

Citrixperience.com

**1Y0-456 Citrix Access Suite 4.0:
Build/Test**

Study Guide

Version 1.0

(September 15, 2006)

Citrix® Access Suite 4.0: Build/Test Study Guide

This study guide was created by Citrixxperience.com. Used for creation of this study guide, besides personal field experience, was the Citrix® courseware CTX-1456AI Citrix® Access Suite 4.0: Build/Test Workshop, which is a copyright of Citrix® Systems.

Along with the courseware listed above, this study guide is meant to be used in preparation for the 1Y0-456 Citrix® Access Suite 4.0: Build/Test exam. Also suggested for preparation are other books that relate to the subjects and above all, personal experience with the products. Citrixxperience.com recommends further preparation by using other 1Y0-456 products found at www.Citrixxperience.com.

The license for this study guide is for one user only. It is a copyright of Citrixxperience.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 Citrixxperience.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 Citrixxperience.com in any way.

Table of Contents

<u>Subject</u>	<u>Page</u>
Building and Testing Citrix Presentation Server	1
Building and Testing Citrix Password Manager	14
Building and Testing Access Gateway Advanced Edition	25

Building and Testing Citrix Presentation Server

Windows concepts

Group Policy objects allow the administrator to restrict or permit specific user functions and actions without having to change the registry directly.

NTFS Permissions set the level of access user groups have to files and folders on the server.

Profiles provide users with pre-configured or personalized environments, including the Windows desktop and application settings.

Presentation Server testing and developing environments

Testing or development Presentation Server environments should be segregated from the production environment so that they do not impact the existing production environment.

- ❖ Testing and development Presentation Servers should not belong to the same farm as the production servers.
- ❖ Setting up a separate zone for the test servers in the production farm is not a good option.

Presentation Server features

Session Reliability enables users to continue to view their published applications while the connection to the server is temporarily interrupted. After connectivity is regained, users can resume interaction with the published applications without launching them again.

- ❖ Presentation Server uses the Citrix Server XTE Service for session reliability.
- ❖ Session reliability uses TCP port 2598.
- ❖ Session reliability is tunneled by means of the Citrix Common Gateway Protocol.
- ❖ Session reliability is enabled by default in the farm properties of the Presentation Server farm.

Virtual IP addressing assigns an IP address to a session to address some of the issues associated with applications that identify the client connection to the back end of Presentation Server-based applications by an IP address.

- ❖ Use virtual IP addressing for:
 - ◆ Applications that require each session to have its own IP address for licensing, routing or addressing purposes.
 - ◆ Network monitoring systems that require each session to have its own IP address in order to track individual user's traffic
 - Without the use of a virtual IP address, all users appear to have the same IP address when connecting from Presentation Server to a backend application. The virtual IP address feature assigns an IP address to a session, not to a user.

- ◆ Applications that may be hard-coded to a specific port on a loopback interface or that may be hard-coded to listen to a specific port on all interfaces and require more than one IP address when running multiple instances in a Terminal Server environment
- ❖ Virtual IP addressing is only available for ICA sessions, not for RDP sessions.
- ❖ Virtual IP addressing is available with the Advanced and Enterprise editions of Presentation Server.

Add groups to Citrix administrators

- ❖ Click **Start > All Programs > Citrix > Management Consoles > Presentation Server Console**.
- ❖ Right-click the **MetaFrame Administrators** node in the left pane.
- ❖ Click **Add MetaFrame Administrator**.
- ❖ Double-click the desired domain.
- ❖ In the domain, double-click the desired user groups.
- ❖ Click **Next** in the **Alert Contact Details** screen.
- ❖ Click **Custom** and click **Next**.
- ❖ Select the permissions that the groups will have.
- ❖ Click **Finish**.

Create a Presentation Server policy

- ❖ In the Presentation Server Console, right-click the **Policies** node in the left pane and select **Create Policy**.
- ❖ Type the policy name in the **Policy Name** field.
- ❖ Click **OK**.

Configure a Presentation Server policy

- ❖ In the Presentation Server Console, click the **Policies** node.
- ❖ Right-click the desired policy in the right pane and select **Properties**.
- ❖ Navigate to the desired policy in the left pane of the policy's properties window.
- ❖ Configure the policy in the right pane of the policy's properties window.
- ❖ After configuring the policy, apply the policy to using **Access Control, Client IP Address, Client Name, Servers** or **Users**.

Apply a Presentation Server policy

- ❖ In the Presentation Server Console, click the **Policies** node.
- ❖ Right-click the desired policy in the right pane and select **Apply this policy to**.
- ❖ The **Policy Filters** window launches.
- ❖ In the left pane of the **Policy Filters** window, select from the following:
 - ◆ **Access Control**
 - Check **Filter based on Access Control**.
 - Check **Apply to connections made through MetaFrame Secure Access Manager (version 4.0 or later)**.
 - Check either:
 - **Any connection**
 - Or
 - **Any connection that meets any of the following filters**
 - The **Add MetaFrame Secure Access Manager Filter** window pops up.
 - Add the MetaFrame Secure Access Manager farm and MetaFrame Secure Access Manager filter in the drop down lists.
 - Click **OK** to close the **Add MetaFrame Secure Access Manager Filter** window.
 - If desired, check **Apply to all other connections**.
 - ◆ Click **OK** to close the **Policy Filters** window.
 - ◆ **Client IP Address**
 - Check **Filter based on client IP address**.
 - Check **Apply to all IP addresses**.
 - Or
 - Click **Add**.
 - The **Add Client Address to Policy Filter** window launches.
 - Add an IP range or an IP address.
 - Click **OK** to close the **Add Client Address to Policy Filter** window.
 - ◆ Click **OK** to close the **Policy Filters** window.
 - ◆ **Client Name**
 - Check **Filter based on client name**.

