

App-V Security Best Practices

App-V Security Best Practices

This document provides administrators with the starting place for designing security into the App-V infrastructure. The following document describes recommended security configurations available in App-V today.

Copyright © 2008 MICROSOFT CORPORATION

[Introduction 4](#_Toc208824225)

[App-V Components and Services 5](#_Toc208824226)

[List of App-V Infrastructure Components 5](#_Toc208824227)

[Before You Begin 7](#_Toc208824228)

[Securing the Environment 7](#_Toc208824229)

[Operating System 7](#_Toc208824230)

[SQL Server 7](#_Toc208824231)

[Networking Infrastructure 8](#_Toc208824232)

[Securing Application Virtualization Communications 9](#_Toc208824233)

[Server to Server 9](#_Toc208824234)

[Data Store 9](#_Toc208824235)

[Content 9](#_Toc208824236)

[Client to Server 10](#_Toc208824237)

[Publishing Refresh 10](#_Toc208824238)

[Configuring App-V Management or Streaming Server for RTSPS 11](#_Toc208824239)

[Configuring IIS with HTTPS to Support App-V Operations 12](#_Toc208824240)

[App-V Client to Management Server for Package Streaming 12](#_Toc208824241)

[Management Console to Management Service 12](#_Toc208824242)

[App-V Server Security 13](#_Toc208824243)

[Application Level Security 13](#_Toc208824244)

[App-V Client Security 15](#_Toc208824245)

[Authorization 15](#_Toc208824246)

[ADM Template 16](#_Toc208824247)

[Registry 16](#_Toc208824248)

[Virus Scanning the Client 16](#_Toc208824249)

[Roaming Profiles\Folder Redirection 16](#_Toc208824250)

[App-V Sequencing Security 17](#_Toc208824251)

[Virus Scanning on the Sequencer 17](#_Toc208824252)

[Capturing ACLs on Files (NTFS) 17](#_Toc208824253)

[Sequencer Doesn’t Capture Registry ACLs 18](#_Toc208824254)

[Application Services 19](#_Toc208824255)

[Persisted Security Information 19](#_Toc208824256)

[Internet-Facing Scenarios 20](#_Toc208824257)

[App-V Servers Behind ISA 21](#_Toc208824258)

[App-V Servers in DMZ 22](#_Toc208824259)

[Client Internet Facing Considerations 23](#_Toc208824260)

[Conclusion 24](#_Toc208824261)

# Introduction

One of the biggest challenges today for infrastructure administrators is how to provide a secure, yet productive and supportable, environment. As many organizations begin planning and deploying Microsoft Application Virtualization 4.5 (App-V), an understanding of the security capabilities and best practices for administrative and operational tasks is important for any infrastructure administrator. Security of the App-V system relies on proper setup of the software and the environment in which it operates. This document covers, describes, and provides guidance for configuring the various components of App-V from a security perspective. Administrators should carefully consider their exposure and attack surface before deciding to deploy a system without the security recommendations outlined in this document.

Development of App-V 4.5 followed the standard Microsoft Security Development Lifecycle, which includes security initiatives such as:

* Trustworthy Computing (TwC)
* Secure Windows Initiative (SWI)
* Security Development Lifecycle (SDL)

These development practices and design goals provide many new features and scenarios that can be supported in an enterprise. App-V 4.5 security features and enhancements include:

* Support for Internet-facing
* Adoption of Kerberos Authentication and Authorization
* “Secure by Default” configuration– all of the highest security settings are the defaults for installation out of the box
* Secure logfile access and control over logfile size
* Secure user permissions to the App-V Desktop Client
* Ability to capture file-based ACLs as part of the sequencing process

