

**Citrixxperience.com**

**1Y0-259 Citrix Presentation Server 4.5:  
Administration**

**Study Guide**

**Version 1.0**

(September 4, 2008)

## **Citrix® Presentation Server 4.5: Administration Study Guide**

---

This study guide was created by Citrixexperience.com. Used for creation of this study guide was the Citrix® courseware CTX-1259AI Citrix® Presentation Server 4.5: Administration, 1Y0-259 Exam Enablement Guide, Presentation Server 4.5 Administrator's Guide, Web Interface Administrator's Guide, Getting Started with Citrix Licensing, Clients for Windows Administrator's Guide, Load Manager Administrator's Guide, and various articles from the Citrix® Knowledge Center, which are all copyrights of Citrix® Systems.

Along with the documents listed above, this study guide is meant to be used in preparation for the 1Y0-259 Citrix® Presentation Server 4.5: Administration exam. Also suggested for preparation are other books that relate to the subjects and above all, personal experience with the products. Citrixexperience.com recommends further preparation by using other 1Y0-259 products found at [www.Citrixexperience.com](http://www.Citrixexperience.com).

The license for this study guide is for one user only. It is a copyright of Citrixexperience.com and may not be reprinted, copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including but not limited to electronic, mechanical, photocopying, recording, or other means, in full or in part, without the prior express written permission of Citrixexperience.com.

Citrix, the Citrix logo, Citrix ICA, Citrix MetaFrame, Citrix MetaFrame XP, Citrix Nfuse, Citrix Extranet, Citrix Program Neighborhood, Citrix WinFrame, and other Citrix product names referenced herein are registered trademarks or trademarks of Citrix Systems, Inc. in the United States and other jurisdictions. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.

Citrix® Systems, Inc. is not affiliated with Citrixexperience.com in any way.

## Table of Contents

---

<b><u>Subject</u></b>	<b><u>Page</u></b>
Installing and Managing Citrix Presentation Server	1
Configuring Farm Settings	3
Configuring ICA Sessions	10
Configuring Policies	14
Publishing Applications and Content	20
Deploying Applications	25
Creating and Assigning Load Evaluators	28
Configuring Printing	31
Enabling Web Access to Published Applications and Content	36
Securing Access to Published Applications and Content	41

## 1Y0-259 Citrix XenApp: Administration Study Guide

### Installing and Managing Citrix Presentation Server

---

#### Install Presentation Server 4.5 License

- Open the **License Management Console**.
- Click **Configure License Server > Step 1: Download license file from MyCitrix.com**.
- Login to **My Citrix** and from the **Current Tool** drop-down list select **Activate/Allocate**.
- Download the license file.
- Copy the license file to your license server with the **License Server Management Console**.
- Make sure the directory appears in the **Upload license** page, or browse to it and click **Upload**.
- On the **License Files** page, click **Update license data**.
- The file will appear in the table on the page.

#### Installing Program Neighborhood Agent

When using the Program Neighborhood Agent, if you want the users to be prompted for authentication to a Citrix Presentation Server every time, select **No** when configuring pass-through authentication during Program Neighborhood Agent installation.

When configuring Program Neighborhood Agent:

- Type the name of the server hosting the Program Neighborhood Agent Services site.
  - In the format of `http://servername` or `https://servername` and then click **Next**.
    - ◆ Replace `servername` with the name of the Web Interface server.

#### Update Presentation Server

To update a Presentation Server 3.0 or 4.0 server farm running on Windows 2003 you can take advantage of the automatic upgrade path.

- On the initial **Autorun** screen of **Setup**, select **Install Citrix Presentation Server 4.5 and its components**.

- Setup detects the existing Presentation Server installation and automatically displays the appropriate options for upgrading your farm.
- Just keep the default settings.

### **Databases**

Microsoft SQL Server, Oracle and IBM DB2:

- Support replication.
- Are suitable for large farms.

Microsoft Access and SQL Server 2005 Express Edition SP1:

- Do not support replication.
- Are suitable for all small and many medium-sized environments that are located in one physical location.
- They require much less administration than Microsoft SQL Server, Oracle and IBM DB2.

### **Start-up License**

Presentation Server comes with a start-up license that allows for up to 2 user connections to Presentation Server prior to the installation of a valid license.

After 96-hours, the start-up license grace period expires and user sessions will not be able to connect to servers running Presentation Server.

- However, an administrator can continue to configure Presentation Server after the start-up license grace period expires.

### **Citrix XML Service**

The Citrix XML Service shares port 80 with IIS, by default.

### **Farm and Zone Architecture**

In general, a single server farm meets the needs of most environments.

Sometimes business reasons dictate the need for multiple server farms.

Single zones work best when all Presentation Servers are located in the same geographical location while multiple zones work best when Presentation Servers are separated geographically.

### **Configuring Shadowing During Installation**

Shadowing restrictions set during the installation of Presentation Server are permanent.

If shadowing was disabled or capabilities restricted during the installation, neither shadowing nor the restricted capabilities can be enabled after the installation is complete without reinstalling Presentation Server.

### **IMA Encryption**

Presentation Server can be configured to encrypt the IMA communications used to send information to the data store and configuration logging databases.

- This encryption can add a layer of security to the sensitive data stored in the databases.

### **Users and Groups Considerations at Installation**

During the installation of Presentation Server, the existing users and groups and the anonymous user accounts created by Presentation Server can be added to the local **Remote Desktop Users** group on the server.

Only users and groups that are members of the local **Remote Desktop Users** group can access resources on the server using the ICA or RDP protocol.

If the users and groups do not exist at the time of the installation or the administrator wants to manually add the users and groups, the administrator can use the **Computer Management** utility on the server to perform this task after the installation completes.

## **Configuring Farm Settings**

---

### **Health Monitoring and Recovery**

Citrix provides a standard set of Health Monitoring and Recovery tests.

- **Citrix IMA Service test**
- **Citrix XML Service test**

- **Logon monitor test**
- **Terminal Services test**

You can also develop your own tests using the Health Monitoring and Recovery SDK.

If a Health Monitoring and Recovery test identifies an issue with a server, one of the following actions can be taken:

- **Alert Only**
- **Remove Server from Load Balancing**
- **Shutdown IMA**
- **Restart IMA**
- **Reboot Server**

In the case that the administrator wishes to keep connections to the server but not allow new connections, the administrator would choose **Remove Server from Load Balancing**.

- This can be configured in the properties of the server or the server farm.

**Alert Only** allows new connections, while **Shutdown IMA**, **Restart IMA** and **Reboot Server** disconnect all of the existing sessions.

### **CPU Utilization Management**

When you enable **CPU utilization management** the server allocates an equal share of the CPU to each user.

- This prevents one user from impacting the productivity of other users and allows more users to connect to a server.