- Check **Apply to all client names**.
- Or
- Click **Add**.
 - The **Add Client Name to Policy Filter** window launches.
 - Type a client name in the **Client Name** field and click **OK** to close the **Add Client Name to Policy Filter** window.
- ◆ Click **OK** to close the **Policy Filters** window.
- ◆ **Servers**
 - Check **Filter based on servers**.
 - Select the desired servers and click **OK** to close the **Policy Filters** window.
- ◆ **Users**
 - Check **Filter based on users**.
 - Select **Apply to all explicit (non-anonymous) users**.
 - Or
 - Select **Apply to anonymous users**.
 - If desired, explicitly select groups and/or users and choose to either **Allow** or **Deny** them.
- ◆ Click **OK** to close the **Policy Filters** window.

Configure a drive mapping policy

- ❖ Create a policy.
- ❖ Right-click on the policy and select **Properties**.
- ❖ Navigate to **Client Devices > Resources > Drives > Mappings**.
- ❖ In the mapping policy rule, select **Not Configured**, **Disabled** or **Enabled**.
 - ◆ If **Enabled** is selected, select the drives you do not want to map to client devices by checking **Turn off Floppy disk drives**, **Turn off Hard drives**, **Turn off CD-ROM drives** and/or **Turn off Remote drives**.
- ❖ Filter the connections that this policy will be applied to by **Access Control**, **Client IP address**, **Client Name**, **Servers** or **Users**.

Configure COM and LPT ports in a policy

- ❖ Create a policy.
- ❖ Right-click on the policy and select **Properties**.

- ❖ Navigate to **Client Devices > Resources > Ports**.
- ❖ Configure the policy rules **Turn off COM ports** and **Turn off LPT ports**.
- ❖ Filter the connections that this policy will be applied to by **Access Control, Client IP address, Client Name, Servers** or **Users**.

Configure a printer auto-creation policy

- ❖ Create a policy.
- ❖ Right-click on the policy and select **Properties**.
- ❖ Navigate to **Printing > Client Printers**.
- ❖ In the **Auto-creation policy** rule, select **Not Configured, Disabled** or **Enabled**.
 - ◆ If **Enabled** is selected, select to **Auto-create all client printers, Auto-create local (non-network) client printers only, Auto-create the client's default printer only** or **Do not auto-create client printers**.
- ❖ Filter the connections that this policy will be applied to by **Access Control, Client IP address, Client Name, Servers** or **Users**.

Configure a shadowing policy

- ❖ Create a policy.
- ❖ Right-click on the policy and select **Properties**.
- ❖ Navigate to **User Workspace > Shadowing**.
- ❖ Configure the **Configuration** and **Permissions** policy rules.
- ❖ In each policy rule, select **Not Configured, Disabled** or **Enabled**.
 - ◆ If the Configuration rule is **Enabled**, select **Do Not Allow Shadowing** or **Allow Shadowing**.
 - If **Allow Shadowing** is chosen, check **Prohibit Being Shadowed Without Notification** and/or **Prohibit Remote Input When Being Shadowed**.
 - ◆ If the **Permissions** policy rule is **Enabled**, select users to give permissions to shadow the connections to which the policy applies.
- ❖ Filter the connections that this policy will be applied to by **Access Control, Client IP address, Client Name, Servers** or **Users**.

Shadow a user

- ❖ Open the Presentation Server Console, expand the **Servers** node and click a server.
- ❖ Select the **Users** tab.
- ❖ Right-click a user and select **Shadow**.

- ❖ Note the shadow termination hotkey setting (CTRL + *) and click **OK**.
- ❖ Authenticate with your username and password.
- ❖ When done shadowing, click **Stop Shadowing** or use the hotkey, **CTRL + ***.

Configure and verify a Zone Preference and Failover policy

- ❖ Create a policy named **Zone Preference and Failover**.
- ❖ Right-click on the **Zone Preference and Failover** policy and select **Properties**.
- ❖ Navigate to **User Workspace > Connections > Zone preference and failover**.
- ❖ Click **Enabled** in the right pane.
- ❖ Select one primary and up to five backup zones.
- ❖ Filter the connections that this policy will be applied to by **Access Control, Client IP address, Client Name, Servers** or **Users**.
- ❖ In the Presentation Server Console, expand the **Servers** node, click a server and select the **Users** tab.
- ❖ Verify that the users are connected to the correct servers according to the **Zone Preference and Failover** policy.

Rename a zone

- ❖ Right-click the farm node in the Presentation Server Console and select **Properties**.
- ❖ Select **Zones** in the left pane of the farm properties.
- ❖ Select the desired zone name in the right pane and click **Rename**.
- ❖ Type a new name in the **New zone name** field and click **OK**.