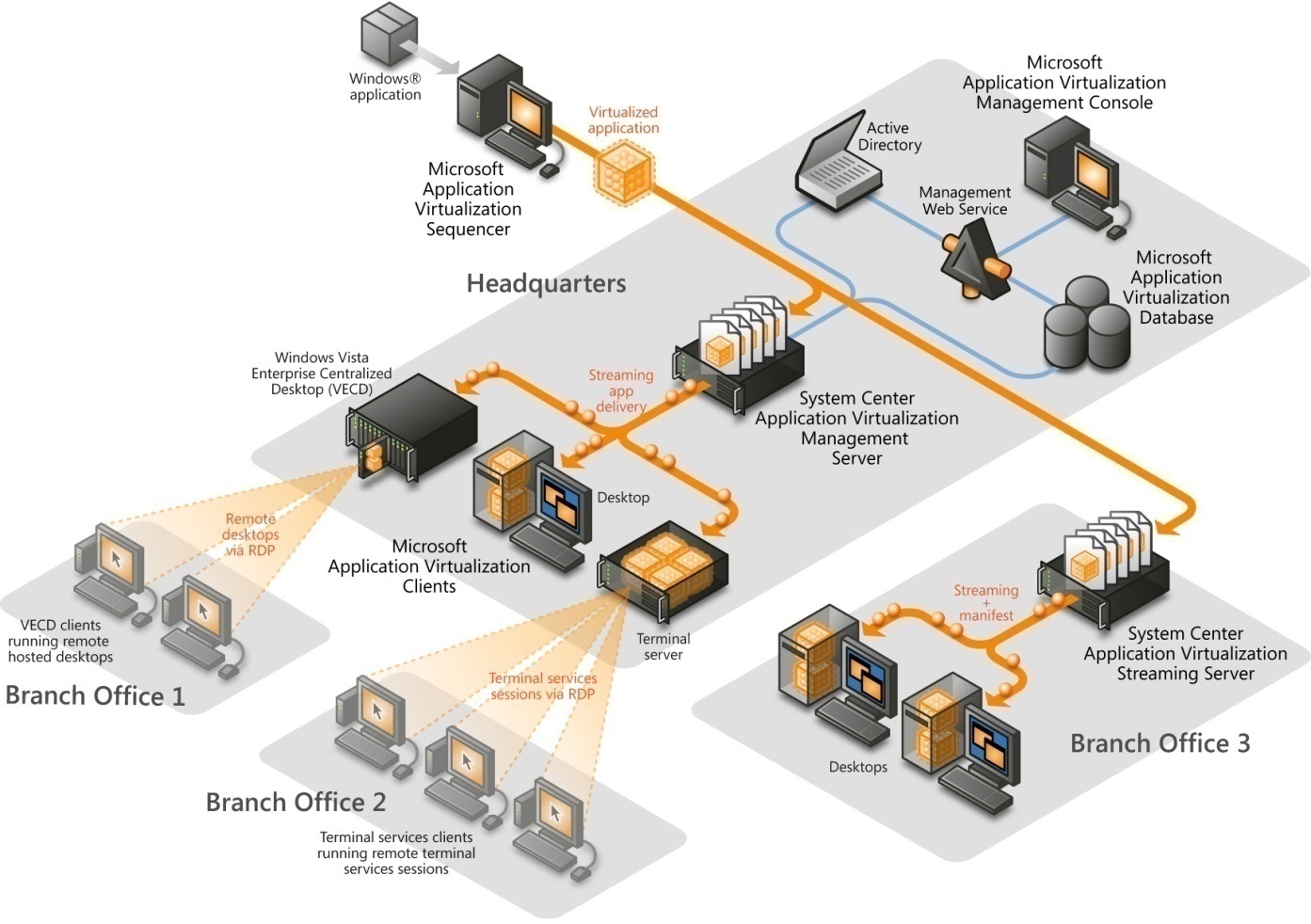
Most of the features and enhancements listed above require or allow the administrator to choose which security features to implement and are described later in this document. Other features, not requiring nor allowing such configuration, are not covered in detail herein. Detailed steps for securing App-V are provided in the App-V Security Operations Guide at <http://go.microsoft.com/fwlink/?LinkId=127120>.

One of the largest dependencies for implementing a secure App-V environment is on certificates to enable secure communication between the server and client. Certificates are used for securing many types of network communication in an App-V infrastructure. Further documentation will be provided in the form of links for setting up an environment to support creation and deployment of certificates. This process is well-known, so this document will point out steps unique to App-V.

## App-V Components and Services

Securing an App-V infrastructure requires an understanding of the components which make up the environment. This new version of App-V (previously “SoftGrid”) changes the names for several components and services; further, an additional streaming-only server has been added to the infrastructure. Figure 1 diagrams and describes 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 Design Guide.](http://technet.microsoft.com/en-us/library/bb897450(TechNet.10).aspx)

# Before You Begin

Increasing security in any environment requires looking at all exposure to potential threats in the environment. Providing security for an App-V infrastructure requires using the App-V specific security features and the normal security practices for the underlying infrastructure. In an App-V infrastructure, data specific to launching applications, configuration information, and other security sensitive information is transmitted on the network and is susceptible to security threats, like a man in the middle attack. Securing these communications is imperative to provide security of the data transmitted by App-V. Securing the underlying infrastructure for services like IIS, Active Directory, and SQL will improve the overall security for an App-V infrastructure. This document provides general guidance and links to documentation that provide additional information to secure the infrastructure.