When CPU utilization management is being used:

- Approximately 20 percent of the CPU resource is reserved and not available for the users.
  - This leaves 80 percent available to share among the users.
    - ◆ For example, if 20 users are connected, they will each get 4 percent of the CPU resources.

### **Election Preference**

To configure a server as the data collector, the administrator should set the server's election preference to **Most Preferred**.

To configure a server to never become the data collector, the administrator should set the server's election preference to **Not Preferred**.

Other election preferences are: **Preferred**, which is the backup data collector, and **Default Preference**, which allows the server to be the data collector if the most preferred data collector and backup data collector are not available.

After configuring the election preference, restart the IMA Service or reboot the server.

### **Configuration Logging**

The *configuration logging* feature allows you to keep track of administrative changes made to your server farm and generates reports that show what changes were made, when they were made and who made them.

A high-level explanation of configuring configuration logging:

- Create the configuration logging database.
- Verify the configuration logging database is specified in the **Database type** field.
- Configure the configuration settings for the server farm.

When needed, the administrator can clear the data stored in the configuration logging database.

To set up logging of administrative tasks:

- Open the **Access Management Console**.
- Right-click the server farm node and click **Properties**.
- Expand the **Farm-wide** node and click **Configuration Logging**.
- Verify that a configuration logging database is specified in the **Database type** field.
- Select **Log administrative tasks to the logging database**.
- Click **OK**.

### **Virtual IP Addressing**

Some applications need a unique IP address for each application for licensing, addressing, identification or other purposes.

With *virtual IP addressing*, you can assign a static range of IP addresses to a server or servers and have these addresses individually allocated to each session so that configured applications running within that session appear to have a unique IP address.

To configure virtual IP addressing:

- Open the **Access Management Console** select a farm.
- Select **Action > Modify farm properties > Modify virtual IP properties**.
- Open **Address Configuration** from the **Virtual IP** page in the farm's **Properties** list.
- Use the **Address Configuration** dialog box to configure the virtual IP address ranges and assign them to servers.
- Click **OK** to restart the affected servers.

The number of virtual IP addresses specified for a server should be equal to or exceed the maximum number of concurrent sessions to the server.

If a virtual IP address is not available at connection time, an "Insufficient virtual IP addresses are not available" error message is displayed on the client. The session may open, but applications that require an IP address may not work correctly.

### **Citrix Ports**

- Port 2512 is used for server to server communication using the IMA Service.
- The Access Management Console uses port 135.
- Citrix SSL Relay uses port 443.
- ICA sessions use port 1494.
- Client to server UDP sessions use port 1604.
- The IMA Service uses port 2513 for communication between the Presentation Server Console and Presentation Servers.
- Session reliability uses port 2598.
- The License Management Console uses port 8082.
- Server to license server communication takes place over port 27000.

### **Virtual Loopback**

*Virtual loopback* provides published applications with loopback addresses to use in sessions.

When enabled, the virtual loopback function does not require any additional configuration other than specifying which processes use the feature.

When an application uses the localhost address (127.0.0.1) in a Winsock call, the virtual loopback feature simply replaces 127.0.0.1 with 127.X.X.X where X.X.X is a representation of the session ID + 1.

- For example, a session ID of 7 is 127.0.0.8.

### **Session Reliability**

*Session reliability* keeps sessions active on the user's screen when network connectivity is interrupted.

Users continue to see the application they are using until network connectivity resumes, but the display freezes and the cursor changes to a spinning hourglass.

The advantage is that when network connectivity resumes, they don't have to reconnect to the application.

To enable session reliability, choose **Allow users to view sessions during broken connection** in the session reliability settings.

### **Auto Client Reconnect**

*Auto client reconnect* allows Clients for Windows, Java and Windows CE to detect broken connections and automatically reconnect users to disconnected sessions.

When a client detects an involuntary disconnection of a session, it attempts to reconnect the user to the session until there is a successful reconnection or the user cancels the reconnection attempts.

When configuring session reliability:

- An administrator can enable it by selecting **Allow users to view sessions during a broken connection**.
- Disable it by deselecting **Allow users to view sessions during a broken connection**.
- Change the port number in the **Port number** field.

- Change the amount of time sessions remain active when connectivity is lost in the **Seconds to keep sessions active** field.

If an administrator wants users to re-authenticate before reconnecting to active sessions, auto client reconnect should be enabled.

When session reliability is enabled, Keep-Alive settings are not used even when they are configured in the server farm.

### **Virtual Memory Management**

*Virtual memory management* monitors and regulates the .DLL and virtual memory utilization so memory is used more efficiently.

Schedule virtual memory optimization at a time when your servers have their lightest loads.

### **Rebalancer Service**

The *Rebalancer Service* is responsible for enhancing resource management on servers with multiple CPUs.

The service is set to start manually by default.

If an environment is running many short-lived applications and the applications appear to be running on the same CPU, the administrator should set the service to start automatically.

If this service is not started on servers with multiple CPUs, the benefits of CPU utilization management are lost.

### **Citrix Administrator Accounts**

When creating a new Citrix administrator account you can choose **View Only**, **Full Administration**, or **Custom** permissions.

- Administrators with **View Only** privileges can view all areas of server farm management but cannot modify them.
- Administrators with **Full Administration** privileges can view and modify all areas of server farm management.
  - Only administrators with **Full Administration** can create other administrators and create or delete server and application folders.
- By default, administrators with custom accounts are created with the **Log on to Management Console** permission. Use the **Permissions** screen to allow custom administrators to perform additional tasks.

The most trusted web site for Citrix certification preparation, Citrixexperience.com

To modify permissions for a Citrix administrator account:

- Open the **Access Management Console**.
- Click the server farm node.
- Double click **Administrators** in the drop-down list details pane.
- Right-click the administrator account or group in the details pane and click **Modify administrator properties**.
- Click **Permissions** in the left pane of the **Properties** screen.
- Click a folder and then select the permissions in the right pane that the selected administrator or group will have for that folder.
- Repeat the last step until all the appropriate permissions are set.
- Click **OK**.

### **ICA Connections**

When a user starts a published application, an ICA connection is made to a Presentation Server.

If the user starts a published application on a different server, another ICA connection is made.

If a user starts a published application on a server that the user already has an ICA connection to, the same ICA connection will be used; a new ICA connection will not be started.

To configure ICA connections:

- Open the **Access Management Console**.
- Right-click the server farm node and click **Properties**.
- Expand the **Farm-wide** node and click **Connection Limits**.
- Configure the number of ICA connections allowed per user.
- Configure the number of ICA connections allowed per administrator.
- Configure ICA connection limit logging.
- Click **OK**.

### ICA Keep-Alive

*ICA Keep-Alive* is a setting used to manage the states of the ICA sessions to ensure that they are accurately reported.

When ICA Keep-Alive is configured, packets are sent to each client device to determine whether a connection still exists.