Create a new zone

- ❖ Right-click the farm node in the Presentation Server Console and select **Properties**.
- ❖ Select **Zones** in the left pane of the farm properties.
- ❖ Click **New Zone** in the right pane.
- ❖ Type a new name in the **New zone name field** and click **OK**.

Move a server between zones

- ❖ Right-click the farm node in the Presentation Server Console and select **Properties**.
- ❖ Select **Zones** in the left pane of the farm properties.
- ❖ Expand the desired zone in the right pane of the farm properties.

- ❖ Click the desired server name under the desired zone.
- ❖ Click **Move Servers**.
- ❖ Click **Yes** in the **Server Reboot Required** message.
- ❖ Verify that the correct zone is selected in the **Select Target Zone** drop-down list and click **OK**.
- ❖ Reboot the server that was moved.

Change data collector preference

- ❖ Right-click the farm node in the Presentation Server Console and select **Properties**.
- ❖ Select **Zones** in the left pane of the farm properties.
- ❖ Expand the desired zone in the right pane of the farm properties.
- ❖ Right-click the desired server name under the desired zone.
- ❖ Click **Set Election Preference**.
- ❖ Choose among **Most Preferred**, **Preferred**, **Default Preference** and **Not Preferred** and click **OK**.
- ❖ Reboot the server whose preference was changed.

Publish an application

- ❖ To publish an application, right click on the **Applications** node in the Presentation Server Console and select **Publish Application**.
- ❖ Type the display name in the **Display Name** field of the **Welcome** screen and click **Next**.
- ❖ In the **Specify What to Publish** screen, verify that **Application** is selected, click **Browse** and navigate to the application file and click **Next**.
- ❖ Click **Next** in the **Program Neighborhood Settings** screen.
- ❖ Select the color depth in the **Specify Application Appearance** screen and click **Next**.
- ❖ Click **Next** in the **Specify Requirements** screen, **Specify Application Limits Screen** and **Configure Access Control** screen.
- ❖ In the **Specify Servers** screen, click on the first server you desire to run the application, hold down the **Control** key and click on any other servers you desire to select.
- ❖ Click **Add** to add the servers and click **Next**.
- ❖ Drill down to the correct **Organizational Unit** and select the groups and/or users that will have access to this published application in the **Specify Users** screen and click **Next**.

- ❖ Click **Finish** in the **Specify File Type Associations** screen.

Publishing multiple applications

To save time publishing multiple applications, use the **Copy Published Application** feature.

- ❖ To use this feature, create the first published application using the **Application Publishing Wizard**.
- ❖ Right-click on the published application and select **Copy Published Application**.
- ❖ Right-click on the copied application and select **Rename**.
- ❖ Type the name of the application in the **Display Name** field and click **OK**.
- ❖ Right-click the new published application and select **Properties**.
- ❖ In **Properties**, select **Application Location**.
- ❖ Click **Browse**, browse to the application you wish to publish and click **OK**.
- ❖ Click **Program Neighborhood Settings**, click **Change Icon**, select the correct icon and click **OK**.
- ❖ Configure anything else in the properties that the new published application warrants.

Application isolation environment

An *application isolation environment* allows an application in Presentation Server to use virtual copies of resources instead of the actual resources by redirecting communication between the application and system resources, such as the file system and registry.

Install an application into an application isolation environment

- ❖ In the Presentation Server Console, right-click on the **Isolation Environments** node and select **New isolation environment**.
- ❖ Type the name of the isolation environment in the **Application isolation environment name** field and click **OK**.
- ❖ Open a command prompt and type **AIESETUP "<isolation environment name>" <path>** and press enter.
 - ◆ For example, if you are installing Power Point Viewer 97 and you already created an isolation environment named **PowerPointViewer97**, you would type the following: **AIESETUP "PowerPointViewer97" "c:\Program Files\Microsoft\Power Point Viewer\PPVIEW97.EXE"**.
- ❖ Run through the application installation.
- ❖ Press **Enter** at the command prompt to begin the application discovery process.
- ❖ Exit the command prompt after the application discovery completes.

- ❖ Right-click the **Applications** node in the Presentation Server Console and select **Publish Application** to launch the **Application Publishing Wizard**.
- ❖ Type the display name in the **Display Name** field and click **Next**.
- ❖ Verify that **Application** is selected in the **Specify What to Publish** screen, check **Isolate Application** and click **Settings**.
- ❖ Click the correct isolation environment name and select **Application was installed into environment**.
- ❖ Click the **Application** name in the **Choose installed application** drop-down list and click **OK**.
- ❖ Go through the rest of the **Application Publishing Wizard**.

Client-to-server redirection

Client-to-server redirection allows a published application to launch when a file with a certain file extension is accessed on a client device.

- ❖ To specify client-to-server content redirection, in the **Application Publishing Wizard**:
 - ◆ In the **Specify File Type Associations** screen, check the file types that you wish to associate with the application.
- ❖ To specify client-to-server redirection in the properties of a published application:
 - ◆ Select **Content Redirection** in the right pane of **Properties** and check the file types that you wish to associate with the application.

Server-to-client redirection

Server-to-client redirection allows URL links in a server session to redirect information back to an application on the client device.

