-V Server or on a separate workstation that has MMC 3.0 and .NET 2.0 installed.

#### App-V Sequencer

This component monitors and captures the installation of applications in order to create virtual application packages.

The output of this component consists of the application’s icon(s), an OSD file(s) containing application definition information, a package manifest file, and a SFT file containing the application program’s content files. Optionally, an MSI, for installing the package without using the App-V infrastructure, can be created.

#### App-V Client

This component is installed on the Application Virtualization Desktop Client or on the Application Virtualization Terminal Services Client. It provides the virtual environment for the virtualized applications.

The App-V Client manages the package streaming into cache, publishing refresh, and interaction with the Application Virtualization Servers.

When planning a secure App-V environment, several different infrastructure models can be considered. These models utilize some, but possibly not all, of the components listed previously in this document. For more information on App-V infrastructure models, please refer to the App-V Planning and Deployment Guide or the [App-V Infrastructure Planning and Deployment Guide.](http://go.microsoft.com/fwlink/?LinkId=122063)

# Installing App-V Management Server or Streaming Server Securely

Installing or configuring an App-V Management or Streaming Server to use Enhanced Security (i.e., TLS) requires that an X.509 V3 certificate has been provisioned to the App-V server. When preparing to install or configure a secure Management or Streaming Server some tasks need to be completed. Technical requirements for deploying and configuring certificates for a secure App-V Management or Streaming Server include:

* **Certificate must be valid**. If the certificate is not valid, the client ends the connection.
* **Certificate must contain the correct Enhanced Key Usage (EKU) - Server Authentication (OID 1.3.6.1.5.5.7.3.1).** If the certificate does not contain this EKU, the client ends the connection..
* **Certificate FQDN must match the server on which it’s installed.** This means if the client is calling RTSPS://Myserver.mycompany.com/content/MyApp.sft AND the certificate “Issued To” field is set to “Fooserver1.mycompany.com,” the client will not connect to the server and the session will end. The user will be notified of the failure and why.

NOTE: If using App-V in a Network Load Balanced cluster, the certificate will have to be configured with Subject Alternate Names (SAN) in order to support RTSPS. For information on configuring the certificate authority and creating certificates with SANs, see <http://support.microsoft.com/kb/931351>.

* **Client (and server) needs to trust root CA** – The CA issuing the certificate to the App V Server must by trusted by the client connecting to the server. If not trusted, the client ends the connection.
* **Certificate Private Key has to have permissions changed to allow App-V Service account access to certificate.** By default App-V uses the Network Service account and by default the Network Service account does not have permission to access the private key. This will prevent secure connections.

## Configuring Certificates to Support Secure Streaming

App-V services no longer run under the system context, in contrast to previous versions. By default, the service runs under the Network Service account. However, you can create a service account in Active Directory and replace the Network Service account with the Active Directory Domain account.

The security context the service runs under is important for configuring secure communications. This security context (Network Service by default) must have READ permissions on the certificate private key. When a PKCS#10 Certificate Signing Request (CSR) is generated for the App-V server, the Windows Cryptographic Service Provider is called and a private key is generated. The private key generated is secured with permissions given to the System and Administrator accounts only.

Modifying the ACLs on the private key is required to allow the App-V Management or Streaming Server to access the private key required for successful TLS secured communication. If this is not done, all TLS communications will fail when Schannel attempts to access the key during a TLS transaction.

### Obtaining and Installing a Certificate

There are two scenarios for obtaining and installing a certificate for App-V:

* Internal Public Key Infrastructure
* Third-party certificate issuing Certificate Authority

In the first scenarios, if a PKI infrastructure has been deployed, consult with the PKI administrators to acquire a certificate that complies with the requirements listed above. If no PKI infrastructure is available, using a 3rd-party Certificate Authority to obtain a valid certificate can be completed. The following link provides step-by-step guidance for obtaining and installing a certificate:

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/596cdf5a-c852-4b79-b55a-708e5283ced5.mspx?mfr=true>.

NOTE: If obtaining a certificate from a third-party CA follow the documentation available on that CA’s website.

## Modifying Private Key Permissions to Support Management Server or Streaming Server

In order to modify the permissions of the private key, a Windows Server 2003 Resource Kit tool, WinHttpCertCfg.exe can be used. There are other ways to modify the certificate permissions, however this is the most straightforward and easy way of completing this task. The following steps explain how to modify the permissions of a certificate to support a secure App-V installation.

## Managing Private Keys on Windows 2003

### Use WinHttpCertCfg.exe to set the correct ACL on the private key

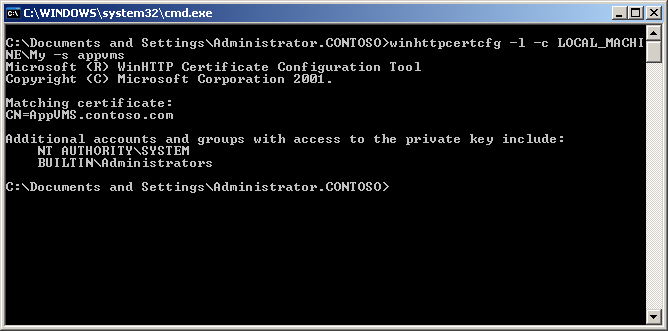
On Windows Server 2003, the process of changing the permissions on the Private Key to support App-V is described in the steps below. This process requires that a certificate that meets the prerequisites listed above has already been installed on the machine or machines that App-V Management or Streaming Server will be installed on.

Additional information on using the WinHttpCertCfg.exe tools is available at the link below.

<http://msdn.microsoft.com/en-us/library/aa384088(VS.85).aspx>

1. On the machine that will become the App-V Management or Streaming server, type the following commands in the command shell to list the current permissions assigned to a specific certificate.

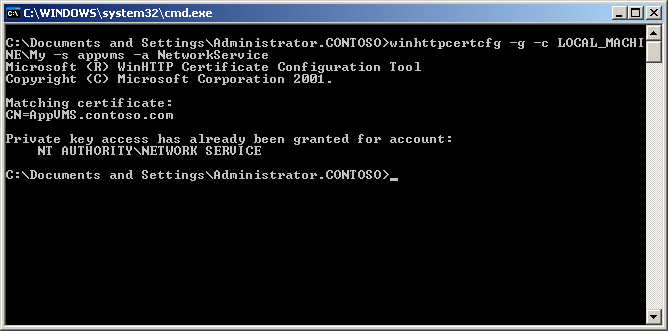
winhttpcertcfg -l -c LOCAL\_MACHINE\My -s Name\_of\_cert



1. Next, if necessary modify the permissions of the certificate to provide read access to the security context that will be used for Management or Streaming Service.

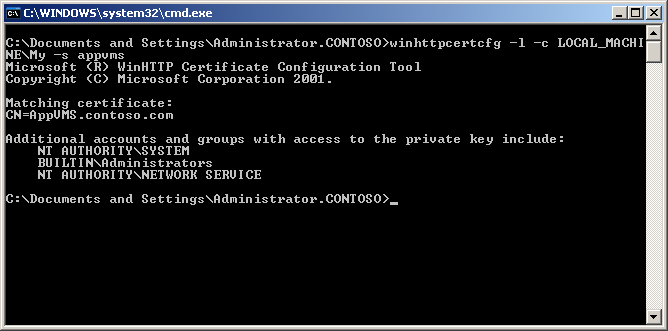
NOTE: The default security context is Network Service, some organizations don’t use built in accounts and a domain account may be used instead.

winhttpcertcfg -g -c LOCAL\_MACHINE\My -s Name\_of\_cert -a NetworkService



1. Verify that the security context was properly added by listing the permissions on the certificate.

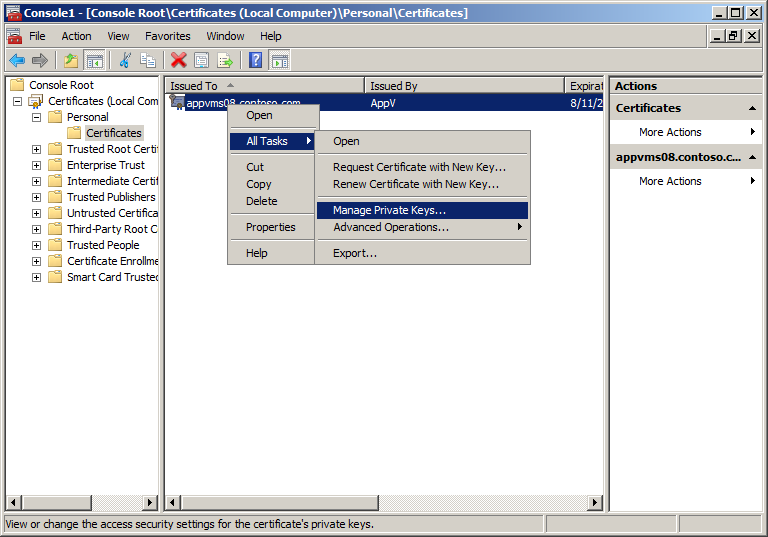
winhttpcertcfg –l –c LOCAL\_MACHINE\My –s Name\_of\_cert



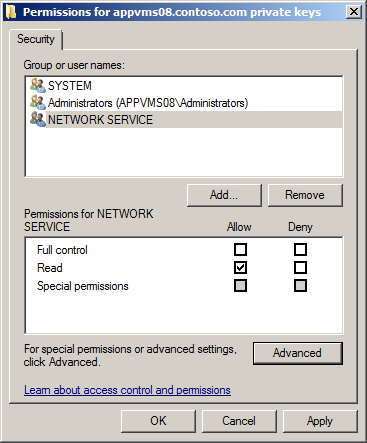
## Managing Private Keys on Windows 2008

Windows Server 2008 makes the process of changing the ACLs on the private key much easier. The certificates GUI can be used to manage private key permissions.