If the client device does not respond, the state of the session using the connection is changed from active to disconnected.

## Configuring ICA Sessions

---

### SpeedScreen

*SpeedScreen Latency Reduction Manager* provides mouse click feedback and local text echo to reduce the user's perception of latency when typing and clicking.

*SpeedScreen Browser Acceleration* optimizes the responsiveness of graphics-rich HTML pages in published versions of Microsoft Outlook, Outlook Express and Internet Explorer.

- SpeedScreen Browser Acceleration must be enabled at either the farm lever (default) or the server level and 'Determine when to compress' must be selected.
  - (Author's note: The selection may also be 'Adjust compression level based on available bandwidth').
- To further accelerate the accessibility of Web pages and email using SpeedScreen Browser Acceleration, JPEG compression can be enabled.
  - JPEG compression offers a trade-off between the quality of the JPEG images as they appear on the client devices and the amount of bandwidth the files consume transferring from server to client.
  - JPEG image acceleration results in slightly lower image resolution and slightly higher resource consumption on both server and client.
  - When JPEG image acceleration is enabled, select the **Image compression level** based on available bandwidth: **Low**, **Medium** or **High**.

*SpeedScreen Multimedia Acceleration* allows you to control and optimize the way Citrix Presentation Server passes streaming audio and video to users.

*SpeedScreen Flash Acceleration* allows you to control and optimize the way Citrix Presentation Server passes Macromedia Flash animations to users.

*SpeedScreen Image Acceleration* offers you a trade-off between the quality of photographic image files as they appear on client devices and the amount of bandwidth the files consume on their way from the server to the client.

*SpeedScreen Progressive Display* allows you to improve interactivity when displaying high-detail images by temporarily increasing the level of compression (decreasing the quality) of such an image when it is first transmitted over a limited bandwidth connection, to provide a fast (but low quality) initial display.

- If the image is not immediately changed or overwritten by the application, it is then improved in the background to produce the normal quality image, as defined by the normal lossy compression level.
- *Heavyweight compression* allows you to increase the compression of the SpeedScreen Image Acceleration and SpeedScreen Progressive Display without impacting image quality.
- Because heavyweight compression is CPU intensive and affects server scalability, it is recommended for use only with low bandwidth connections.

### **Program Neighborhood Agent**

The *Program Neighborhood Agent* allows your users to access all of their published resources in a familiar Windows desktop environment.

- Users work with your published resources the same way they work with local applications and files.
- Published resources are represented throughout the client desktop, including the Start Menu and Windows notification area, by icons that behave just like local icons.

Program Neighborhood Agent is configured at a site created in the Access Management Console and associated with the site for the Web Interface server.

When configuring Program Neighborhood Agent, the URL of the appropriate Web Interface server must be entered in the format `http://servername` or `https://servername`.

Program Neighborhood Agent connects to the server at startup to get the latest configuration information including available published resources and permissions to change local settings.

### **Web Client**

The *Web Client* is a smaller client that can be installed from a .CAB file or from the main .MSI file.

The Web Client setup files are significantly smaller than the other clients.

The most trusted web site for Citrix certification preparation, Citrixexperience.com

- The small size allows users to quickly download and install the client software.

The Web Client does not require user configuration and does not have a user interface.

Users access the published resources by clicking on links from a Web page or corporate intranet.

The following browsers will work with the Client for Web:

- Internet Explorer 5.0 through 7.0
- Netscape Navigator 4.78, and 6.2 through 7.1
- Mozilla Firefox 1.0 through 1.5

To use the built-in Web Interface client installation feature, you must make sure the web server's **\Clients** folder contains the appropriate client files.

### **Program Neighborhood**

*Program Neighborhood* supports the full Citrix Presentation Server feature set and it requires user configuration and maintenance.

Choose Program Neighborhood for the Presentation Server Client if you do not want to publish your resources using Web Interface.

If you choose to implement the Web Interface at a later time, Program Neighborhood users can also access resources published through Web Interface.

### **Client Deployment**

Before deploying a client package via Active Directory to any clients before Windows XP, Windows Installer 2.0 must be installed on the clients.

Administrators can use Active Directory to deploy clients using the .MSI file on the Components CD for Presentation Server or using a custom client file package created with Client Packager.

To assign a client package to an Organizational Unit (OU):

- Create a network share and copy the .MSI file containing the client to the network share location.
- In **Active Directory Users and Computers** right-click the appropriate OU and click **Properties**.
- Click the **Group Policy** tab and click **New** to create a new **Group Policy**.

The most trusted web site for Citrix certification preparation, Citrixexperience.com

- Type the name for the Group Policy and press **Enter**.
- Click **Edit** and navigate to **Computer Configuration > Software Settings > Software Installation**.
- Right-click the blank area in the right pane and click **New > Package**.
- Locate the client package on the network share and click **Open**.
- Click **Assigned** in the **Deploy Software** dialog and click **OK**.
- As the client restarts, Active Directory Group Policy automatically installs the client on the computer.
- After deploying a client package via Active Directory and restarting the client device, the administrator should log in to the client device to verify that the client is installed.

### Client Packager

When creating a package with the Client Packager, the default client name option is **Use machine name as client name**.

- By default, Citrix clients get the same name as the machine at deployment.
- The other client name option is **Let users specify a client name**.

By choosing **No** on the pass-through authentication screen, the administrator would make sure that the users must enter their username and password to log on to sessions.

**Enable Quick Launch Bar** and **Enable Custom ICA Connections** are both configuration choices for Program Neighborhood.

While creating a Program Neighborhood package:

- To help ensure duplicate client names do not exist on the network, allow the user to name the client by choosing **Let user specify a client name**.
- To let users open sessions without entering their username and password, choose **Use Kerberos only** to enable pass-through authentication.
- To allow users to make server connections without using the ICA Connection Wizard, choose **Enable Quick Launch Bar**.
- To ensure older client versions are overwritten with newer clients, leave **Allow upgrade if package is newer than existing client version** chosen; that is the default client replacement option.

## Configuring Policies

---

### Limit Concurrent Sessions

To allow users to have more sessions running than the server farm is configured to allow:

- Create a new policy in the **Presentation Server Console**.
- Add the policy rule **Limit total concurrent sessions**.
- Configure the sessions to as many as needed and apply the policy to the desired users or groups.

### Policy Filters

After a policy has been created and configured, and administrator can filter the policy using:

- **Client names**
- **Access control (connections made through Access Gateway)**
- **Users and user groups**
- **Servers**
- **Client IP addresses**

To filter a policy to affect only a certain range of IP addresses:

- Click the **Policy** node in the **Presentation Server Console**, right-click the appropriate policy in the right pane and select **Apply this policy to**.
- Click **Client IP Address**.
- Click **Filter based on client IP address**.
- Click **Add**.
- Click **IP Range** and click **OK**.
- Click **Allow** and click **OK**.