- ❖ Server-to-client redirection is configured in a policy in **User Workspace > Content Redirection > Server to client**.

Update file type association data

- ❖ In the Presentation Server Console, right-click on the farm node and select **Update File Types from Registry**.
- ❖ In the **Update File Type Association** screen, select the servers you wish to add to the update and click **OK**.
- ❖ Click **OK** on the pop-up that says **File type association data is being updated. This may take several minutes to complete.**

Apply a load evaluator to servers

- ❖ To apply a load evaluator to all of the servers in the farm, right-click the **Servers** node in the Presentation Server Console and select **Load Manage Servers**.
- ❖ Click **Add All** in the **Load Manage Servers** screen under **Available Servers**.
- ❖ Verify the correct load evaluator is chosen under **Available Load Evaluators** and click **OK**.
- ❖ To confirm the load evaluator, click the **Load Evaluators** node and select the **Usage Reports** tab.
- ❖ Verify that the correct load evaluator is listed for all of the servers.

The scheduling load evaluator

- ❖ To create a new load evaluator based on scheduling, right-click the **Load Evaluators** node in the Presentation Server Console and select **New Load Evaluator**.
- ❖ Select **Scheduling** in the **Available Rules** box.
- ❖ Select the days of week and times of day under **Rule Settings** and click **OK**.

Attach a load evaluator to an application

- ❖ To attach a load evaluator to an application and confirm on a server, expand the **Applications** node in the Presentation Server Console.
- ❖ Right-click the desired published application and select **Load Manage Application**.
- ❖ Select the servers that the application will be monitored on in the **Available Servers** list and click **Add**, or if all servers, click **Add All**.
- ❖ Select the load evaluator in the **Available Load Evaluators** list and click **OK**.
- ❖ To verify the configuration, click the **Load Evaluators** node, select the **Usage Reports** tab and click **By Application**.

Enable virtual IP addressing

- ❖ Right-click the farm node in the Presentation Server Console and select **Properties**.
- ❖ In **Properties**, select **Virtual IP Address Configuration** in the left pane and click **Add IP Range** in the right pane.
- ❖ The **Add IP Range** window launches.
- ❖ Type the IP address range and subnet mask in the **Add IP Range** window and click **OK**.
- ❖ Click **Yes** on the **Configure Servers** pop up.
- ❖ The **Virtual IP Address Range** widow launches.

- ❖ Click **Add** in the **Virtual IP Address Range** window.
- ❖ The **Add Server For** window launches.
- ❖ Select the servers in the **Add Server For** window and click **OK**.

Apply and verify virtual IP addressing to an application

- ❖ Right-click the farm node in the Presentation Server Console and select **Properties**.
- ❖ Select **Virtual IP Processes** in the left pane of **Properties**.
- ❖ Click **Add Processes** in the right pane of **Properties**.
- ❖ The **Add Process for Virtual IP** window launches.
- ❖ Type the application name in the **Add Process for Virtual IP** window and click **OK**.
- ❖ Restart the server.
- ❖ To verify that virtual IP addresses are applied to the application configured for virtual IP addresses, in the Presentation Server Console, expand the **Servers** node.
- ❖ Click a server and select the **Sessions** tab.
- ❖ Verify that virtual IP addresses are assigned for the virtual IP address-configured application sessions.

Use the universal printer driver exclusively

- ❖ To use only the universal printer driver and disable automatic printer driver installation in the Presentation Server environment, create a policy in the Presentation Server Console.
- ❖ Right-click on the policy and click **Properties**.
- ❖ In the policy properties, expand **Printing > Drivers** and select **Universal Driver** in the left pane.
- ❖ Select **Enabled** in the right pane.
- ❖ Select **Use universal driver only** from the **When auto-creating client printers** drop-down list and click **Apply**.
- ❖ Select **Native printer auto-install** in the left pane of the policy properties.
- ❖ Select **Enabled** in the right pane.
- ❖ Select **Do not automatically install drivers** and click **OK**.

Verify the exclusive use of the universal printer driver

- ❖ To verify that only the universal printer driver is being used for printing in the Presentation Server environment, first add a printer to use for testing.

- ◆ To add a printer, click **Start > Printers and Faxes**.
- ◆ Click **Add a Printer** and click **Next**.
- ◆ Verify that **Local printer attached to this computer** is selected.
- ◆ Deselect **Automatically detect and install my Plug and Play printer** and click **Next**.
- ◆ Verify that **Use the following port: LPT1** is selected and click **Next**.
- ◆ Select any printer and click **Next**.
- ◆ Accept the default printer name and click **Next**.
- ◆ Click **Next** in the **Location and Comment** screen.
- ◆ Click **No** in the **Print Test Page** screen and click **Next**.
- ◆ Click **Finish**.
- ❖ Launch an application from Web Interface.
- ❖ In the application, click **File > Print**.
- ❖ Select your printer from the drop-down list.
- ❖ Verify that the **Citrix Universal Printer** is listed as the printer type.
- ❖ Close the **Print** window.