1. Create an MMC with the **Certificates** snap-in that targets the **Local Machine** certificate store.
2. Expand the MMC as shown in the diagram below and select **Manage Private Keys.**

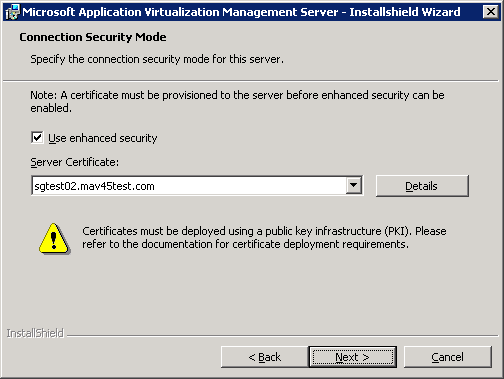


1. Use the **Security** tab to add the **Network Service** account with **Read** access.



## Installing App-V Management Server or Streaming Server

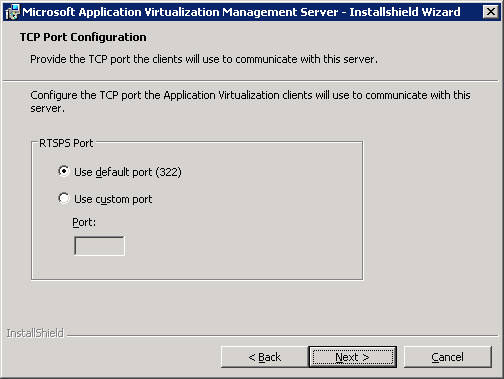
After completing the certificate provisioning process and changing the private key permissions to support the App-V installation, an administrator can launch the setup of either the Management Server or the Streaming Server. During setup, if a certificate is provisioned before executing the setup program, the wizard will display the certificate in the **Connection Security Mode** screen and, by default, will have the **Use enhanced security** check box selected, as shown below.



NOTE: Make sure to select the certificate that was configured for App-V if there is more than one certificate provisioned for this server.

**IMPORTANT: If upgrading from 4.2 to 4.5 the setup offers the option for “Use enhanced security,” however, if it is selected it will not disable streaming over RTSP. The Management Console will need to be used to disable RTSP after installation.**

Next, the administrator will select the TCP port to be used by the service for client communications. The default port is TCP 322, however, this could be changed to a custom port for the organization’s specific environment. The following picture shows the wizard screen.



NOTE: During sequencing the use of RTSPS can be selected so no modification would need to be made to the individual OSD files. However, it will default to TCP Port 322.

All other steps of the wizard are the same as if you were deploying an App-V Management or Streaming Server without using the “Enhanced security” feature.

### Configuring Certificates for NLB environments

In order to support large enterprises, often the Management Server will be placed into a Network Load Balancing (NLB) cluster to support more connections. This requires at least two Management Servers that will appear to be one Management Server. Using a NLB Cluster with several Management Servers presents an advanced configuration of the Certificate used for the NLB Cluster.

This article describes how to add a Subject Alternative Name (SAN) to a secure App-V certificate. The App-V certificate is submitted to a certification authority (CA) that is configured on a computer running Microsoft Windows Server 2003. The SAN lets you connect to a management server NLB cluster hostname by using a Domain Name System (DNS) name other than the individual computer names, since there may be up to 32 individual servers that make up the NLB Cluster. This article includes information about how to add SAN attributes to a certification request that is submitted to an enterprise CA, a stand-alone CA, or a third-party CA.

This configuration is only present when using a NLB cluster, because when the client connects to the server it will be connecting using the FQDN of the NLB Cluster and not the FQDN of the individual server that they are connecting to. Without the addition of the SAN property with the FQDN of the server nodes in the cluster, all client connections will be refused. This is because the common name of the certificate won’t match the server name.

Additional information on configuring Certificates with the SAN attribute is available at: <http://support.microsoft.com/kb/931351>

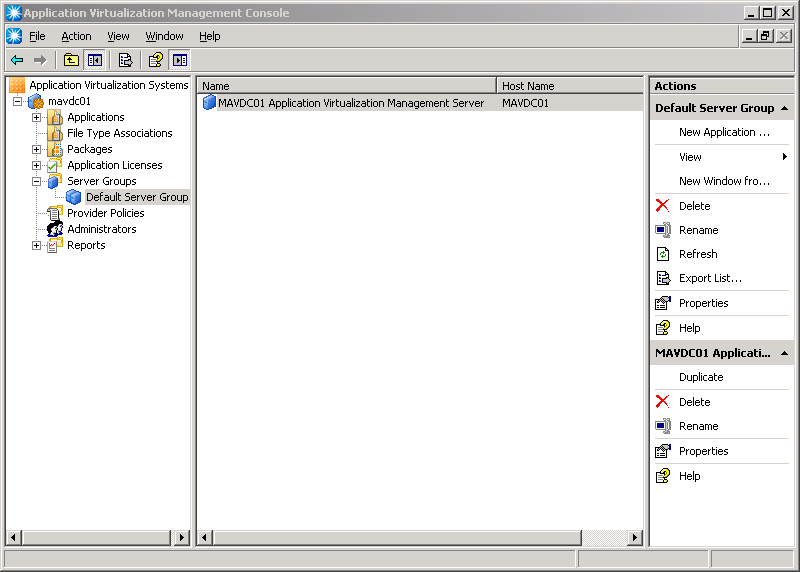
# Configuring Management or Streaming Server for Secure Communications Post-Installation

In many cases, the proper certificate might not be provisioned before the installation of the App-V Management or Streaming Server. App-V can be configured secure after the initial installation. However, the steps used are different as the Management Server can be managed with the App-V Management Console, where the Streaming Server is managed with the registry. In both cases the certificate will have to include the proper EKU for Server authentication and the Network Service has to be given read access to the private key.

## Post-Installation Security for App-V Management Server

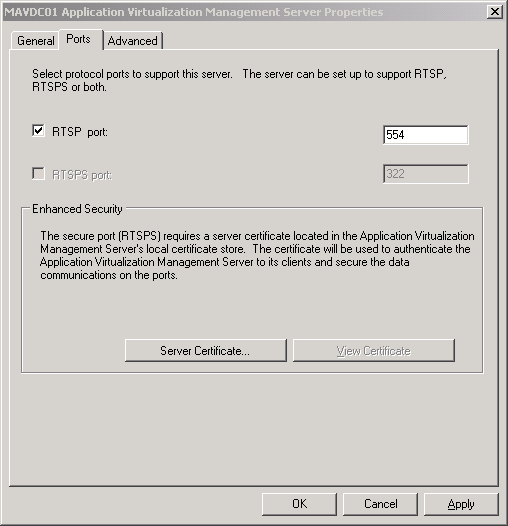
As was mentioned above, the configuration of an App-V Management Server uses the Management Console to add the certificate and configure security. The following steps are for post-installation configuration of security:

1. Open the **App-V Management Console** and connect to the **Management Service** with App-V administrator privileges.
2. Expand the Server, then **Server Groups**, and the appropriate Server Group that the Management Server was registered with.

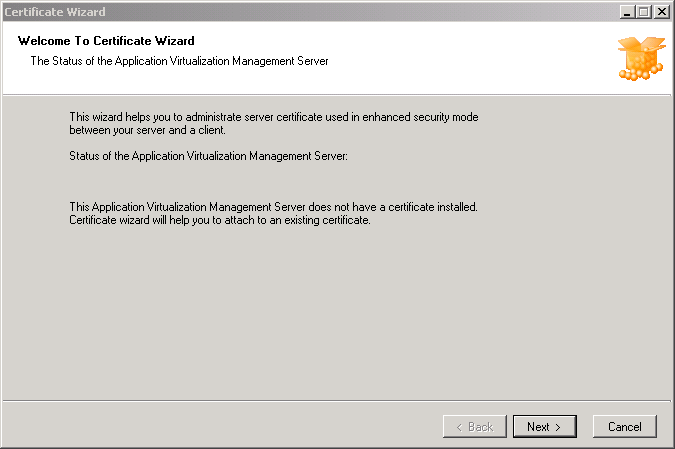


1. **Right-click** the **Management Server object** and select **Properties**.
2. On the **Ports** tab click **Server Certificate** and complete the wizard to select the properly provisioned certificate.