### Shadowing

To create a new shadowing policy where the users are notified that they are being shadowed and the user doing the shadowing cannot control the keyboard or mouse:

The most trusted web site for Citrix certification preparation, Citrixexperience.com

- Create a new policy in the **Presentation Server Console**.
- In the policy's properties open the **Shadowing** folder under the **User Workspace** folder in the left pane.
- Select the **Configuration** rule and enable it.
- Select **Allow shadowing**.
- Select **Prohibit being shadowed without notification**.
- Select **Prohibit remote input when being shadowed**.
- Select the rule named **Permissions** in the left pane and enable it.
- Click **Configure** to select the users who will do the shadowing.
- Click OK when done adding the users.
- Click OK at the bottom of the policy's properties.
- Apply the policy to the users who will be shadowed.

### **Zone Preference and Failover**

A Zone Preference and Failover policy is configured in the **User Workspace** folder in the properties of a policy.

The primary and backup zones are configured and which zone users connect to is identified.

Client for Web and Program Neighborhood Agent support Zone Preference and Failover.

In a Zone Preference and Failover policy, connections can be directed to a preferred zone and failover to a backup zone.

### **Print Job Routing Policy**

Print job routing has two settings:

- **Connect directly to network print server if possible**
- **Always connect indirectly as a client printer**

If the concern is bandwidth usage over a WAN connection, **Always connect indirectly as a client printer** should be used.

### **Sound Quality and Bandwidth**

To cut down on the bandwidth used for audio in an audio-enabled application:

- Create a Presentation Server policy.
- Enable the **Sound Quality** rule in the **Client Devices > Resources > Audio** folder.
- Limit the audio bandwidth per session to desired level.
- Apply the policy to the users that are experiencing the application degradation.

### **Audio Rules**

The audio rules available in the **Client Devices > Resources > Audio** folder for Presentation Server policies are:

- **Microphones**
  - Allows microphones on client devices to be used in a session.
- **Sound Quality**
  - Configures the maximum allowable client audio quality per session.
- **Turn off speakers**
  - Disables audio mapping to client speakers.

### **Bandwidth**

If an administrator is concerned about bandwidth and needs to create a policy to help contend with bandwidth issues, there are many policy rules that can be configured.

In the **Bandwidth** folder of a Presentation Server policy, the administrator can configure:

- **Visual effects**, including:
  - **Turn off desktop wallpaper**
  - **Turn off animations**
  - **Turn off windows content while dragging**

- **SpeedScreen**
  - **Image Acceleration using lossy compression**
- **Session Limits**, including:
  - **Audio**
  - **Clipboard**
  - **COM Ports**
  - **LPT Ports**
  - **Drives**
  - **OEM Virtual Channels**
  - **Overall Session**
  - **Printing**
  - **TWAIN Redirection**

### **PDA Synchronization**

To configure PDA synchronization using USB-tethering:

- Enable the policy rule **Turn on automatic virtual COM port mapping**.
  - This rule allows USB to virtual COM port emulation in client sessions.
  - This rule is found in a policy at **Client Devices > Resources > PDA Devices**.

### **User Workspace Folder in Policies**

In the User Workspace folder of a Presentation Server policy, an administrator can configure:

- **Connections**, including:
- **Limit total concurrent sessions**
- **Zone preference and failover**

- **Server to client content redirection**
- **Shadowing**
  - configuration and permissions
- **Time Zones**
  - **Do not estimate local time for legacy clients**
  - **Do not use Client's local time**
- **Citrix Password Manager**
  - **Central Credential Store**
  - **Do not use Citrix Password Manager**
- **Streamed Application**
  - **Configure delivery protocol**
- Specifies the application delivery method used to stream applications to the desktops of client devices or servers.

### **Application Delivery Method**

When configuring an application delivery method policy, the administrator can configure:

- **Force server access**
  - Forces streamed applications to always launch from the server.
- **Force streamed delivery**
  - Forces the applications to always stream to the desktops of the client devices.

### **SecureICA**

An administrator can configure the required SecureICA encryption level per session in **Security > Encryption > SecureICA encryption**. This is the only policy rule available in a Presentation Server policy.

### **Apply Policy to Users and Groups**

To apply a Presentation Server policy to a user or group:

- In the **Presentation Server Console**, click the **Policy** node in the left pane.
- Right-click the appropriate policy in the right pane and click **Apply this policy to**.
- Click **Users**.
- Click **Filter based on users**.
- Configure the users and groups filter option in one of four ways:
  - **Apply the policy to all explicit users (non-anonymous)**
  - **Apply the policy to all anonymous users**
  - **Apply the policy to a specific user account or user group**
  - **Avoid applying the policy to a specific user account or user group**
- Click **OK**.

### **Policy Priority**

Each policy receives a number upon creation. By default, a new policy has the lowest priority of all policies. The number assigned is based on the number of policies that exist in a server farm.

To prioritize a policy, in the Presentation Server Console:

- Click the **Policies** node.
- Right-click the policy in the right pane and click **Priority**.
  - If you want to assign the policy the highest priority, click **Make Highest Priority**.
  - If you want to assign the policy the lowest priority, click **Make Lowest Priority**.
  - If you want to increase the priority of the policy one level, click **Increase Priority**.
  - If you want to decrease the priority one level, click **Decrease Priority**.

### **Policy Search Engine**

The *policy search engine* is a feature of the Presentation Server Console that allows an administrator to find all policies that can potentially apply to a specific connection and confirm how final policy rules are merged for that connection, thus making sure it is applied correctly.

To use the policy search engine:

- Right-click on the **Policy** node in the **Presentation Server Console** and click **Search**.
- Configure the search criteria (IP Address, Client Name, User, Server, Access Control) and click Search.
- Click **Yes** to search the entire Active Directory if desired.
- Optionally, double-click a policy in the search results to view the policy priorities.
- Click **View Resultant Policy** and the **Resultant Policy Properties** screen launches.
- Expand each node to view individual resultant policy rules.
- Click **OK** to close the **Resultant Policy Properties** screen.
- Click **OK** to close the **Search** screen.

## **Publishing Applications and Content**

---

### **Published Applications**

When published, users can access applications installed on the Presentation Servers.

The applications appear to run locally on the client devices.

Published applications provide the administrators control over what resources users can access on a server, unlike published server desktops.

Published applications provide administrators control over what resources users can access on a server.

### **Published Server Desktops**

Published server desktops allow users unlimited access to the resources on a server which can result in users changing configurations and settings that can cause server vulnerabilities.

### **Published Content**

The most trusted web site for Citrix certification preparation, Citrixexperience.com

Users can open published content using client-to-server or server-to-client content redirection.