Create a Web Interface site

- ❖ Open the Access Suite Console.
- ❖ Launch the **Configure and run discovery** wizard from **Common Tasks** of the farm node.
- ❖ Click **Next** in the **Welcome** screen.
- ❖ Click **Next** in the **Select Products or Components** screen.
- ❖ In the **Configuration Servers** screen, verify **Contact the following Web Interface configuration servers** is selected and click **Add**.
- ❖ The **Add Server** window launches.
- ❖ Type the server name and click **OK**.
- ❖ Click **Next** in the **Configuration Servers** screen.
- ❖ Select **Add Local Computer** if desired and click **Next**.
- ❖ Click **Next** in the **Preview Discovery** screen.
- ❖ Wait for **Discovery** to finish running and click **Finish**.
- ❖ Click the **Web Interface** node in the Access Suite Console.

- ❖ Click **Create site** under **Common Tasks**.
- ❖ In the **Select Site Type** screen, select **MetaFrame Presentation Server** and click **Next**.
- ❖ In the **IIS Hosting** screen, select **Set as the default page for the IIS site** to apply the path and click **Next**.
- ❖ In the **Configuration Source** screen, select **Use local configuration file(s)** or **Use centralized configuration** and click **Next**.
- ❖ In the **Server farm** screen, type the name of the server farm.
- ❖ Click **Add** to type the name of any servers desired for failover.
- ❖ In the **New Site Summary** screen, verify the information and click **Next**.
- ❖ After the new site is created, click **Finish**.

Configure authentication for Web Interface

- ❖ In the Access Suite Console, navigate to **Suite Components > Configuration Tools > Web Interface** and click on the desired Web Interface site.
- ❖ Click **Configure authentication methods** under **Common Tasks**.
- ❖ The **Configure Authentication Methods** wizard launches.
- ❖ In the **Specify authentication methods** screen, choose **Explicit**, **Pass-through**, **Pass-through with smart card**, **Smart card** or **Anonymous**.
 - ◆ If **Explicit** or **Pass-through** is chosen, configure the settings.
- ❖ Click **Next**.
- ❖ Configure **Define selected methods** screen and click **Next**.
- ❖ Configure **Specify authentication type settings** screen and click **Next**.
- ❖ Verify the information in the **Check Summary** screen and click **Finish**.

Client for Web deployment

- ❖ To configure an English Client for Web deployment, create a new folder named **en** in **C:\Program Files\Citrix\Web Interface\4.0\ICAWEB** on the Presentation Server.
- ❖ Inside of the **en** folder, create a new folder named **ica32**.
 - ◆ Make sure **ica32** is typed in lower case.
- ❖ Copy the **WFICAT.CAB** file from the **Presentation Server Components CD** to the **ica32** folder.
- ❖ Navigate to the **Web Interface** site in the Access Suite Console and click **Manage client deployment** in **Common Tasks**.

- ❖ The **Manage Client Deployment** wizard launches.
- ❖ Select the clients in the **Select launch clients** screen, choosing among **Local client (Default)**, **Native embedded client**, **Client for Java** and **Embedded Remote Desktop Connection**.
 - ◆ You can also allow the user to select.
- ❖ Configure automatic client update, automatic client fallback to Client for Java, installation caption and client version support in the **Specify launch client settings** screen.
- ❖ Specify the file name, version and class ID in the **Web Client settings** screen.
- ❖ In the **Client for Java** screen, choose packages to include with in the Java Client.
 - ◆ Packages include **Audio**, **Clipboard**, **Local text echo**, **SSL/TLS**, **Encryption**, **Client drive mapping**, **Printer mapping** and **Configuration UI**.
 - You can also let the user choose.
- ❖ Select a private root certificate, if desired.
- ❖ Review the **Preview summary** screen and click **Finish** when satisfied.

Verify the Web Interface automatic Web Client download

- ❖ To test the Web Interface configuration for automatic Web Client download, open Internet Explorer and browse to **http://<WebInterfaceServer>/Citrix/MetaFrame** (replace **<WebInterfaceServer>** with the name of your Web Interface server).
- ❖ Logon as a user, click **Yes** in the download screen to download the Web Client and click **Yes** on the **Citrix License Agreement**.
- ❖ The Client software installs without user interaction.

Building and Testing Citrix Password Manager

Using Active Directory for the central store

To use Active Directory as the central store, an administrator must:

- ❖ Enable schema updates.
 - ◆ Windows 2000 Server only, not Windows Server 2003.
- ❖ Extend the schema.
- ❖ Create a central store.
- ❖ Assign permissions to the domain.

Password Manager features

The *Password Manager Service* provides the foundation for the optional features, including *Account Self-Service*, *Automatic Key Recovery*, *Cryptographic Data Integrity Assurance* and *Password Provisioning*. Password Manager must be installed and configured before implementing any of these features.

- ❖ The *XTE Service* hosts the Password Manager Services.
- ❖ The Citrix Password Manager Service is run on a web server that uses SSL to encrypt the data shared by the Citrix Password Manager Service, the console and the agent.

Account Self-Service allows users to reset their Active Directory passwords.

- ❖ *Self-Service Password Reset* is a feature of Account Self-Service which allows Password Manager users in an Active Directory environment to reset their primary domain password without the intervention of the Help Desk or an administrator.
- ❖ *Self-Service Password Unlock* is a feature of Account Self-Service which works in the same way as Self-Service Password reset to unlock domain accounts.