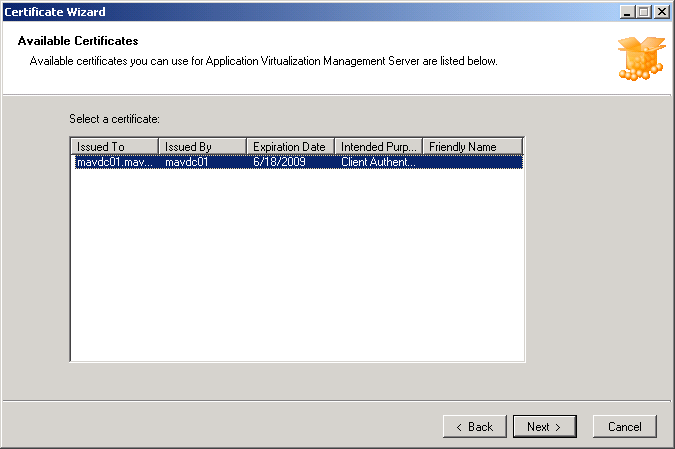
Note: If no certificates are displayed in the wizard, either a certificate has not been provisioned or the certificate does meet the requirements of App-V.



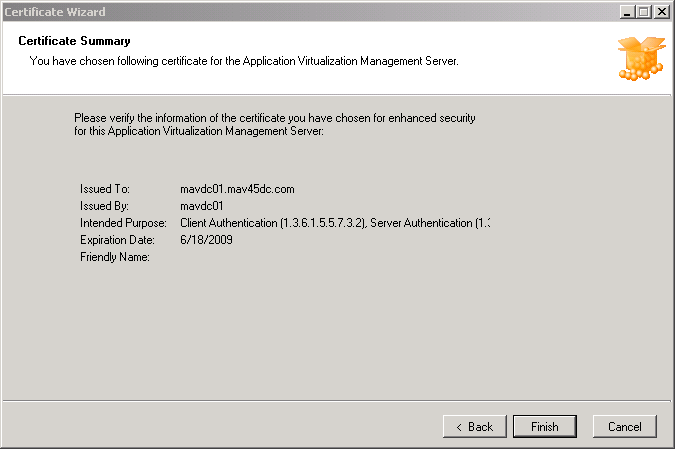
1. Click **Next** to continue the **Welcome To Certificate Wizard** page.



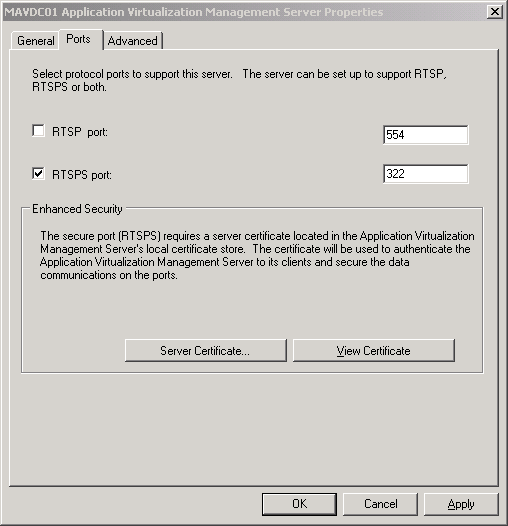
1. Select the correct certificate in the **Available Certificates** screen.



1. After selecting the correct certificate, click **Finish.**



1. After completing the wizard deselect RTSP as an available listening port. This will remove the possibility for connections to be made over a non-secure communication channel.

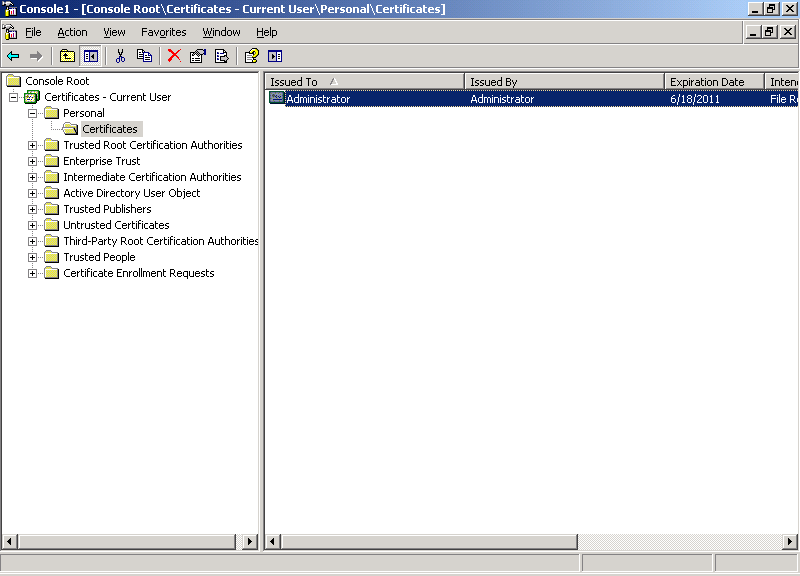


1. Click apply and restart the Microsoft Virtual Application Server service. This can be accomplished using the services MMC snap-in.

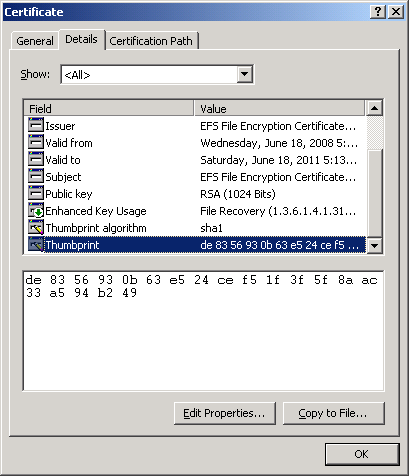
## Post-Installation Security for App-V Streaming Server

The steps for configuring the Streaming Server for secure communications after the installation are different from the Management Server as there is no App-V MMC for configuration. The Streaming Server is managed with the registry. Again, a certificate must be properly provisioned with the correct EKU identifier for Server Authentication prior to completing these steps.

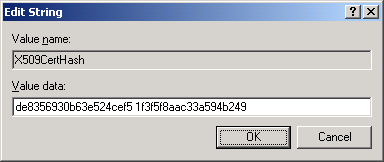
1. Create and MMC and add the **Certificates** snap-in and select the Local Machine certificate store.
2. Open the **Personal** certificates for the machine and **open** the certificate provisioned for App-V:



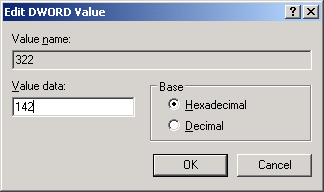
1. On the **Details** tab scroll-down to the **Thumbprint** and copy the **Hash** in the details pane:



1. Open the registry editor and navigate to **HKLM\Software\Microsoft\SoftGrid\4.5\Distribution server**
2. Edit the **X509CertHash** value and **paste** the **thumbprint hash** into the value field and **remove all spaces**. Click on **OK** to accept the edit.



1. In the registry editor navigate to **HKLM\Software\Microsoft\SoftGrid\4.5\Distribution server\RtspsPorts**
2. Create a new **DWORD** value named **322** and enter the data **322 in decimal** or **142 in hex**.



1. Restart the **Streaming Service**.

## Troubleshooting Certificate Permission issues

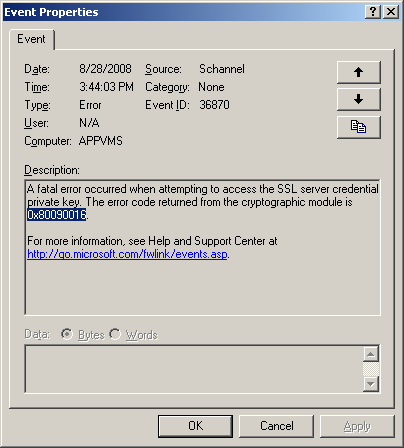
If the private key has not been configured with the proper ACL for the Network Service, an event will be logged in the NT Event Log and an entry is placed in the Sft-server.log file.

### Error Message

**Windows Server 2003**

Event ID 36870

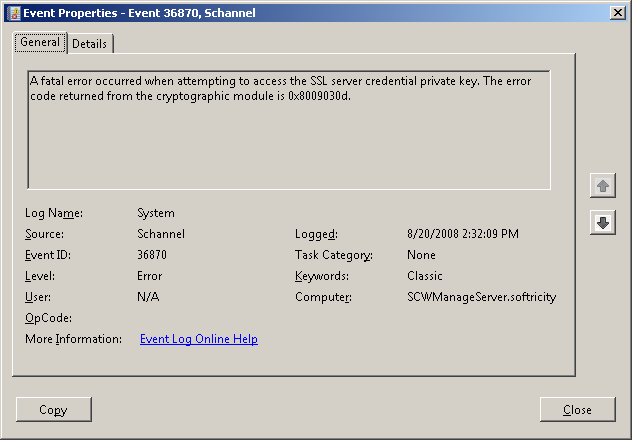
A fatal error occurred when attempting to access the SSL server credential private key. The error code returned from the cryptographic module is 0x80090016.