When content is published, it provides users access to data files, such as:

- Documents
- Spreadsheets
- Media files and other data that are accessible by users using an HTML web site
  - Such as <http://www.citrixexperience.com>
- A file on a web site
  - Such as <http://www.citrixexperience.com/study/archive/exams/218.doc>
- A directory on an FTP server
  - Such as <ftp://ftp.citrix.com/edu>
- A file on an FTP server
  - Such as <ftp://ftp.citrix.com/edu/readme.txt>
- A UNC file path
  - Such as `\\servername\sharename\filename`
- A UNC directory path
  - Such as `\\servername\sharename`

### **Organize Published Resources**

An administrator can organize published resources in an application set by placing the published resources in folders during the resource publishing process or afterwards.

By default, all resources are published to the root folder of the application set.

An administrator can organize the published resources into folders to help users quickly locate the applications they need.

- For example, if many Microsoft Office applications are published, an administrator might decide to place the Microsoft Office applications into a folder called Microsoft Office making it easier for users to locate these applications.

### **Client-to-Server Content Redirection**

*Client-to-server content redirection* allows users of the Program Neighborhood Agent to use a published application to access files residing on the local client device.

Client-to-server content redirection through file type association requires Program Neighborhood Agent on the client devices.

Client drive mapping must be enabled so that the local content can be accessed by the application on the server.

- If drive mapping is not enabled, the published application opens and displays an error because the application is unable to access the local content that initially triggered the application to start.

### **File Type Association**

If you install and publish an application after installing Presentation Server, you must update the file type association in the server's Windows registry.

To update file type associations:

- In the **Access Management Console**, select the server where the application is published.
- Select **Action > All Tasks > Update file types from registry**.

### **Server-to-Client Content Redirection**

Users might frequently access web and multimedia URLs they encounter when running an email program published on a server.

If you do not enable *server-to-client content redirection*, users open these URLs with web browsers or multimedia players on the Presentation Servers.

To free servers from processing these types of requests, you can redirect application launching for supported URLs from the server to the local client device.

The following URL types are redirected:

- HTTP
- HTTPS
- RTSP (Real Player and QuickTime)

- RTSPU (Real Player and QuickTime)
- PNM (Legacy Real Player)
- MMS (Microsoft's Media Format)

### **Application Isolation Environment**

An application isolation environment has the following properties:

- **Applications**
- Specifies which applications are associated with or installed in this particular isolation environment.
- **Roots**
- Specifies the directories and registry locations in which files modified by users (user profile root) and applications (installation root) reside.
- **Rules**
- Specifies policies that specify how an isolated application accesses system resources, such as files, registry and named objects.
- **Security**
- Specifies the security policy to apply to the isolation environment, which can either be enhanced or relaxed.

An application isolation environment can contain associated, installed or published applications.

- *Associated applications* are installed directly on to the operating system of one or more Presentation Servers and are configured to launch within the confines of the isolation environment and can be accessed from outside of the environment.
- *Installed applications* are installed into an isolation environment using the AIESETUP command and must be published on a Presentation Server before they can be made available to users.
- *Published applications* have been installed into the isolation environment using AIESETUP and are published for one or more user.

Deleting an isolation environment has no effect on an application; however, user-specific files created within the isolation environment are deleted.

In an application isolation environment, the user profile root (where files created or saved by the current user are located) is: **%APPDATA%\Citrix\AIE\AIE\_name**

- Where **%APPDATA%** is a Windows environment variable and is replaced by the application data folder for the current user.
  - Typically **C:\Documents and Settings\%USERNAME%\Application Data**.
- **AIE\_name** is replaced by the name of the application isolation environment.

*Installation root* specifies the per isolation environment location of directory or registry key hierarchy for applications installed into an isolation environment.

Installation root is unique for each isolation environment.

When an application is installed in an isolation environment, the installation root is located at **C:\Program Files\Citrix\AIE\AIE\_name**.

- **AIE\_name** is the name of the application isolation environment.

The path to the actual file is added on to the installation root so each application has its own virtual copy of the files so they don't conflict with each other.

The APPUTIL command line utility can be used to install packaged applications into an isolation environment.

Applications can be associated with isolation environments during the application publishing process using the Publish Application Wizard.

They can be associated after the application has been published in the Presentation Server Console.

AIESETUP is used to install applications into isolation environments.

After an application is installed in an isolation environment (using AIESETUP) it can only be removed from the isolation environment by uninstalling the application.

### **Configure Published Resources**

Published resources can be configured to control the following options for the client device:

- **Legacy audio**
  - Allows support for applications to which SpeedScreen Multimedia Acceleration does not apply.
- **SSL and TLS protocols**

The most trusted web site for Citrix certification preparation, Citrixexperience.com

- Requests the use of the SSL and TLS protocols for clients connecting to the published resource.
- **Encryption**
  - Controls which clients are allowed to connect based on their encryption level.
- **Client printers**
  - Allows the published resource to open without waiting for the client printers to be created.

## **Deploying Applications**

---

### **Installation Manager Components**

The following components are required for Installation Manager to function:

- **Packager**
  - Creates an ADF (Application Definition File) package.
- **File share**
  - The file server on which the packages created are stored.
- **Installation Manager database**
  - Holds information about the package after its addition to the Presentation Server Console.
- **Installation Manager plug-in**
  - Allows for Installation Manager administration through the Presentation Server Console.
- **Network account**
  - A Windows domain account with Read/Write access to the network share point on the file server that stores the packages
- **ADF Installer Service**
  - Responsible for installing ADF packages on target Presentation Servers.

### **Installation Manager Deployment Process**

The user who installs packages to the target servers must have read access to the network share point and administrative access on the target servers.

Before you publish a packaged application, make sure the package has been added to the Installation Manager database.

The following processes are involved in deploying a package using Installation Manager:

- A package is created using the **Packager** and the ADF file is placed on the file server.
- The package is added to the **Installation Manager database** using the **Presentation Server Console, Packager** or **APPUTIL**.
- The package is scheduled for deployment using the **Presentation Server Console** or **APPUTIL**.
- The package is deployed to the target Presentation Servers.
- The **Presentation Server Console** is updated to display a job status of successful when the package has been deployed successfully.

### **Packager**

After using the Packager to create a package containing a recording, the Packager must be returned to a clean state.

The *rollback* function in the Packager returns the Packager to a clean state by removing all the changes made to the operating system, files and registry as a result of packaging an application.

The Packager does not need to be rolled back after creating a package that does not include a recording of an application installation.

To determine if a package must be rolled back, click **Tools** and select **Rollback** in the **Packager**.

If multiple packages are created before the Packager is rolled back, the packages must be rolled back in reverse order.

- For example, if Package1 was created and the Package2 was created without rolling back Package1, then Package2 must be rolled back before Package1 can be rolled back.

To rollback a package:

- Open the **Packager** and click **Tools > Rollback**.