## Securing the Environment

An App-V infrastructure relies substantially on these components:

### Operating System

Hardening the operating system that the App-V infrastructure will be installed on is an important step in providing the most comprehensive security solution. The operating system could be a weakness in your App-V infrastructure if proper security is not implemented. Many of the tasks for securing the operating system are common practice in today’s IT world. Detailed guidance on securing the server operating system is provided in the two following guides:

[Window Server 2003 Security Guide](http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en)

[Windows Server 2008 Security Guide](http://www.microsoft.com/downloads/details.aspx?FamilyID=fb8b981f-227c-4af6-a44b-b115696a80ac&displaylang=en)

Some of the general security configurations to evaluate are:

* Operating system patching
* Physically securing servers
* Reducing attack surface
* Reducing default permissions and rights
* Hardening file servers
* Hardening web servers

### SQL Server

App-V utilizes SQL Server to store configuration and usage information. General security hardening should be performed on SQL Servers before installing App-V into the environment. Detailed information is provided in the SQL Server 2005 Security Best Practices Guide (<http://www.microsoft.com/technet/prodtechnol/sql/2005/sql2005secbestpract.mspx>). Some of the general security configurations to evaluate are:

* Surface area reduction
* Authentication mode
* Network connectivity
* Service account selection and management

### Networking Infrastructure

Mitigating the risks of the networking infrastructure is important and often a difficult task. Typically, untrusted users have access to the organization’s network through wired and wireless connections. These users are potential (even if unwitting) threats to the network and the App-V infrastructure. Although this guide doesn’t provide guidance on securing your network infrastructure, it will provide guidance in configuring the App-V infrastructure to minimize the threats present on the network.

### 

# Securing Application Virtualization Communications

App-V implements many different methods of communication among the various components of the infrastructure. The practice of increasing security involves evaluating risks and then mitigating those risks. When planning an App-V infrastructure, securing the communications between server-to-server and client-to-server can reduce the risks that might already be present on the existing network.

## Server to Server

### Data Store

The Application Virtualization Management Server and Management Service communicate with the data store utilizing a SQL connection over TCP port 1433. The Management Server uses the data store to retrieve application and configuration data, and also writes usage information to the database. The Management Service communicates with the data store on behalf of an administrator who is configuring the App-V infrastructure. Because the data store contains critical information, it is important to eliminate any threats to this data.

It is recommended that communications between App-V Management Server, Management Service and the Data Store are secured with IPsec. Specifically, create policies that secure the communication channel between the Data Store (SQL) and Management Server; and the Data Store (SQL) and the Management Service. Another option is to deploy server and domain isolation with IPsec ensuring all App-V infrastructure components only communicate with secure channels. Additional information on implementing IPsec is available 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>

### Content

The App-V Management Server installation configures a location for the content directory. This directory is the location where the virtualized application packages are placed for the Management or Streaming Server to retrieve them for streaming. This location could be local to the server or it could be placed on a remote network share. Also, when utilizing a SAN-based environment, the option for remote storage is present. Therefore, implement IPsec to secure the communication with a remote location for the content directory.

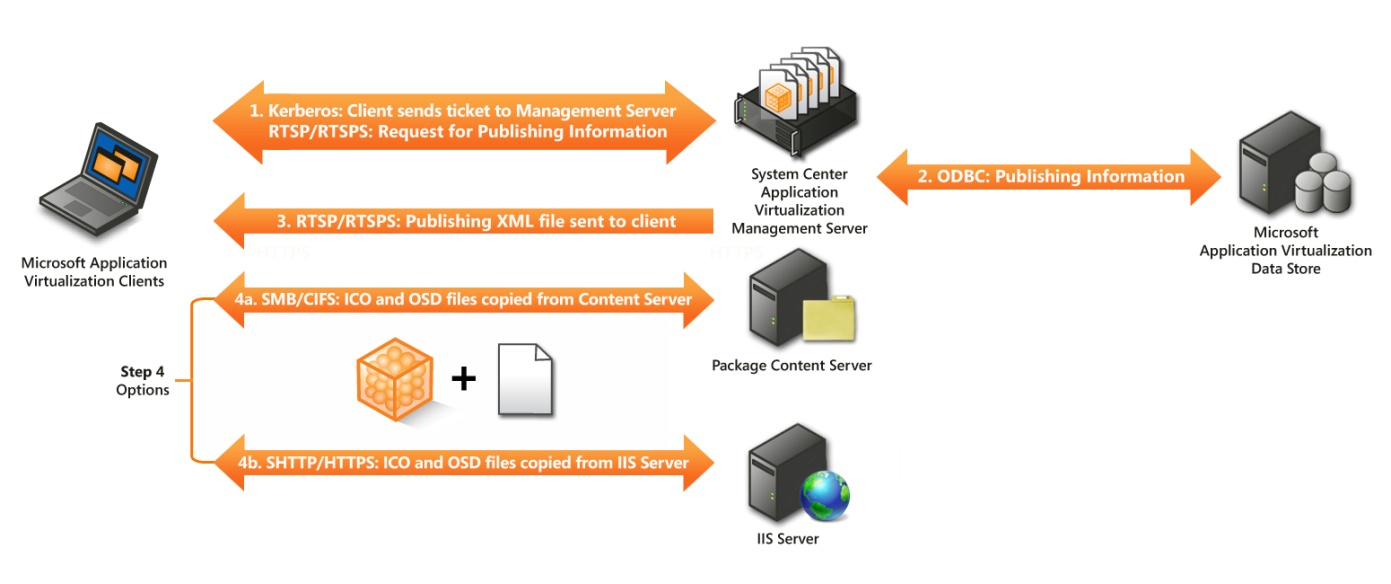
Another option for streaming packages to the clients is to utilize a virtual directory on an IIS server. If the virtual directory that is created for content is located on a remote source, it is recommended to secure the communication between the IIS server and the remote storage location with IPsec.