**Windows Server 2008**

Event ID 36870

A fatal error occurred when attempting to access the SSL server credential private key. The error code returned from the cryptographic module is 0x8009030d.



### Sft-server.log

The following error is placed in the **sft-server.log** file located at **%ProgramFiles%\Microsoft System Center App Virt Management Server\App Virt Management Server\logs** directory:

Certificate could not be loaded. Error code [-2146893043]. Make sure that the Network Service account has proper access to the certificate and its corresponding private key file.

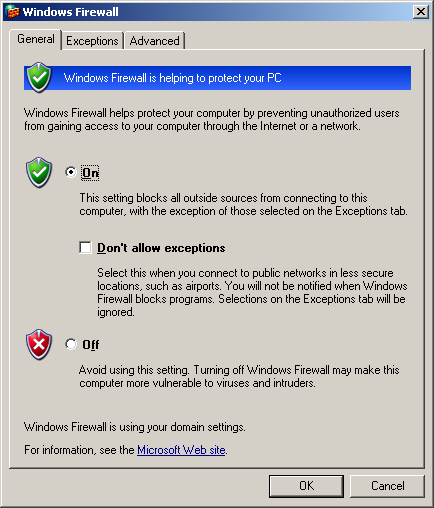
# Configuring Windows Firewall for App-V

Securing the communication between different components in an App-V infrastructure is only one element in securing the environment. Utilizing a firewall program on the server can help reduce the attack surface area. The following steps document the process of configuring Windows built-in firewall capabilities to support App-V. These steps assume that the installation is a Management Server and that it has been configured for RTSPS communication. Notes will be provided for Streaming Servers and environments where RTSP is being used for communication inline.

## Windows Server 2003

1. In **Control Panel** open the **Windows Firewall**.

Note: If the server hasn’t been configured to run the firewall service before this step it will prompt you to start the firewall service.

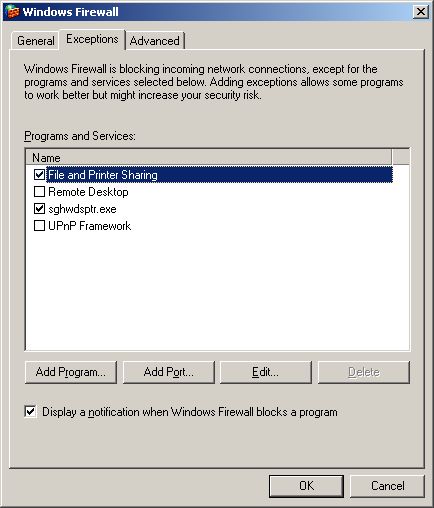


1. If the publishing of ICO and OSD files is done via SMB, ensure that **File and Printer Sharing** is an enabled exception on the **Exceptions** tab.

Note: If the publishing of ICO and OSD files is done via HTTP/HTTPS on the Management Server, an exception would need to be added for HTTP or HTTPS. If the IIS server hosting the ICO and OSD files is hosted on a machine separate from the Management Server, the exception would need to be added to that machine.

Note: For performance reasons it would be recommended to host the ICO and OSD files on a separate server from the Management Server.

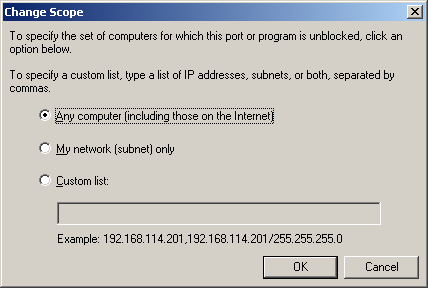
1. Add a program exception for the **sghwdsptr.exe** program which is the Management Server service executable. The default path to this executable is **%ProgramFiles%\Microsoft System Center App Virt Management Server\App Virt Management Server\bin**



NOTE: If the Management Server utilizes RTSP for communication, a program exception for **sghwsvr.exe** will have to be added as well.

NOTE: **App-V Streaming Server** would require that the program exception **sglwdsptr.exe** for RTSPS communication**.** **App-V Streaming Server** that utilizes RTSP for communication will require a program exception for **sglwsvr.exe** as well.

1. Ensure that the proper scope is configured for each exception. Removing **Any computer** and strictly limiting the IP addresses to which the server will respond will reduce risk.



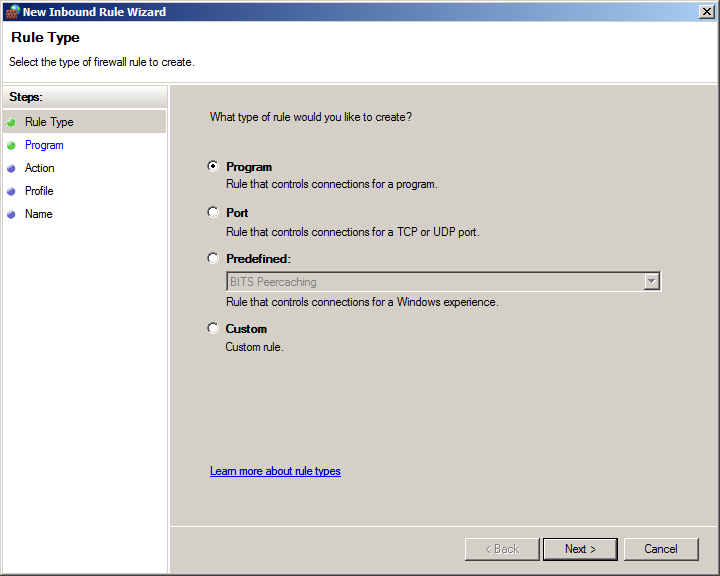
## Windows Server 2008

With the introduction of Windows Server 2008, the firewall and IPSec components were merged into one service and its capabilities were enhanced. The new firewall service supports both incoming and outgoing stateful inspection. Also, management of the specific firewall rules and IPSec policies can be configured via group policies. Additional information on the Windows Firewall in Windows Server 2008 is available at: <http://technet.microsoft.com/en-us/network/bb545423.aspx>

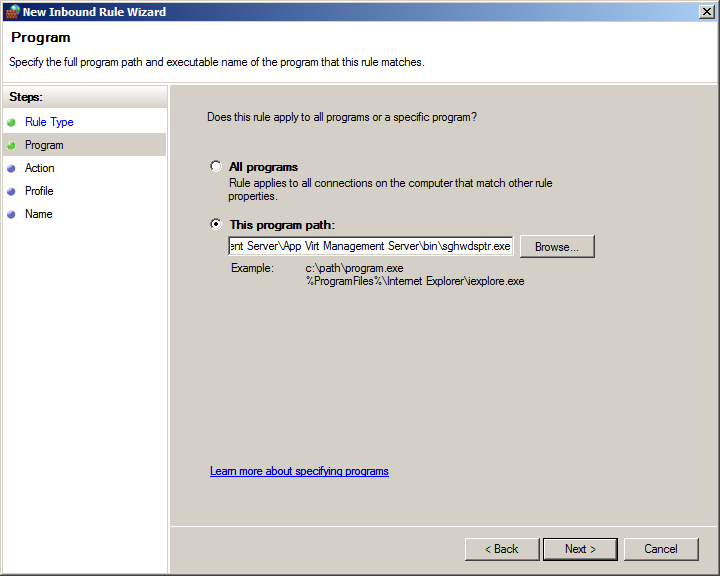
1. Open the **Windows Firewall with Advanced Security** management console via the control panel or by typing **wf.msc** on the Run line.

#### 

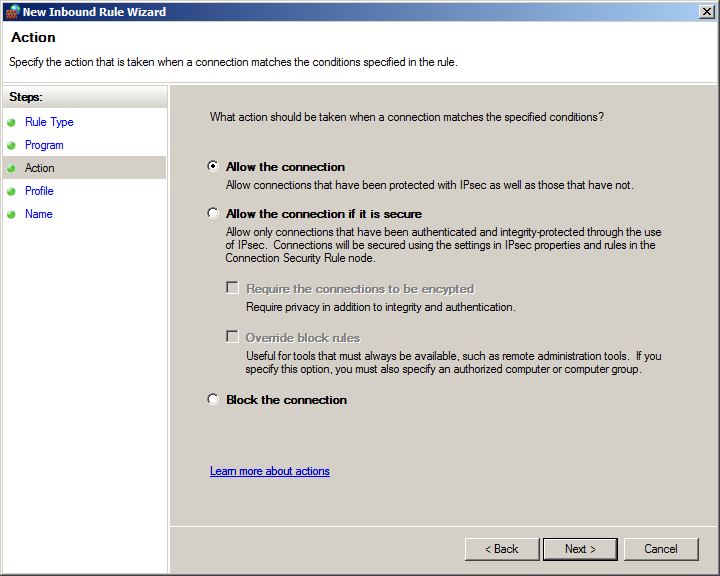
1. Create a new **Inbound Rule** and select **Program.**



1. Select **This program path:** and browse to **sghwdsptr.exe** located by default at: %ProgramFiles%\Microsoft System Center App Virt Management Server\App Virt Management Server\bin**.**
2. Click **Next.**



1. On the **Action** page select **Allow the connection** and select **Next**.



1. Select the appropriate **Profiles** to apply the Inbound Rule.
2. **Name** and provide a **description** for the rule and select **Finish**.