- Select the name of the project to be rolled back.
- Click **Rollback**.
  - Click **Delete** instead of **Rollback** if you want to delete a project from the Packager without removing the changes made to the system during the package creation.
- Click **Yes**.
- Click **Close** and exit the **Packager**.

### Package Group

After applications are placed into a *package group*, an administrator can specify:

- The order in which the packages deploy to the target servers.
- The default network credentials to use when installing the packages.
- The file share location from which to locate the packages.

### Server Groups

*Server groups* simplify package installation. If an administrator is deploying packages to the same servers repeatedly, the servers can be grouped.

Using server groups, an administrator can select the name of the server group as the target rather than the names of the individual target servers.

### Unattended Installation

An administrator can perform an *unattended installation* or silent installation of an application by providing all of the responses necessary for the installation in an answer file.

To package an unattended installation:

- Open the **Packager** and click **Create a new project using project wizard** and click **Next**.
- Click **Package an Unattended Program (Service Pack, etc.)** and click **Next**.
- Specify a project name and location and click **Next**.
- Click **Browse**, navigate to the application installation program to be packaged and click **Open**.

- If needed, type the command line parameters for the installation program in the **Command Line Parameters** field.
- Select the packaging options. Choose from:
  - **Reboot after program installation**
  - **Run program from source location**
  - **Copy program plus the following files locally and then run the program**
- Select the file or folder options if **Copy program...** was chosen. Click **Next**.
- Click **Browse**, navigate to the network share point on the file server where the package is stored and click **OK**. Click **Next**.
- Verify the information on the **Results** screen and click **Finish**.
- Click **Project > Build Package**.
- Click **File > Save Project**.
- Check the network share point to verify that the package exists.

## Creating and Assigning Load Evaluators

---

### Load Evaluators

A *load evaluator* is a set of rules that can be used to determine the load on a server based on system resources and system resource consumption.

Load evaluators can be assigned to servers and applications.

All servers must have a load evaluator applied to them.

Only one load evaluator can be assigned to each server and each published application.

### Rules

The default full load for the **CPU Utilization** and **Memory Usage** rules is 90%. The default no load for both is 10%.

The **Context Switches** rule defines the number of times the operating system switches from one process to another.

The **Load Throttling** rule limits the number of concurrent connection attempts a server is expected to handle and cannot be applied to an individual application.

- The Load Throttling rule must be attached to a server to work.
  - If the Load Throttling rule is included in a load evaluator that is attached to a published application, the rule is ignored.

The **Server User Load** rule limits the number of sessions allowed to connect to a selected server.

The **CPU Utilization** rule defines the range of processor utilization for a selected server.

The **Memory Usage** rule defines the range of memory usage for a server.

### **Advanced Load Evaluator**

The *Advanced load evaluator* includes the rules:

- **CPU Utilization**
- **Load Throttling**
- **Memory Usage**
- **Page Swap rules**

### **Default Load Evaluator**

The *Default load evaluator* includes the rules:

- **Load Throttling**
- **Server User Load rules**

### **Boolean Rules**

*Boolean rules* are based on conditions being true or false.

Boolean rules must be used in conjunction with at least one other rule because they do not return actual load values for a server.

The two Boolean rules are:

- **IP Range**

The most trusted web site for Citrix certification preparation, Citrixexperience.com

- Defines the range of allowed or denied client IP addresses for a published application.
- **Scheduling**
  - Schedules the availability of selected published applications.

### **Custom Load Evaluator**

To create a custom load evaluator:

- Open the **Presentation Server Console**.
- Right-click the **Load Evaluators** node and click **New Load Evaluator**.
- Type the name for the custom load evaluator in the **Name** field.
- Type a description in the description field if desired.
- Click a rule in the **Available Rules** list and click **Add**.
- Configure the parameters for the selected rule and click **OK**.

### **Maximum Server Load**

When creating a custom load evaluator, the full load threshold value should be set below the value determined as the maximum sever load.

To determine the maximum server load, an administrator must first determine the baseline and peak values for key metrics on the server.

### **Sharing Information Across Zones**

By default, a data collector does not communicate the load information to other data collectors in the server farm.

If the administrator wants to share load information across zones, the **Share load information across zones** option must be selected in the server farm properties of the **Presentation Server Console**.

## Configuring Printing

---

### Types of Printing

In *client local printing*, the print job spools from the Presentation Server to the client device and then to the client local printer.

In *client network printing*, the print job spools from the Presentation Server to the client device or network print server, depending on the policy configuration, to the network print server and then to the network printer.

In *server network printing*, the print job spools from the Presentation Server to the network print server and then to the printer.

In *server local printing*, the print job spools from the Presentation Server to the server local printer.

### Import Print Server

To import a print server:

- In the **Presentation Server Console**, right-click **Printer Management** and click **Import Network Print Server**.
- In the **Network Print Server** dialog box:
  - Type the name or IP address of the print server in the **Server field**.
  - Type a user account name that has access rights to the specified printer in the **Connected As** field.
  - Type the password for the user account in the **Password** field. Click **OK**.

### Printer Policy Rules

**Auto-create all client printers** automatically connects all the printers on a client device.

**Always connect indirectly as a client printer** routes print jobs through the client device, where it is redirected to the network print server.

- Data sent to the client device is compressed using the ICA protocol; therefore, less bandwidth is consumed as the data travels across the WAN.

Applying a printer bandwidth policy allows the administrator to control the amount of maximum bandwidth in kilobytes per second that may be used for printing.

- This will free up some bandwidth for other resources, including applications, using the WAN link.

By creating a policy with **Auto-create client's default printer only**, logon times will be sped up because the client devices will no longer try to connect to and auto-create network print devices.

**Legacy client printers** enables the use of old-style client printer names as used by Terminal Services or Presentation Server 3.0 or earlier.

**Auto-creation** enables the use of auto-creation of all, local, default or no client printers.

**Printer properties retention** controls whether or not printer properties are stored on the client device or the user profile on the server.

**Print job routing** controls whether or not network print jobs flow directly from Presentation Server to the print server or take an extra step and are routed back through the client device.

- When the rule is configured to **Connect directly to network print server if possible**, the print jobs are routed directly from the Presentation Server to the network print server.
- If **Always connect indirectly as a client printer** is configured, print jobs are routed through the client device via the ICA protocol and redirected to the network print server.

**Turn off client printer mapping** disables the mapping of all client printers.

**Session printers** allows an administrator to control the assignment of network printers.

- Administrators can assign the default printer as well as designate the connection to network printers based on the desired policy filter.
- The policy can be configured by IP address.
  - For example: The IP range of the computers on each floor of a building can have a different policy so when a user is on the fifth floor they will have access to the fifth floor printers and when they have to move to floor two, they will have access to the second floor printers.

### **Print Drivers**

Before a printer can be used, a print driver must be installed on the Presentation Server.