## Client to Server

### Publishing Refresh

In a connected App-V infrastructure the client communicates with the server to perform a publishing refresh. The publishing refresh is done at user logon by default, can be triggered by the user, and can be configured to occur at a timed interval. The publishing refresh is done under the logged on user’s credentials and information about the application packages is passed to the clients for proper publishing. It is important to secure the communication that occurs between the App-V client and App-V Management Server to ensure that none of the publishing information is sent in a non-secure channel. The publishing data is sent from the Management Server to the client in a XML file, which has no built-in security and contains the path to OSD files. If this information was compromised someone could redirect App-V clients to launch applications using a malicious OSD file. Two steps occur during a publishing refresh:

Figure 2: Publishing Refresh Traffic



1. Receive application publishing information in which a client makes a request to a management server for a list of published applications. This information is sent back to the client in the form of a XML file via:

* RTSP/RTSPS

NOTE: Using RTSPS utilizes Transport Layer Security (TLS) and only supports server authentication. There is no support for mutual certificate authentication between the client and the server. The client only verifies the identity of the server for secure streaming.

* HTTP/HTTPS

NOTE: App-V Management server does not accept Publishing Refresh requests over HTTP/HTTPS.

1. The publishing information in the XML file will contain the location of the ICO and OSD files. They will then be copied to the client for publishing shortcuts and file type associations via:
   * SMB/CIFS
   * HTTP/HTTPS

Use RTSPS or HTTPS to secure the communication for the first step of the publishing refresh. Selecting the communication method for the first step is done when adding a publishing server to the client. For the second step, use IPsec for a SMB/CIFS share and HTTPS for a web server. Selecting the communication method for the second step occurs when the application record is created in the database.

NOTE: If using IIS to publish the ICO and OSD files, a MIME types for OSD = TXT will have to be configured or IIS will refuse serving them to.

### Configuring App-V Management or Streaming Server for RTSPS

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, but the certificate “Issued To” field is set to “Fooserver1.mycompany.com,” the client will not connect to the server and the session will end, even if myserver.mycompany.com and Fooserver1.mycompany.com are the same server (they resolve to the same IP address).

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 the root CA** – The Certificate Authority (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 Server App-V Service access.** By default, the App-V Management and Streaming Server service run under the Network Service account. When a PKCS#10 is generated on the server, a private key is created. Only the Local System and Administrators groups have access to this key. These default ACLs will prevent the App-V server from accepting secure connections. The App-V Security Operations Guide has detailed steps on configuring the proper ACLs on the Private Key.

NOTE: Additional guidance on configuring Public Key Infrastructures is available at <http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx>.

NOTE: Administrators need to monitor the validity of the certificates to ensure that the certificates issued for App-V or other services do not expire.

### Configuring IIS with HTTPS to Support App-V Operations

App-V uses IIS servers in certain infrastructure configurations. Configuring IIS servers to support HTTPS is a well-known task. More information can be found at: <http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/596cdf5a-c852-4b79-b55a-708e5283ced5.mspx?mfr=true>

### App-V Client to Management Server for Package Streaming

When a user launches an application for the first time, or if auto loading parameters have been set on the client, the application package will be streamed (moved) from a server to the client cache. This process supports the RTSP/RTSPS, HTTP/HTTPS, and SMB/CIFS protocols. OSD files control which of the protocols are used, unless the Application Source Root or OverrideURL setting has been configured on the clients.

Therefore, as previously described in this document, configure communication to occur over RTSPS, HTTPS, and IPsec for SMB/CIFS in order to achieve higher levels of security. More information is available on choosing which communication method to use in the App-V Planning and Deployment Guide at <http://go.microsoft.com/fwlink/?LinkId=122063>.

NOTE: If using IIS to publish packages (SFT files), a MIME type for SFT=Binary will have to be configured or IIS will refuse to serve them to clients.

### Management Console to Management Service

The App-V Management Console allows administrators to make changes to the data store. However, it has to communicate through the Management Service. Therefore, configure the communication of the Management Console to the Management Service to utilize HTTPS as previously described in the [Configuring IIS with HTTPS to support App-V operations](#_Configuring_IIS_with).

## App-V Server Security

Earlier in the document it was stated that all of the defaults for the installation of the server were the highest levels of security. However, some of the components rely on underlying infrastructure components that are not configured as part of the installation. Following up with these post-installation steps will enhance the security of the App-V infrastructure.