Note: If the **Management Server** is configured to use **RTSP,** repeat the steps to add the **sghwsvr.exe** program as an exception.

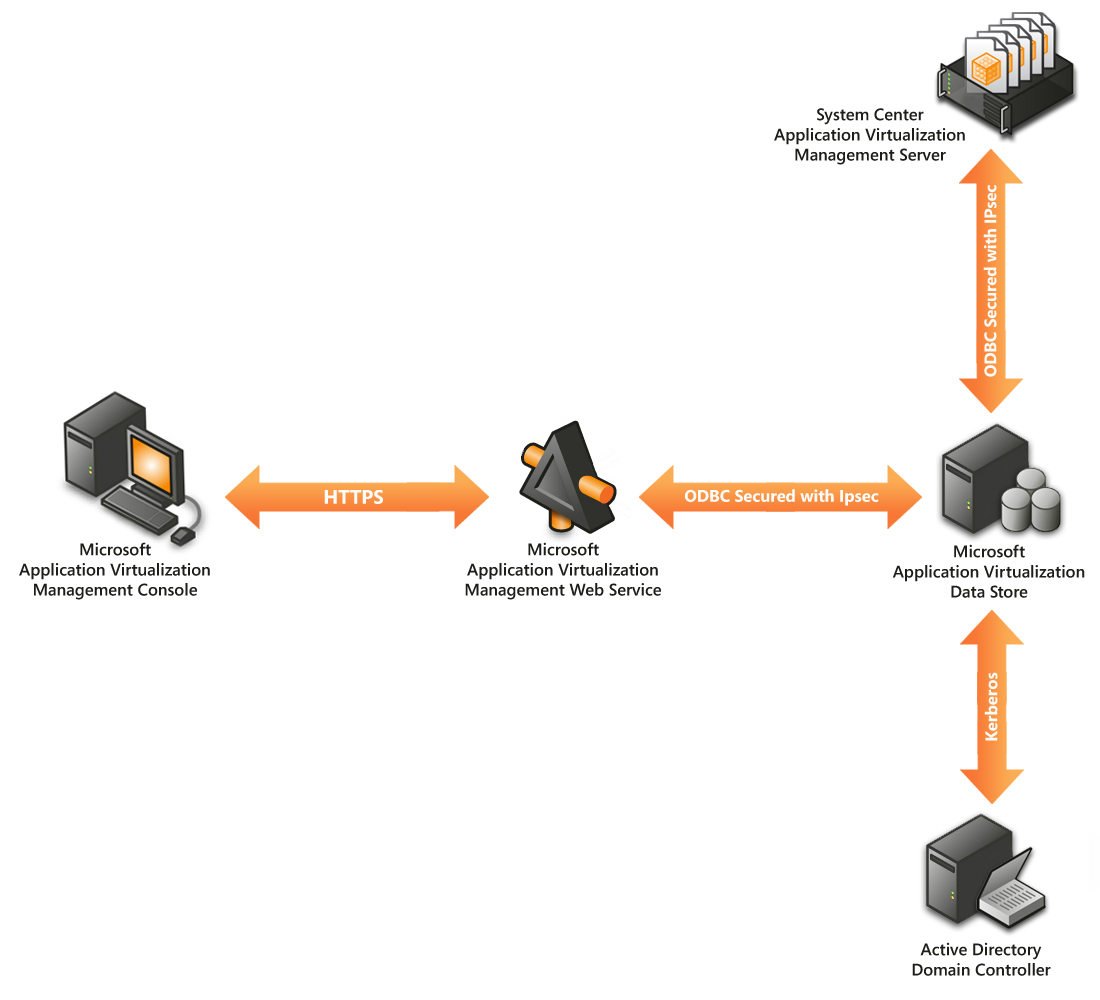
NOTE: **App-V Streaming Server** would require that the program exception **sglwdsptr.exe** for RTSPS communication**.** **App-V Streaming Server** that utilizes RTSP for communication will require a program exception for **sglwsvr.exe** as well.

These steps do not include adding an exception for ICO and OSD publishing via SMB or HTTP/HTTPS. Those exceptions will be automatically added based on the network profile and roles installed on Windows Server 2008 Firewall.

# Configuring App-V for Secure Administration

This scenario is for environments where securing administrative operations is important. App-V allows for the Management Service to require secure communication from the Management Console. Since the Management Service is a web-based application it requires securing the App-V Management application on the web server hosting the management service. This process will include using HTTPS for communication and configuring the IIS server to only allow Windows Integrated Authentication.

Figure 2: App-V Secure Administration Traffic



## Installing Management Service Securely

The Management Service installs as a web-application on IIS. Configuring the Management Service to support secure (SSL) connections between the App-V Management Console and the App-V Management Service, requires configuring the IIS server where the Management Service is installed and configuring the connection on the App-V Management Console.

### Configuring Certificates to Support Secure Management Service

The management service will need to be configured to support SSL-based connections in order to secure the communication. This process requires that the web server or computer that the Management Service is installed on has a certificate issued to the service or computer.

There are several scenarios on how to obtain a certificate for this purpose:

1. The company infrastructure already has a Public Key Infrastructure (PKI) in place that automatically issues certificates to computers.
2. The company infrastructure already has a Public Key Infrastructure (PKI) in place, though it does not automatically issue certificates to computers.
3. The company infrastructure has no Public Key Infrastructure (PKI) in place.

In each of these scenarios how one obtains the certificate is different, but the end result will be the same. The administrator needs to assign a certificate to the IIS Default Web Site and configure the Management Service application to require secure communications.

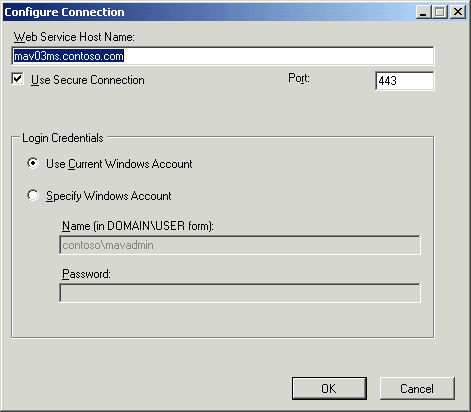
An important aspect of creating certificates for secure communications is that the name of the certificate needs to match the name of the server. It is a best practice to always use Fully Qualified Domain Names (FQDNs) for the common name of the certificate.

App-V can utilize IIS servers to support different infrastructure configurations. Configuring IIS servers to support HTTPS is a well-known task. More information can be found at: <http://technet.microsoft.com/en-us/library/bb727098.aspx>

### Installing and Configuring APP-V MMC for Secure Environment

Installing the App-V MMC automatically includes support for secure communications, which are then configured on a per connection basis when starting the MMC for the first time or connecting to an additional Management Service. The default is to use SSL over TCP port 443. The port number can be changed if it has been modified on the server. The following steps demonstrate the process of connecting to an App-V Management Service using a secure connection.

1. Open the Application Virtualization Management Console.
2. Click on Configure Connection in the Actions pane of the MMC.
3. Type in the Web Service Host Name and ensure that Use Secure Connection is selected.



IMPORTANT: The name provided in the Web Service Host Name must match the common name on the certificate or the connection will fail.

1. Select the appropriate Login Credentials and click on OK.

# Configuring App-V Administration for a Distributed Environment

When designing an infrastructure for a specific organization the App-V Management Service can be installed on a different machine than the App-V Management Server. Common reasons for separating these App-V components include:

* Performance
* Reliability
* Availability
* Scalability

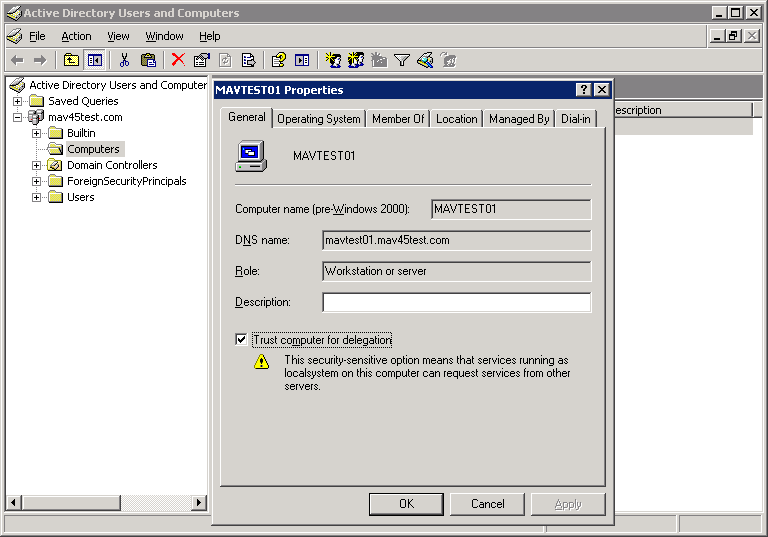
The separation of the Management Server and Management Service requires additional configuration for the infrastructure to operate correctly. When the two components are separated, and the proper steps listed below are not completed, the Management Console will connect to the Management Service but will not be able to properly authenticate with the Data Store. The Management Console will fail to load properly and the administrator will not be able to do any administrative tasks.