Automatic Key Recovery allows users to log on to the network and have immediate access to applications managed by Password Manager without the need to verify their identity.

Cryptographic Data Integrity Assurance protects the central store data from being compromised while in transit to the agent.

Password Provisioning pre-populates the central store with users' secondary credentials, ensuring that they do not have to provide their credentials to the agent when launching the application for the first time.

Question-based authentication provides an additional layer of security to the Password Manager agent software by protecting against impersonation of unauthorized password changes. This security feature requires that users answer questions in the questionnaire provided by the administrator when they first used the Password Manager agent and when password reset is used. The questionnaire is the same one as used for Account Self-Service.

Password expirations allow administrators to manage regular and transparent changes on applications that do not have password change functionality.

Password Manager used with Java applications

For Java applications, administrators can select the **Control ID** option instead of the **SendKeys** option to configure the application definitions. The **Control ID** option provides visual cues, such as highlighting the selected field, during the configuration process.

Requirements for the Password Manager Service

- ❖ A server authentication certificate must be installed on the server hosting the Password Manager Service to enable SSL configuration.
- ❖ The certificate common name needs to match the FQDN of the server running the Password Manager Service.

- ❖ An administrator must install the certificate in the local machine certificate store on the server running the Password Manager Service and install the trusted root certificate on all systems communicating with the Password Manager Service.

Extend the Schema and verify its success

- ❖ Register the **Active Directory Schema** snap-in by running **REGSVR32 SCHMMGMT.DLL** in a command prompt.
- ❖ Type **OK** to the **RegSvr32** message.
- ❖ Open an MMC and add the **Active Directory Schema** snap-in.
- ❖ Expand the **Classes** and **Attributes** nodes to verify there are no Citrix-related items (any item names that begin with **citrix**).
- ❖ After verification, insert the **Password Manager CD**, and when the splash screen appears, click **Prerequisite: Create your Central Store**.
- ❖ In the **Prerequisite: Create your Central Store** screen, click **Active Directory**.
- ❖ In the **Create your Central Store using Active Directory** screen, click **Extend your Active directory schema for the new directory objects**.
 - ◆ This option runs the **CitrixSchemaPrep.EXE** utility.
- ❖ Click **Yes** in the warning pop-up.
- ❖ Press **Enter** to continue.
- ❖ To verify success, open the **Active Directory Schema** in the MMC and click the **Classes** node.
 - ◆ Verify that **citrix-SSOConfig** and **citrix-SSOSecret** were added.
- ❖ Click the **Attributes** node.
 - ◆ Verify that **citrix-SSOConfigData**, **citrix-SSOConfigType** and **citrix-SSOSecretData** were added.

Create an Active Directory central store

- ❖ In the **Password Manager CD** installation window, click **Create your central store in the extended schema**.
 - ◆ Clicking this option runs the **CtxDomainPrep.EXE** utility that updates permissions of the domain root, allowing users to create the objects they need to use Citrix Password Manager.
- ❖ Click **Yes** in the warning pop-up.
- ❖ Press **Enter** to continue when prompted.

Request and install a web certificate

- ❖ Connect to the **Certificate Authority** in Internet Explorer by browsing to **http://<ServerName>/certsrv**.
 - ◆ Replace **<ServerName>** with the name of the server running the **Certificate Authority**.
- ❖ Click **Request a certificate**.
- ❖ Click **advanced certificate request**.
- ❖ Click **Create and submit a request to this CA**.
- ❖ Click **Web Server** from the **Certificate Template** drop-down list.
- ❖ Type the FQDN of the server running the Password Manager Service.
- ❖ Verify that **1024** is selected in the **Key Size** field.
- ❖ Select **Store certificate in the local computer certificate store**.
- ❖ Click **Submit** to generate the server certificate.
- ❖ Click **Yes** in the **Potential Scripting Violation** warning.
- ❖ Click **Install this certificate**.
- ❖ Click **Yes** in the **Potential Scripting Violation** warning.
- ❖ Close Internet Explorer when the **Certificate Installed** screen appears.

Verify that a server certificate is installed correctly

- ❖ Open the Microsoft Management Console and add the **Certificates** snap-in.
- ❖ Expand the **Certificates** node.
- ❖ Expand the **Personal** node.
- ❖ Click **Certificates** and confirm that the Password Manager FQDN is listed.
- ❖ Double-click the certificate and confirm that:
 - ◆ No errors appear.
 - ◆ The **Issued to** information is correct.
 - ◆ The **Valid dates** are correct.
 - ◆ A message states that a private key corresponds to this certificate.
- ❖ Click the **Certification Path** tab and confirm that the FQDN path is correct and click **OK**.
- ❖ Expand the **Trusted Root Certificate Authorities** node.

- ❖ Click **Certificates**, double-click **Enterprise** and confirm that there is no private key message and click **OK**.
- ❖ Close the MMC.