To add, remove and reinstall print drivers on a server, and administrator can use the Drivers utility on a Windows Server by going to **Printers and Faxes > File > Server Properties > Drivers Utility**.

### **Print Driver Replication**

In order to make the print driver available on other servers in the server farm an administrator can leverage print driver replication to deploy the print driver to all member servers.

Print driver replication requires that the driver be installed and available on one server per base operating system.

The driver replication process can take a considerable amount of time and requires a substantial amount of system resources.

Because of these resource requirements, the replication should be performed during off-peak hours when higher priority traffic is not impacted.

An auto-replication list is created using the Presentation Server Console.

If a server is added to the server farm that does not have the print driver detected, the driver is installed.

To create a driver auto-replication list:

- Expand the **Printer Management** node in the **Presentation Server Console**.
- Right-click **Drivers**.
- Select **Auto-replication**.
- In the **Auto-replication** dialog box, select the appropriate operating system platform from the platform drop-down list.
- Click **Add** to add a print driver to replicate for the selected platform.
- Select the appropriate source server in the **Server** drop-down list.
  - If no specific source is required, the **Any** option can be used to list all print drivers available on all servers in the farm.
- Select **Overwrite existing drivers** if desired.
- Click **OK** in the confirmation if **Any** was chosen as the source server.
- Click **OK** in the **Auto-replication** dialog box.
- Click **OK** in the replication queue confirmation message.

### **Universal Print Driver**

The most trusted web site for Citrix certification preparation, Citrixexperience.com

Benefits of the universal print driver include:

- The enhanced metafile format which:
  - Reduces the size of some print jobs.
  - Allows jobs to print faster.
  - Allows users to set printer properties and preview documents ready for printing.
  - Reduces load on the server.
  - Bandwidth and CPU processing are saved.
- Reduces delays when spooling over slow connections.
- Avoids more problems in a diverse environment.
- Limits the installation and duplication of print drivers on servers.
- Ensures that client printers auto-create regardless of print driver availability on the server.
- Minimizes help desk calls.
- Enables users to print to almost any printer.
- Redirects client printers only.

By enabling the **Universal driver rule Use only printer model specific drivers**, the administrator makes sure that only the manufacturer's drivers are used.

By selecting the **Use universal driver only if the requested driver is unavailable** rule, an administrator makes sure that there is always a driver available, whether it's the manufacturer's driver or the universal driver by allowing the printers to first try to use the manufacturer's drivers, but if they are not available, the universal driver will be a fallback.

### **Native Drivers**

By not allowing native print drivers to automatically be installed from auto-created printers, administrators can make sure that no rogue drivers make it into the farm.

By using a print driver compatibility list, administrators can control which drivers are allowed in the farm.

If an administrator knows the drivers that are allowed, but doesn't know which drivers might try to install later, the administrator can select **Allow only drivers in the list** and add the known acceptable drivers to the list.

The policy **Native driver auto-install** can be set to the rule **Install Windows native drivers as needed**.

- That allows the manufacturer's print drivers to be used in the farm.

### **Printer Mappings**

Printer mappings can be managed using the Presentation Server Console or in an editable file named WTSUPRN.INF.

Note: The WTSPRNT.INF file lists the printer mappings made using the Presentation Server Console and should not be edited.

### **Printer Creation**

With *synchronous* printer creation, printers create before the users have access to interact with and use their sessions.

- Should be used when applications require all printers to be created first or when applications require a stable printing environment.
- The users must wait for all printers to create in the background before they can perform any activities.

With *asynchronous* printer creation, printers create in the background while the users have control of and are using their sessions.

- This minimizes the amount of time it takes for the users to begin using the application and does not impact the users because some application activity usually occurs before printing.

### **Printer Bandwidth**

Printer bandwidth can be limited on a per server basis through server properties or with a policy rule.

### **Printer Auto-Creation**

In some instances, it might be preferable to not auto-create client printers. In this case, an administrator can use the **Turn off client printer mapping** rule to auto-create only network printers or printers connected directly to the server.

By using the rule **Auto-create local client printers only**, only the printers connected directly to the user's client device through an LPT or other local port will be automatically connected.

- Enabling this setting ensures any network printers defined on the client device are not auto-created within the ICA session and logon times will be reduced for those who have several network printers configured on their client device.

### **SmoothRoaming**

*SmoothRoaming* allows a user to disconnect from one ICA session and reconnect from another device to continue that same session.

### **Print Driver Compatibility List**

The *print driver compatibility list* allows an administrator to control print drivers available to users.

During user logon, native drivers are permitted and the auto-created printers are checked against the list of allowed or denied print drivers.

A print driver mapping list resolves compatibility issues between print drivers that have different names for the same printer on different server operating systems.

## **Enabling Web Access to Published Applications and Content**

---

### **Web Interface Communication**

When a user logs into the Web Interface, the Web Interface forwards the logon credentials to the Citrix XML Service on the Presentation Server.

The Citrix XML Service retrieves a list of applications (the application set) that the user can access based on the supplied credentials.

### **Web Interface Browsing**

The following browsers can log on to the Web Interface: Internet Explorer 5.x, 6.x, and 7.0; Safari 2.0; Firefox 1.x; Mozilla 1.x; Netscape 7.0.

### **Configure Web Interface**

The Web Interface can be configured using the Access Management Console or by editing the WEBINTERFACE.CONF file.

### **Web Interface Sites**

An administrator can create:

- *An Access Platform site.*
  - Allows users to access remote and streamed applications and content using a web browser and a client.
- *A Program Neighborhood Agent Services site.*
  - Allows users to access remote and streamed applications, server desktops and content using Program Neighborhood Agent.
- *A Conferencing Manager Guest Attendee site.*
  - Allows guest users to access Conferencing Manager conferences through a web browser.

During the creation of a Web Interface site, an administrator can choose to store the site configuration information in a local file or in a server running the configuration service.

### **Active Directory Federation Services**

By enabling *Active Directory Federation Services* (ADFS), an administrator in a resource domain can create sites for users in an account partner's domain and the users in the account partner's domain will have single sign-on access to the published applications in the resource domain.

### **Web Interface Authentication**

Web Interface can be configured with:

- **Pass-through with smart card**
- **Anonymous**
- **Pass-through**
- **Smart card**
- **Explicit**

To make sure users have to enter their username and password every time they connect, **Explicit** must be selected for authentication.

To use RSA SecurID (or SafeWord), two-factor authentication must be configured.

### **Workspace Control**

In order to use workspace control:

- Client devices must have the Client for Windows 8.x or later.
- Presentation Server must be installed and configured.
- Web Interface must be installed and configured.