This behavior occurs because the Management Service does not have the ability to use the credentials, passed to it from the Management Console, to access the Data Store. The solution is to configure the Management Service server to be “Trusted for delegation.”

## Configuring Active Directory (SQLService uses local system account)

Proper setup in an environment where the SQL Service uses the local system account simply requires an administrator to change the properties of the machine account of the Management Service to be trusted for delegation.

### Trust the Computer Account(s) for Delegation



1. Open **Active Directory Users and Computers** and find the computer account for the machine where the App-V Management Service is installed.
2. **Right-click** on the computer account and select **properties**.
3. Select the check box next to **Trust computer for delegation** and click on **OK**.

NOTE: If the computer that is running SQL Server has a linked server it must also be granted Trust computer for delegation permissions.

NOTE: Windows Server 2008 Active Directory Domain Services automatically trusts computer accounts for delegation; it does not require the above steps.

## Configuring Active Directory (SQLService uses domain-based account)

Setting up an environment where the SQL Server service account is domain-based will require a more extensive setup. SQL Servers use domain-based service accounts for several reasons, such as to support clustering of SQL Server, replication, automated tasks, and linked servers.

Additional information on configuring Active Directory when the SQL Service uses a domain based account is available at: <http://msdn.microsoft.com/en-us/library/ms189585.aspx>

## 

# Configuring IIS for Secure Streaming

The use of HTTP and HTTPS as a protocol for streaming application packages was introduced in App-V 4.5. This option allows organizations to leverage the additional scalability IIS typically offers, via HTTP and HTTPS, over RTSP and RTSPS servers such as App-V Streaming Server. When using IIS as a streaming server, the communications between the client and server should be secured via use of HTTPS instead of HTTP.

Administrators should follow the same steps and rules to securing the content virtual directory as previously described in the Configuring the Management Service for secure administrative communications.

### MIME Types

When using IIS for HTTP or HTTPS streaming of virtual applications, the appropriate MIME types have to be added to the configuration of the IIS server. To support App-V the following MIME types need to be added:

* .OSD=TXT
* .SFT=Binary

Use the following KB article as guidance for adding MIME types

IIS 6.0: <http://support.microsoft.com/kb/326965>

IIS 7.0: <http://technet.microsoft.com/en-us/library/cc753281.aspx>

### Kerberos Authentication

When using HTTP or HTTPS for streaming ICO, OSD, or SFT files using Kerberos authentication enables the best solution from a security perspective. However, in order for IIS to support Kerberos authentication a proper Service Principal Name (SPN) must be configured. The **setspn.exe** tool is available for Windows Server 2003 from the Support Tools on the installation CD and built in to Windows Server 2008.

To create a SPN, run setspn.exe from a command prompt while logged in as a member of Domain Admins. For example: **setspn.exe –A HTTP/FQDN of Server ServerName**

## Configuring File Server for Secure Streaming

With the added support of streaming applications from a file server the communications to the application packages should be secured. This can be achieved using IPsec. The concepts and configuration are described further at the links provided at:

Windows Server 2003

<http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/default.mspx>

Windows Server 2008

<http://technet.microsoft.com/en-us/library/cc732283.aspx>

# App-V Client Security

The App-V Client provides many security enhancements that were not present in previous versions of the product. These changes were made to provide high levels of security either out of the box or through configuration of the client settings.

By default, the App-V Client is configured with only the permissions required to allow a non-administrative user to perform a publishing refresh and stream applications. Other security enhancements provided in the App-V Client include:

* By default an OSD Cache Update is only allowed by a publishing refresh process
* The log file (sftlog.txt) is only accessibly by accounts with local administrative access to the client
* The log file now has a maximum size
* The log files are managed via archive settings
* System Event logging is now performed

## Installation/Upgrading

Installing the App-V Client software on a machine defaults to the most secure settings. However, when upgrading the settings of the client are respected.

After the installation, configure other security settings via registry changes or the ADM Template provided by Microsoft.

## Permissions

The App-V Client has permissions that can be set to restrict regular users or non-administrative users from being able to access all features of the App-V Client. These permissions can be configured through the MMC on an individual client or could be configured using the registry or ADM Template. Additional guidance using the registry and ADM Template is presented in the next sections. For a full list of permissions please reference the App-V Client Help file or App-V Operations Guide.

IMPORTANT: If users in the environment are local administrators of their machines the permissions will be ignored.

## Registry

The App-V Client uses the registry to store its configurations for the client. The keys and values are protected from non-privileged (non-administrative) users by default to prevent a user from tampering with them and modifying their security permissions on the client. A list of the App-V Client Registry keys can be found at: <http://go.microsoft.com/fwlink/?LinkID=121528>

NOTE: App-V client registry keys are all HKEY\_LOCAL\_MACHINE-based and therefore affect the entire machine.

## ADM Template

App-V introduces an ADM Template that can be used to configure the most common client settings through Group Policies. This Template will allow administrators to implement and make changes to many of the client settings from a centralized administration model. Some of the settings available in the ADM Template are security settings.

One important consideration when using the ADM Template is that the settings are Group Policy preference settings and not fully managed Group Policies. To gain a better understanding of this behavior and to successfully deploy clients in an organization, a full description of the ADM Template and the specific settings is available in the App-V ADM Template whitepaper at <http://go.microsoft.com/fwlink/?LinkId=122063>.

### Removing OSD File Type Associations

If an organization does not require the use of opening applications directly from an OSD file, it is recommended for better security to remove the file type associations on the client. Remove the HKEY\_CURRENT\_USERS keys for .osd and Softgird.osd.file using the registry editor. This process could be placed into a logon script or a post-installation script to automate this process.

# Security when Sequencing

The process of packaging applications for App-V or sequencing is the largest ongoing task in an App-V infrastructure. Since this process is an ongoing task, careful consideration should be taken in creating policies and procedures to be followed when sequencing applications. One of the new options available during sequencing is the ability to capture Access Control Lists (ACLs) on the file assets of the virtualized application.

## Virus Scanning on the Sequencer

The recommended practice is to disable all anti-virus and malware detection software on a sequencer workstation during the sequencing process.  This is required to speed the sequencing process and to prevent the anti-virus and anti-malware software components from being detected during sequencing and being included in the virtual application package.

Traditionally install the software on a computer (non-sequencer) and after successful installation, scan the computer for viruses. If viruses are found, the manufacturer of the software should be contacted to inform them of an infected source files and request an updated installation source without viruses. Optionally, the sequencer could be scanned after the installation phase and if a virus is found, the software manufacturer should be contacted as mentioned above.

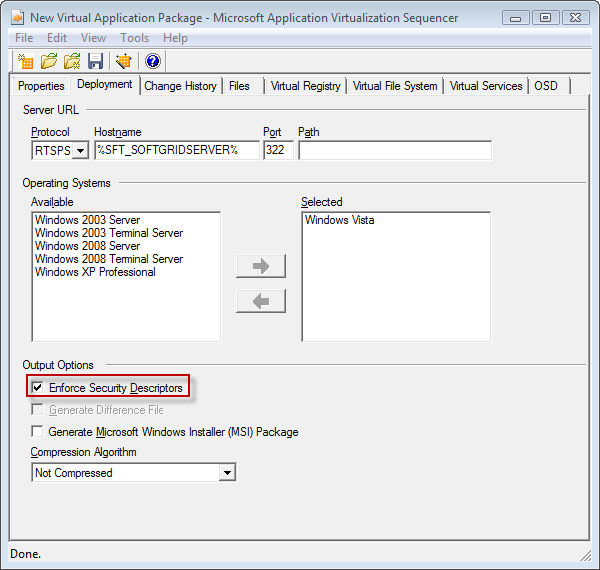
NOTE: If a virus is detected in the application it should not be deployed.

## Capturing ACLs on Files (NTFS)

The App-V Sequencer captures NTFS permissions or the ACLs for the files that are monitored during the installation of the product. This capability allows the sequencing engineer to more accurately capture the behavior of the application as if it were installed locally and not virtualized. In some scenarios an application may store information that users were not intended to access within the application files. An application could store credential information in a file inside of the application. If ACLs are not enforced on the package, a user could potential view and then use this information outside of the application.

NOTE: Applications that store security specific information are not a best practice for applications that are going to be virtualized. Since many applications do this, the ability to secure these locations would be a way of providing the best solution for security.

During the installation phase, a sequencing engineer could modify the default permissions of the files if necessary. After completion of the sequencing process, but before saving the package, the sequencing engineer can choose whether to enforce security descriptors that were captured during the installation of the application. It would be recommended to enforce security descriptors unless no other solution can be made to allow the application to run properly virtualized.