Install Password Manager using Active Directory as the central store

- ❖ Insert the **Password Manager CD** and in the **Welcome** screen, click **Advanced Installation Tasks**.
- ❖ In the **Advanced Installation Tasks** screen, click **Install Citrix Password Manager Service**.
- ❖ **Citrix Password Manager Service Setup** launches.
- ❖ Click **Next** in the **Welcome** screen.
- ❖ Accept the agreement in the **License Agreement** screen and click **Next**.
- ❖ In the **Select Modules** screen, choose among **Key Management**, **Account Self-Service**, **Provisioning** and **Data Integrity**, and click **Next**.
- ❖ In the **Ready to Install the Application** screen, click **Install**.
- ❖ After installation, click **Finish**.
- ❖ A configuration wizard launches after Password Manager Service installation finishes.
- ❖ Click **Next** in the **Welcome** screen.
- ❖ Verify the correct FQDN is selected in the **Select local SSL certificate** drop-down list.
- ❖ Click **NT Authority\Network Service** from the **System account** drop-down list and click **Next**.
- ❖ In the **Create signing certificate** screen, select the certificate expiration and click **Next**.
- ❖ Click **Active Directory**, click the correct FQDN from the drop-down list and click **Next**.
- ❖ Type your user name in the **User name** field.
- ❖ Type your password in the **Password** field.
- ❖ Type the domain in the **Domain** field and click **Next**.
- ❖ If desired, configure the **Configure data proxy** and click **Next**.
- ❖ For data proxy and self-service authentication, type your user name in the **User name** field and your password in the **Password** field, and click **Next**.
- ❖ Click **Finish**.
- ❖ Click **Finish** in the **Applying Settings** screen.

Install the Password Manager console

- ❖ Insert the **Password Manager CD** and if the **Password Manager Main Menu** doesn't launch, double-click **AUTORUN.EXE** in the **CD** folder.
- ❖ On the **Main Menu**, select **Installation Menu**.
- ❖ On the **Installation Menu**, select **Citrix Password Manager Console**.
- ❖ **Citrix Password Manager Console Setup** launches.
- ❖ Click **Next** in the **Welcome** screen.
- ❖ Accept the agreement in the **License Agreement** screen and click **Next**.
- ❖ Select the components you would like to install.
 - ◆ The choices are **Console**, **Application Definition Tool**, **Citrix Access Suite - Licensing**, and **Citrix Access Suite - Diagnostics**.
- ❖ Click **Next** in the **Install Type** screen.
- ❖ Click **Next** in the **Ready to Install the Application** screen.
- ❖ After installation, click **Finish**.
- ❖ To configure the Password Manager console, open the Access Suite Console.
- ❖ Launch the **Configure and run discovery** wizard from **Common Tasks** of the farm node.
- ❖ Click **Next** in the **Welcome** screen.
- ❖ Click **Next** in the **Select Components** screen.
- ❖ In the **Identify Central Store** page, choose among **Active Directory**, **NTFS Network Share** and **Novell Shared Folder**.
- ❖ Select and configure the appropriate choice and click **Next**.
- ❖ Choose whether or not to configure Data Integrity in the **Configure Data Integrity Options** screen and click **Next**.
 - ◆ Data Integrity must have been chosen upon installation to configure this option.
- ❖ Click **Next** in the **Preview Discover** screen.
- ❖ Click **Finish** when discover is complete.

Create an identity verification question

- ❖ Expand the **Identity Verification** node in the Access Suite Console.
- ❖ Click the **Question-Based Authentication** node.
- ❖ Click **Manage Questions** in **Common Tasks**.
- ❖ The **Manage Questions** window launches.

- ❖ In the left pane of the **Manage Questions** window, select **Security Questions**.
- ❖ Click **Add Question** in the right pane and the **Security Question** window launches.
- ❖ Type the question in the **Security Question** window.
- ❖ Type the number of characters in the **User answer must be at least** field.
- ❖ If desired, check **Answer is case sensitive**.
- ❖ Click **OK** to close the **Security Question** window.

Create a new question group

- ❖ Expand the **Identity Verification** node in the Access Suite Console.
- ❖ Click the **Question-Based Authentication** node.
- ❖ Click **Manage Questions** in **Common Tasks**.
- ❖ The **Manage Questions** window launches.
- ❖ In the left pane of the **Manage Questions** window, select **Security Questions**.
- ❖ Click **Add Group** in the right pane and the **Security Question Group** window launches.
- ❖ Put a check beside the desired questions.
- ❖ Type the number of questions that users are required to answer in the **Number of questions from this group that users are required to answer** field.
- ❖ Click **OK** to close the **Security Question Group** window.

Generate a new questionnaire

- ❖ Expand the **Identity Verification** node in the Access Suite Console.
- ❖ Click the **Question-Based Authentication** node.
- ❖ Click **Manage Questions** in **Common Tasks**.
- ❖ The **Manage Questions** window launches.
- ❖ In the left pane of the **Manage Questions** window, select **Questionnaire**.
- ❖ Click **Add** in the right pane to open the **Add Questions or Question Groups** window
- ❖ Add questions and question groups and click **OK** to close the **Add Questions or Question Groups** window.
- ❖ In the right pane, select a question or question group and click **Move Up**, **Move Down** or **Remove** as desired.
- ❖ Click **Security Questions** in the left pane of the **Manage Questions** window to confirm that new questions are marked **Yes** in the **In Use** column.