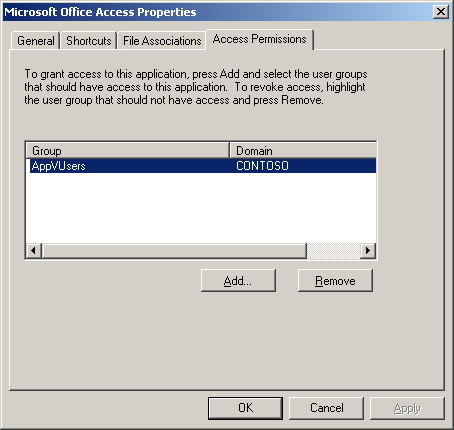
The content directory contains all of the packages that are to be streamed to clients. These resources need to be as secure as possible to eliminate any possible security threats.

* **UNC-based publishing and/or streaming:** The permissions for this location should be the most restrictive by the environment. Using NTFS permissions, implement the most restrictive ACLs for the content directory. (Users=Read, Administrators=Read and Write)
* **IIS is used for publishing and/or streaming**: Configure IIS to support only Windows Integrated authentication. Remove anonymous access to the IIS server and restrict access to the directory with NTFS permissions.
* **RTSP/RTSPS to stream application packages:** Configure the App-V Provider Policy to require authentication, enforce access permissions, and configure only required groups to have access to the provider policy. Configure applications with the appropriate permissions in the database.

The set of App-V administrators should be kept to a minimum to eliminate possible threats to the data in the data store and to avoid publishing malicious applications into the infrastructure.

## Application Level Security

Although permissions can be set on individual applications in a package, security is really at the package level. While the unassigned app will not be published to the user’s desktop, that user can still launch that application based on their access permissions to the package. A scenario is available where a user that has only been given access permissions to some of the applications in a package could launch the other applications in a package. This behavior could occur if the user has the add-application permission or is an administrator on the client. The user could create or use a shortcut on the client to launch an application that they do not have access to, if they have access to at least one application in the same package.



## 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 the highest 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 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

By default, the installation of the client registers FTAs for OSD files. This allows for users to launch applications directly from OSD files instead of the published shortcuts. A scenario concerning security could arise when the permissions on the client have been set to restrict the add application permission, but the user is an administrator. In this scenario the user could be sent an OSD in an email or visit a website that had a malicious OSD. If the user would open the OSD in this way they would be able to launch and add the application and bypass the add application permission. This is because local administrators will bypass the permissions set for the App-V client. Simply unregistering the FTAs for the OSD would prevent this. Also, if there is no reason for users to launch applications via OSD files directly it is recommend that this extension is blocked thru the email system or client and is blocked by the firewall. Documentation configuring these options is available at:

<http://support.microsoft.com/kb/837388>

### Authorization

During the installation of the App-V Client, an administrator can configure the system to require authorization for cached applications. This means that applications that have been streamed from the server require authorization from the App-V infrastructure before launching. However, if the App-V infrastructure is unavailable (App-V infrastructure down or client leaves the App-V infrastructure) then the application will use the last authorization of the package (this could be positive or negative). If the user has not launched the application successfully before the App-V infrastructure is unavailable, they will not be able to launch the application until they can communicate with the App-V infrastructure and receive authorization.

Setting the RequireAuthorizationIfCached registry setting (or deselecting the option during setup) to not require authorization means that authorization will be attempted if the infrastructure is available and the resulting authorization (positive or negative) will be enforced. If the App-V infrastructure is not available all applications that have been previously cached will launch, not just the ones that had been previously authorized successfully. Also, if the user has permission to change the client to Work Offline mode through permissions or if they are a local administrator, a user would be able to open all cached packages as if the App-V infrastructure was unavailable.

### ADM Template

App-V introduces an ADM Template that can be used to configure the most common client settings through Group Policies. This Template allows 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 related.

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 deploy clients in an organization successfully, a full description of the ADM Template and the specific settings are available in the ADM Template whitepaper at <http://go.microsoft.com/fwlink/?LinkId=127120>.

### 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.

### Virus Scanning the Client

Anti-virus software running on an App-V Client PC can detect and report an infected process running in the virtual environment; however, the antivirus software cannot disinfect files that reside within the virtual environment. If a virus is detected in the virtual environment, the antivirus software would perform the configured operation (quarantine or repair), but that operation would be completed in the per user storage locations and not affect the actual package. Virus scanning software should be configured with an exception for the sftfs.fsd file. This file is the cache file that stores packages on the App-V Client.

Note: If a virus is detected in a deployed application or package it should be removed from the production environment until a replacement package without a virus can be created.