The following are some of the functionality of workspace control:

- Can only reconnect to existing sessions on Presentation Servers.
- Cannot reconnect anonymous users to applications after they disconnect.
- Prompts smart card users for their PINs for each reconnected session when pass-through authentication with smart cards is not enabled.
- Requires that the Web Interface be set to override the client name setting in the **Manage session preferences** task.

Workspace control functions are disabled:

- If the Web Interface detects that it is being accessed from within a client session.
- If pass-through or smart card authentication methods are used and no trust relationship exists between the Web Interface server and the Presentation Servers.

An administrator can configure workspace control:

- To provide automatic reconnection during logon.
- Provide automatic reconnection after logon, log off all sessions when a user logs off from the Web Interface site.
- Allow users to customize the Web Interface site.

When configuring workspace control, an administrator can choose:

- **Automatic reconnect to session when user logs in** provides automatic reconnection during logon.

- **Automatic reconnect to sessions after user logs in** provides automatic reconnection after logon.
  - For either configuration, the administrator can choose:
    - ◆ **All sessions**, which allows the user to automatically reconnect both disconnected and active sessions.
    - ◆ **Disconnected sessions only**, which allows users to automatically reconnect to disconnected sessions.
    - ◆ **Allow users to customize**, which allows users to change the setting.

### Multiple Web Interface Sites

Multiple sites can be grouped together, provided they use the same configuration source, use the same operating system (technology), are of the same type (for example, Access Platform), are of the same version and are NOT locally configured.

The **Create site group** task is not available for locally configured sites.

### Configure Web Interface Site

After creating a Web Interface site, the administrator configures the initial settings. During the initial configuration, the administrator can set the type of applications made available to users:

- **Remote**
- **Streaming**
- **Dual mode streaming**

After the initial configuration, the administrator can set:

**Allow users to launch applications using browser bookmarks** to allow users to create persistent links to published applications in their favorites list.

**Using the Advanced Access Control** to allow users to access the site through Citrix Access Gateway.

### Access Platform Configuration

To restrict access based on domains:

- In the **Access Management Console**, expand the **Web Interface** node.
- Click the desired Access Platform Site node.
- Click the **Configure authentication methods** task.
- Click **Properties**.
- Click **Domain Restriction** in the left pane of the Access Platform authentication methods properties.
- Choose **Restrict domains to the following domains**.
- Add the domains that are allowed access. Click **OK**.

### **Citrix Password Manager Integration**

To integrate Citrix Password Manager into the authentication of the Access Platform site:

- In the **Access Management Console**, expand the **Web Interface** node.
- Click the desired Access Platform Site node.
- Click the **Configure authentication methods** task.
- Click **Properties**.
- Click **Account Self Service** in the left pane of the Access Platform authentication methods properties.
- In the **Account Self Service** window, you can choose to enable password reset or allow account unlock.
  - To only allow users to change their password when it expires, **Allow users to change password** must be configured for **Only when it expires** in the **Password Settings** window.
- Click **OK**.

### **DMZ Settings**

*Direct access* is typically configured in situations where internal users connect from trusted environments, such as a corporate intranet, and there is no need to keep the address of the Presentation Server private.

*Alternate access* is configured in situations where the IP address of the Presentation Server must be kept private from users.

- An administrator must configure Presentation Server to use an alternate address by using the ALTADDR command.
- If multiple servers are being used to provide application access, translated access would be used.

*Translated access* is configured in situations where the IP address of the Presentation Server must be kept private from users and multiple servers in the server farm are used to provide application access.

When a firewall is used, Web Interface must be configured with the appropriate IP address in the client files.

## **Securing Access to Published Applications and Content**

---

### **Securing Communication**

*ICA encryption* guards against the threat of eavesdropping by securing the information sent between the client device and Presentation Server.

- Available in Basic, RC5 (128-bit) logon only, RC5 (40-bit), RC5 (56-bit) and RC5 (128-bit).
- Is configured in Presentation Server policies or published applications.

*Citrix SSL Relay* can secure end-to-end communication between client devices and Presentation Servers using encryption and communications with servers that host the XML Service in small environments.

- Can be used to secure communication between the Web Interface server and Presentation Server.
- Provides end-to-end encryption of ICA communications between client devices and Presentation Server and XML communications between Web Interface and Presentation Server.
- When SSL Relay is used, an administrator can configure which ciphersuites will be used.
  - A ciphersuite is an encryption/decryption algorithm.
    - ◆ Presentation Server, by default, provides COM and GOV ciphersuites.

To configure SSL Relay:

The most trusted web site for Citrix certification preparation, Citrixexperience.com

- Obtain and install a unique server certificate on each Presentation Server.
- Install a root certificate on each client device and Web Interface server.
- Configure the relay credentials, connections and ciphersuites using the **SSL Relay Configuration** tool.
- Restart the Presentation Servers.

*Secure Gateway* can secure large server environments and provide Internet access to servers in a server farm with a single point of encryption, the internal IP addresses of servers hidden and two-factor authentication support through Web Interface.

### **Web Interface and Secure Gateway**

To configure a Web Interface site to work with Secure Gateway:

- In the **Access Management Console** click the **Manage secure access** task and click **Edit gateway settings**.
- Type the FQDN of the Secure Gateway server in the **Address (FQDN)** field.
- Configure session reliability.
- Configure the STA settings.
- Click **OK**.

### **DMZ Settings**

In a single-hop DMZ deployment of Secure Gateway, a server certificate must be installed on:

- The Secure Gateway Server
- The Web Interface Server
- The Presentation Server

A root certificate will be installed on:

- Secure Gateway
- Web Interface Server
- Client device

The most trusted web site for Citrix certification preparation, Citrixexperience.com

*Gateway direct* sends the actual address of the Presentation Server to the Secure Gateway.

*Gateway alternate* sends the alternate address of the Presentation Server to the Secure Gateway.

*Gateway translated* uses the address translation mappings in the Web Interface to determine which address is sent to the Secure Gateway server.

- Gateway translated uses the address translation mappings set in the Web Interface to determine which address is sent to the Secure Gateway server.
- This setting is useful when the address and port of the Presentation Server are translated at the internal firewall.

To configure Gateway translation:

- In the **Access Management Console** click the **Manage secure client access** task and click **Edit DMZ settings**.
- Configure the client route by choosing **Add a new client route**, **Edit an existing client route** or **Remove an existing client route**.
- Select **Translated** as the access method.
- Click **Manage secure client access** in the task pane and click **Edit address translations**.
- Click **Add**.
- Configure the internal and external IP address translation mappings by selecting **Client route translation**, **Gateway route translation** or **Client and Gateway route translation**.
- Type the internal IP address of a Presentation Server in to the **Internal IP address** field.
- Type the internal port number of a Presentation Server into the **Internal port** field.
- Type the translated (external) IP address or host name that client devices must use to connect to a Presentation Server into the **External address** field.
- Type the external port number of a Presentation Server into the **External port** field. Click **OK**.