Prior to this release of App-V, ACLs were not captured as part of the sequencing process. This allowed for certain applications to run as low privileged users that would normally require Administrative privileges. This new feature of App-V allows for the application to run more like a traditional installation and adhere to the security that was built by the application developers

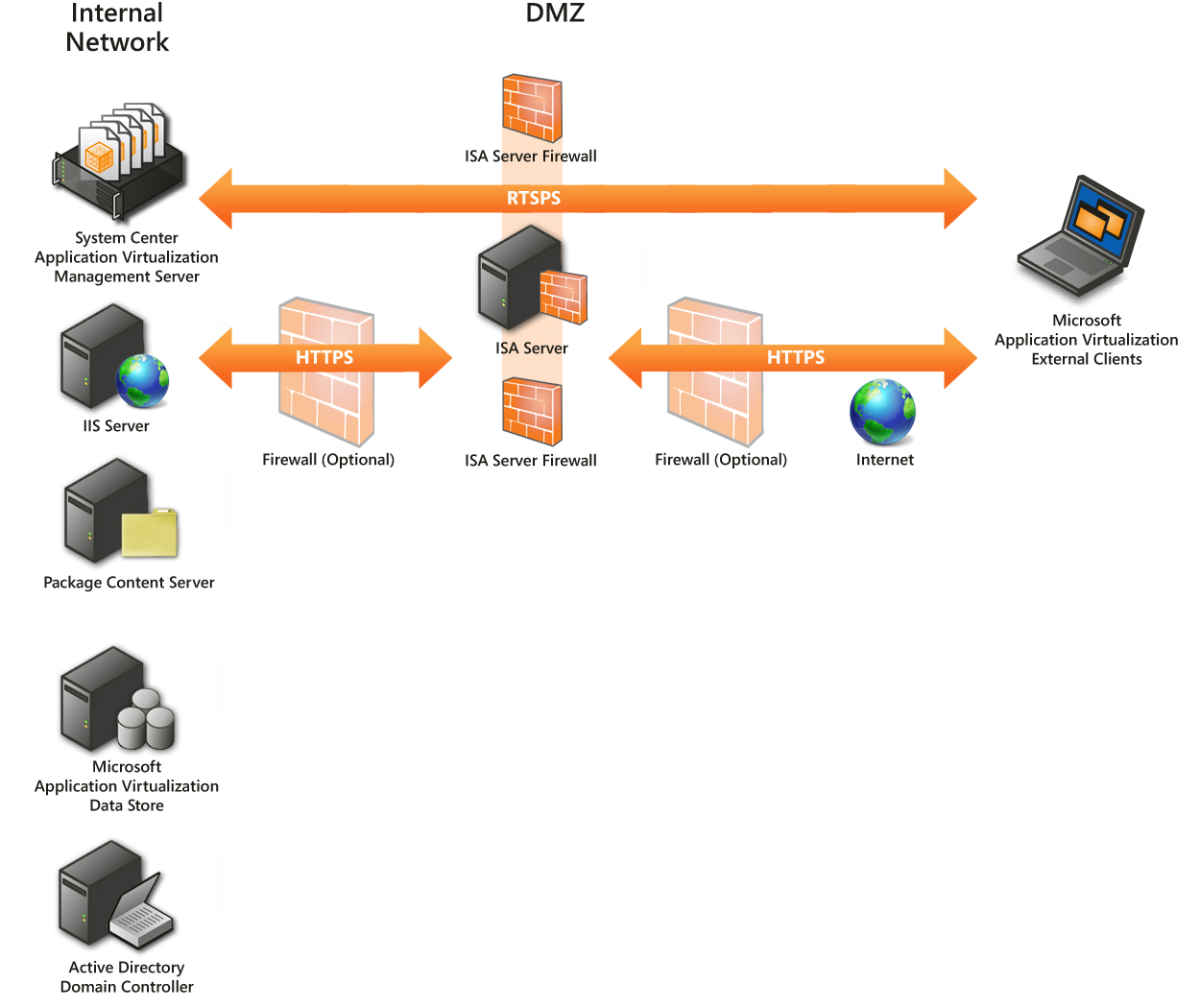
### Sequencer Doesn’t Capture Registry ACLs

Although the sequencer captures the NTFS ACLs during the monitor installation phase of sequencing, it does not capture the ACLs for the registry. Users will have full access to all registry keys for virtual applications except for services. However, if a user modifies the registry of a virtual application, that change will be stored in a specific store (uservol\_sftfs\_v1.pkg) and won’t affect other users.

# Internet-Facing Setup

App-V 4.5 supports internet-facing-server scenarios, in which users that are not on the corporate network or who leave the corporate network can still use App-V. The following scenarios are presented with either step-by-step guidance or pertinent information for completing an internet-facing configuration. The use of non-secure protocols on the internet is not supported (RTSP and HTTP). Follow the guidance earlier in the document for configuring RTSPS and HTTPS communications.

Figure 3: App-V Servers behind ISA

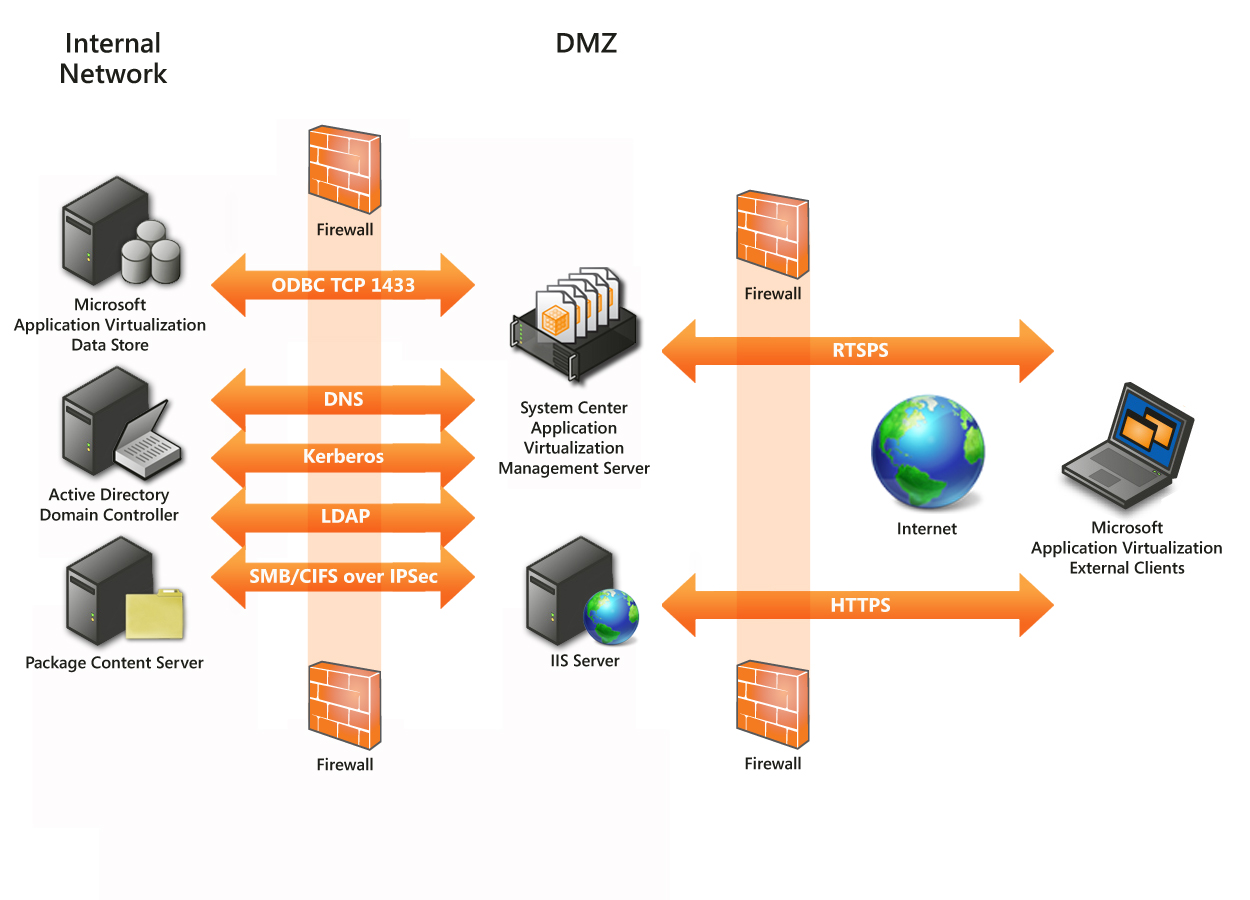


The following tasks explain how to set up an internet-facing App-V solution using ISA server where the App-V infrastructure is on the internal network:

* Create a Web Publishing rule for the IIS Server that is hosting the ICO and OSD files and, optionally, the packages for streaming, located on the internal network. Detailed steps are provided at: <http://technet.microsoft.com/en-us/library/cc723324.aspx>.
* Create a Server Publishing rule for the App-V Server (RTSPS). Detailed steps are provided at: <http://technet.microsoft.com/en-us/library/cc441512.aspx>.

NOTE: If the infrastructure has implemented other firewalls between the client and the ISA Server or between the ISA Server and the internal network, both RTSPS (TCP 322) and HTTPS (TCP 443) firewall rules will need to be created to support the flow of traffic. Also, if firewalls have been implemented between the ISA Server and the Internal network the default traffic required for Domain Members would have to be allowed thru the firewall (DNS, LDAP, Kerberos, SMB/CIFS).