### Roaming Profiles\Folder Redirection

App-V stores user specific changes to packages in the usrvol\_sftfs\_v1.pkg file within the Application Data of a user’s profile. Because the profile or a redirected Application Data folder is transferred between the client and the server, it is imperative that the communication between the client and the server is secured. The use of IPsec policies to secure the communication between endpoints is discussed in this document under [Data Store.](#_Data_Store)

## App-V Sequencing Security

The process of packaging applications for App-V or sequencing is typically the largest ongoing task in an App-V infrastructure. As an ongoing task, careful consideration should be given when creating policies and procedures to be followed when sequencing applications.

### 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.

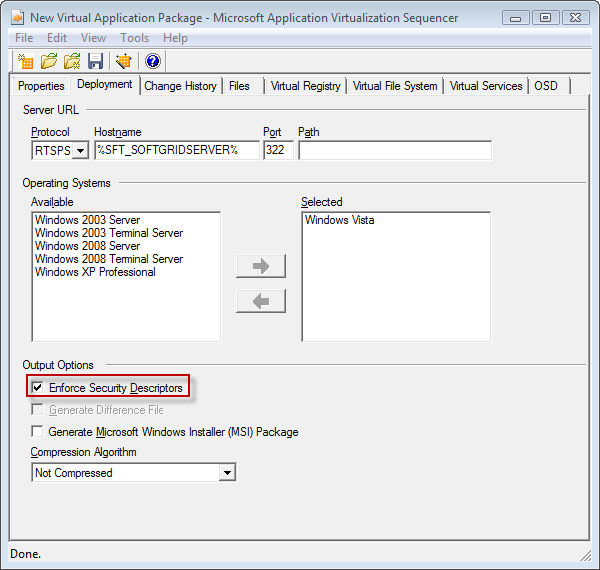
NOTE: If a virus is detected in the application it should not be deployed.

### 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 potentially 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 securing these locations would be a way of providing security for this data.

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, thus, won’t affect other users.

### Application Services

App-V provides support for application services that are part of a virtualized application. While sequencing, application services can be virtualized, however the security context that they will run as in the virtual environment is limited. The only security contexts supported in a virtual environment are Local System, Local Service, or Network Service. During sequencing, if a security context is specified for the application service other than the three supported, the Local System security context will be applied in the virtual environment. If the application service is configured to use either the Local Service or Network Service it will be honored in the virtual environment. Configuring the service account can be done during the sequencing process using these three security contexts.

### Persisted Security Information

When sequencing applications, the sequencing engineer will either install the application as a user would or develop an automated method for installing the application while being monitored. During this phase of sequencing, everything that isn’t being excluded from the package will be captured as part of that package. This is so the application will have the necessary assets to run virtualized. Some applications store sensitive security information (such as passwords) during the installation; if persisted unprotected, it could be accessed by other users with access to the package. During installation, if an application installation asks for a password or other security sensitive information, check with the documentation to ensure that it is either not persisted (removed after installation) or, if persisted, that it is protected (encrypted).

## Internet-Facing Scenarios

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 represent the best choices as they relate to security.

App-V Internet-Facing infrastructures are supported over secure connections that have been described previously in this document. In order to support either scenario, both RTSPS on the Management Server and HTTPS on an IIS server would be required. RTSPS will support both the publishing refresh for an internet-based client and could optionally support the streaming of the application packages. HTTPS will support the copying of ICO and OSD files to the client and optionally support the streaming of the application packages. The choice of RTSPS or HTTPS for streaming packages is dependent on the features that are required for the environment and the desired performance. RTSPS supports active upgrade which may be required for some environments, where HTTPS provides better performance for a larger client base. It is recommended to separate the Management Server from the IIS server to better support the security requirements of an organization.

NOTE: Using RTSP or HTTP for App-V Internet-Facing scenarios is not supported because of possible man in the middle attacks that would be present if the communications channels are not secured across the internet.

There are two recommend scenarios for setting up the App-V infrastructure for internet-based clients:

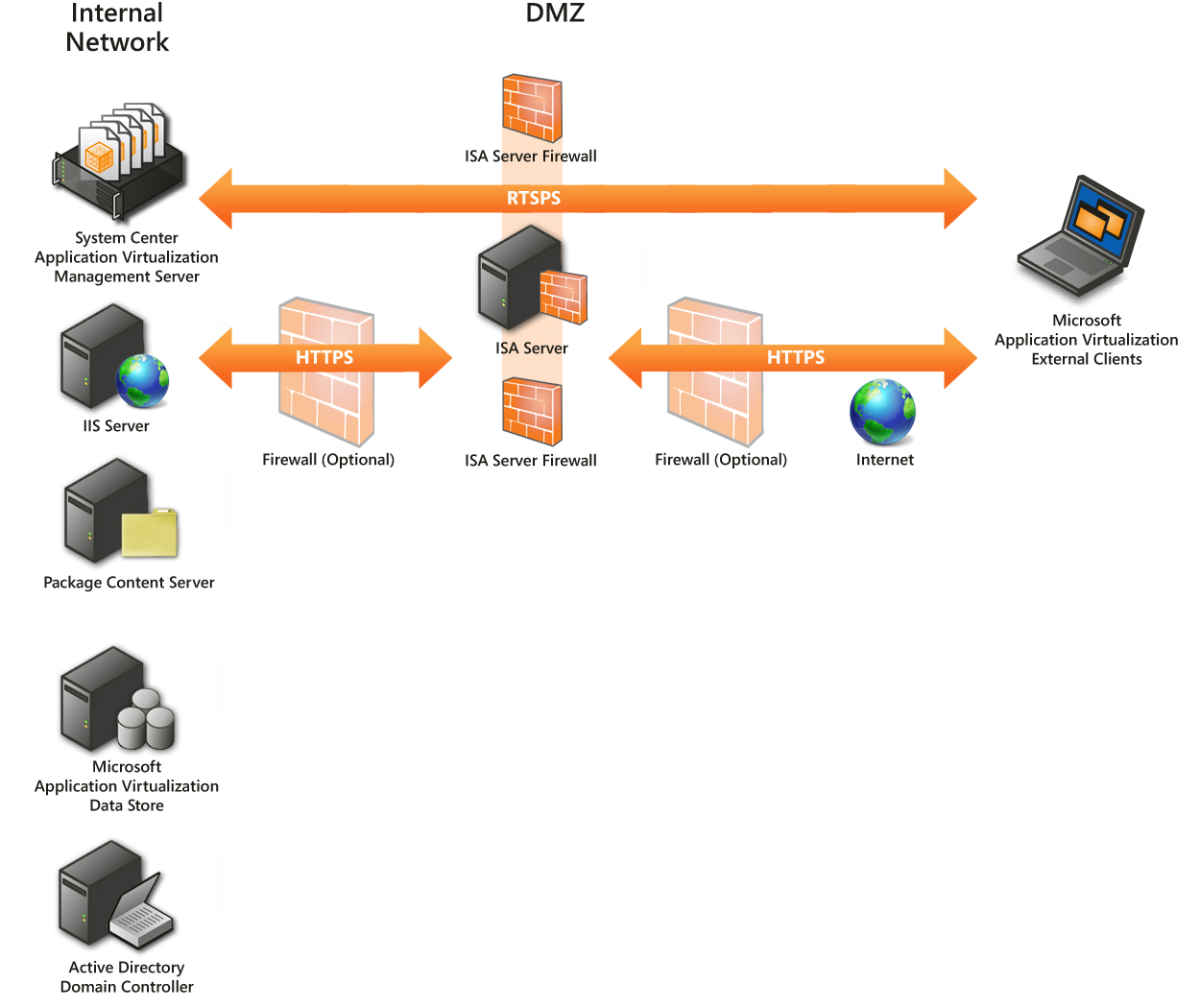
* App-V Servers behind ISA
* App-V Servers in a DMZ

### App-V Servers Behind ISA

This scenario provides the best security solution for supporting internet-facing servers. The use of ISA’s reverse proxy and server publishing capabilities enables administrators to maintain their entire App-V Server Infrastructure inside the corporate network. This enables all users, both internal and internet-based, to access the same App-V Servers. This will reduce the administrative overhead for maintaining the infrastructure. The reverse proxy and server publishing capabilities of ISA allow for the traffic from the internet to be received by the ISA server, and the ISA server will complete the requests inside the corporate infrastructure.

In this scenario the ISA server is required to be able to receive both RTSPS and HTTPS traffic from the internet and make RTSPS and HTTPS requests to the internal network. If additional firewall appliances are utilized in front of or behind the ISA server, the appropriate protocols and addresses will need to be given access.

Figure 3: App-V Servers behind ISA



### App-V Servers in DMZ

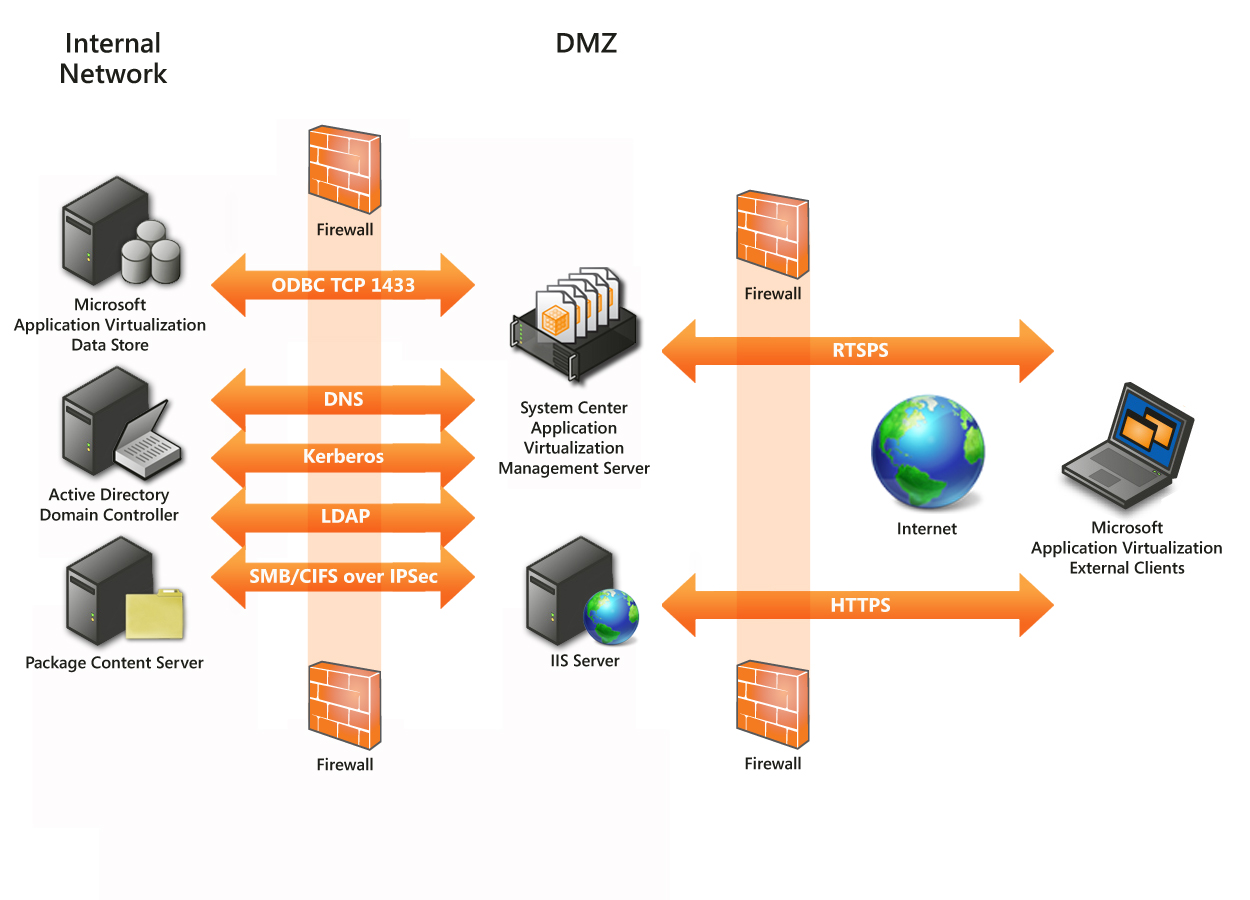
The other scenario places the App-V Management Servers in the DMZ. To support the Management Servers and IIS Servers, the publishing and streaming protocols RTSPS and HTTPS will need to be allowed from the internet to the DMZ. Also, infrastructure-related traffic to support the Management Servers and IIS Servers will need to be allowed from the DMZ to the internal network. This scenario presents additional administrative overhead to ensure that the traffic from the DMZ to the internal network is properly configured.

Another challenge to this environment is if the Management and IIS Servers are in the DMZ and organization would need to allow internal client computers to access the DMZ or have additional App-V Infrastructure Servers in the internal network. This would increase the management overhead for the App-V solution. However, in environments without an ISA server this may be the best solution.

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

* SQL
* SMB/CIFS if the content directory is located internal network
* Kerberos
* DNS
* LDAP

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



## Client Internet Facing Considerations

**Domain Joined Client**

Users on the internal network have access to all of the components of an App-V infrastructure. If a user leaves the internal network, some of the services will not be available. By default, App-V Clients use Kerberos tickets that were issued by the Active Directory for authentication and authorization. Most infrastructures will not place their Domain Controllers on the internet to allow internet users to perform this operation. The client will use the ticket issued to it by Active Directory as long as it is valid for authentication and authorization (default is 10 hours). If the user is away from Active Directory long enough that the ticket would expire, and the user would not be able to renew their ticket, the App-V Client will revert to NTLM authentication utilizing their cached credentials.

**Non-Domain Joined Client**

App-V Clients do not have to be managed by an Active Directory in order to function. This opens opportunities for organizations to utilize App-V to supply partner organizations with virtualized applications, provide virtualized applications as part of a managed service, or to simply support non-domain managed machines. If a user is a home-based worker and their machine is not joined to the company domain, App-V can support delivering applications to them. In order to authenticate and authorize a user to perform the publishing refresh and stream applications, you will need to take an additional step to “store” the username and password for that user on the machine that has access to the App-V environment and has been given appropriate permissions to applications.

# Conclusion

This document provides concepts and guidance to design a more secure App-V infrastructure. Additional implementation details can be found in the App-V Security Operations Guide.