Figure 4: App-V Management Server and IIS Server in DMZ



Because every environment could potentially use different firewall solutions, the guidance provided below is the traffic that would be required to configure an Internet-facing App-V environment in the DMZ and recommended location of servers. In this scenario it would be recommended that only the Management Server and potentially an IIS Server for publishing and streaming be placed in the DMZ. All of the required infrastructure components would be present in the internal network.

### Servers in the DMZ

* App-V Management Server
* IIS Server for publishing and streaming

NOTE: It is recommended to place the Management Server and IIS Server on separate machines.

### Servers in the Internal Network

* Content Server
* Data Store (SQL Server)
* Active Directory Domain Controller

### Traffic required from the Internet to the DMZ

* RTSPS (Publishing Refresh and Streaming packages)
  + TCP 322 by default, this can be changed in App-V Management Server
* HTTPS (Publishing ICO and OSD files; and Streaming packages)
  + TCP 443 by default, this can be changed in IIS configuration

**Traffic required from the DMZ to the internal network:**

* SQL Server
  + TCP 1433 is the default but can be configured in SQL Server
* SMB/CIFS if the content directory is located remotely from the Management Server(s) or IIS server (recommended)
  + Microsoft File Sharing SMB requires TCP ports 135 thru 139
  + Direct Hosted SMB requires both TCP and UPD port 445 (preferred choice)
* Kerberos
  + TCP and UDP 88
* LDAP
  + TCP and UDP 389
* DNS for name resolution of internal resources (this could be eliminated with the use of hosts file on DMZ servers)

## Client Internet-Facing Considerations

### Domain Joined Client

Clients that are domain joined but are outside of the internal network could accomplish communications with the App-V infrastructure by using a VPN connection. Cases where administrators want to provide the ability of users to leave the internal network but still participate in an App-V infrastructure require very little setup. Because the users are already part of the domain, administrators will have to ensure that Cached Credentials are supported on the client. This is the default configuration and any changes to this setting can be accomplished from Group Policies. As mentioned in the App-V Security Best Practices Guide, the user will attempt to send their user ticket to the App-V infrastructure for authentication. If the ticket is expired then it will revert to using NTLM and the cached credentials on the machine. In order to allow roaming, administrators will need to ensure that the publishing server being accessed internally is available at the same name externally for name resolution to work properly.

### Non-Domain Joined Client

In an environment where the clients that need to participate in the App-V infrastructure are non-domain joined machines, configuration on the client will be required to ensure that authentication to the App-V infrastructure can be performed successfully. The App-V Client does not allow for users to be prompted for the publishing refresh process, so the client will need to be configured for the proper credentials to be presented to the App-V Management Server.

The publishing server that has been configured for the non-domain joined client to perform publishing refresh with will require that the external name that clients are accessing is configured as the common name or a subject alternate name (SAN) on the publishing server’s certificate.

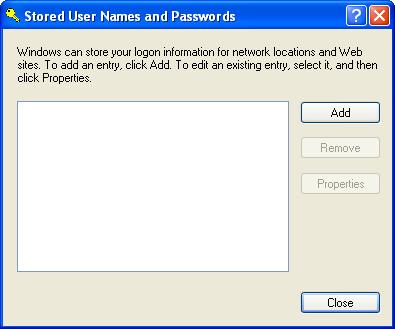
The following steps will need to be performed on the client to ensure that the proper credentials are configured for the user:

### Windows XP

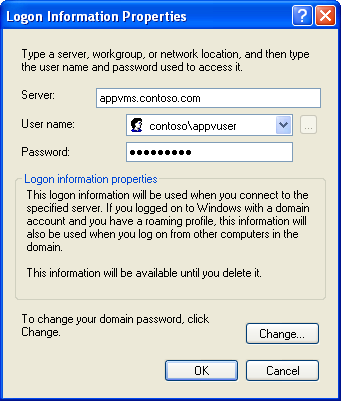
1. On the Windows XP App-V Client an administrator or user with proper rights, open the **User Accounts** from the **Control Panel.** (Classic Control Panel)
2. Next click on the **Advanced Tab** and select **Manage Passwords.**



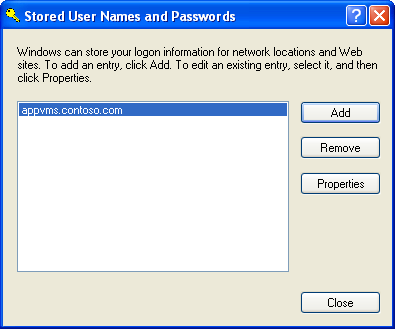
1. On the **Stored User Names and Passwords** screen click on **Add.**



1. On the **Logon Information Properties** fill out the following fields with information from the App-V infrastructure:
   1. Server: Name of Publishing Server external name.
   2. User name: User name for external user in the form **Domain\username.**
   3. Password: Password for the username entered in the User name: field.



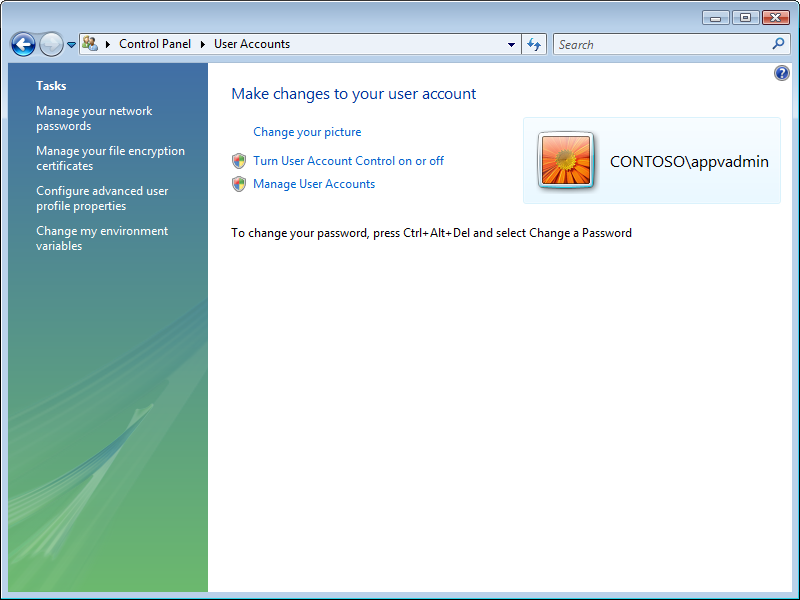
1. Click on OK and the credentials will be stored on the client.



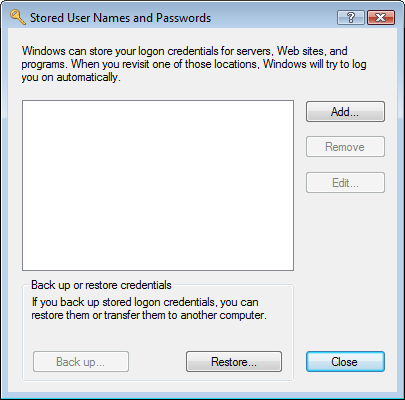
After finishing this process the non-domain joined client will be able to perform a publishing refresh without being joined to a domain.

### Windows Vista

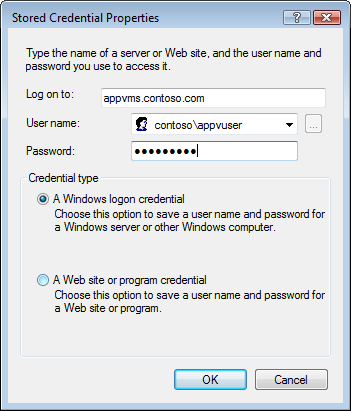
1. On the Windows Vista App-V Client an administrator or user with rights, open **User Accounts** in the **Control Panel**. (Classic View)



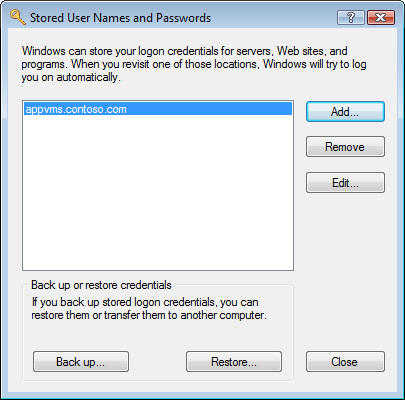
1. Select **Manage your network passwords** from **User Accounts** in the left tasks pane.
2. Select **Add** on the **Stored User Names and Passwords** screen.



1. In the **Stored Credential Properties** provide the information for the App-V infrastructure:
   1. Log on to: External name of the App-V Publishing Server
   2. User name: Enter the username for the external user in the form **Domain\Username.**
   3. Password: Enter the password for the user account entered in the User name: field.
   4. Leave the selected **Credential Type** and click **OK.**



1. Click on close and the credentials are stored in the credential store for proper authentication to the App-V infrastructure.



This task would need to be completed on all non-domain joined machines, which could be a very tedious operation based on the number of non-domain joined machines. The use of scripts and the command line interface into Credential Manager would allow administrators to work towards automating this process.