Configure key recovery

- ❖ Expand the **Identity Verification** node in the Access Suite Console.
- ❖ Click the **Question-Based Authentication** node.
- ❖ Click **Manage Questions** in **Common Tasks**.
- ❖ The **Manage Questions** window launches.
- ❖ In the left pane of the **Manage Questions** window, select **Key Recovery**.
- ❖ Select the questions and/or question groups that will be used for key recovery.
- ❖ Click **OK** to close the **Manage Questions** screen.
- ❖ Click **Yes** in the **Warning** pop-up window.
 - ◆ By clicking **Yes** in the **Warning** pop-up window, you are causing users to have to re-enroll. Click **No** if you do not want them to re-enroll.

Create a password policy

- ❖ Click **Create a new password policy** in **Common Tasks** in the **Password Policies** node of the Access Suite Console.
- ❖ The **Password Policy Wizard** launches.
- ❖ In the **Name the password policy** screen, type a name and description for the policy and click **Next**.
- ❖ In the **Set basic password rules** screen, configure the syntax rules, which include:
 - ◆ **Alphabet case usage**, **Minimum password length**, **Maximum password length**, **Number of times a single character can be repeated** and **Number of times a character can be repeated sequentially**.
 - ◆ Also in the **Set basic password rules** screen, check **New password must not be the same as previous password** if desired and click **Next**.
- ❖ In the **Set numeric character rules** screen, configure:
 - ◆ Whether to allow numeric characters in a password.
 - ◆ Whether the numeric characters can be the first or last character of the password.
 - ◆ The minimum number of numeric characters required.
 - ◆ The maximum number of numeric characters allowed.
- ❖ In the **Set special character rules** screen, configure:
 - ◆ Whether to allow special characters in a password.
 - ◆ Whether the special characters can be the first or last character of the password.
 - ◆ The minimum number of special characters required.

- ◆ The maximum number of special characters allowed.
- ◆ Also in this screen, type the allowed special characters in the **Allowed special characters list**.
 - The special characters allowed by default are: **!@#\$%^&*()_-+=[]\|,?** Click **Next**.
- ❖ In the **Establish logon preferences** screen, configure whether to allow users to reveal passwords for applications or whether to force users to re-authenticate before submitting application credentials.
 - ◆ Also in the **Establish logon preferences** screen, configure **Number of logon retries** and **Time limit for logon retries** and click **Next**.
- ❖ In the **Set password expiration options** screen, decide whether to use the password expiration settings associated with the application definitions.
 - ◆ If using the password expiration settings associated with the application definitions, configure **Number of days until password expires** and **Number of days to warn users before password expires**.
- ❖ In the **Define Password wizard** screen, choose from the following to select how you want new passwords to be generated and submitted to the application:
 - ◆ **User prompted for action, User-created only, User-created with system-generated option, System-generated, user informed, System-generated with user-created option, or System-generated, silent**. Click **Next**.
- ❖ Confirm the settings and click **Finish**.

Application definitions

An *application definition* stores the identifiers the agent software uses to detect credential submission and password change forms to show where to enter the user's credentials and how to submit those credentials.

Application definitions can be created for Windows, Java, host/mainframe and web applications.

- ❖ On the Create Application Definition screen, there are three choices: Windows, Web and Host/Mainframe.
 - ◆ To create an application definition for a Java application, choose Windows.

Create an application definition

- ❖ Click **Create application definition** in **Common Tasks** in the **Application Definition** node of the Access Suite Console.
- ❖ The **Create Application Definition** window launches.
- ❖ Choose among **Windows, Web** and **Host/Mainframe** for the application type
- ❖ Choose between **Create new** and **Create from an application template**.
- ❖ Click **Start Wizard**.

- ❖ In the **Application Definition Wizard**, in the **Identify application** screen, type a name and description for the application definition and click **Next**.
- ❖ In the **Manage forms** screen, add and configure the application forms the agent software must recognize for submitting and changing user credentials.
- ❖ In the **Manage forms** screen, click **Add Form**.
- ❖ The **Add Form Wizard** launches.
- ❖ In the **Add Form Wizard**:
 - ◆ Identify the form.
 - ◆ Select the field detection method.
 - **Send Keys** or **Control ID**,
 - ◆ Set the field detection rules.
 - ◆ Configure whether the agent automatically submits credentials to the application or not.
 - ◆ Configure class information, control matching and initial delay information in the **Advanced Settings**.
 - ◆ Confirm all choices.
- ❖ Click **Finish** to exit the **Add Form Wizard** and return to the **Application Definition Wizard**.
- ❖ Name the custom fields in the **Name custom field** screen and click **Next**.
- ❖ Use the default icon or specify a custom icon in the **Specify Icon** screen and click **Next**.
- ❖ In the **Password Expiration** screen, choose to run a script when the password expires and you can choose to use the **Citrix Password Manager** expiration warning and click **Next**.
- ❖ Confirm the settings and click **Finish**.

Create a user configuration

- ❖ In the Access Suite Console, click **Add new user configuration** in **Common Tasks** of the **User Configurations** node.
- ❖ The **User Configuration Wizard** launches.
- ❖ Type a name, description and data location for the user in the **Name user configuration** screen and click **Next**.
- ❖ Add application groups in the **Choose policies and applications** screen and click **Next**.
- ❖ Customize how the agent works for this user configuration in the **Configure agent interaction** screen and click **Next**.

- ❖ Set the licensing model and licensing communication for this user configuration in the **Configure licensing** screen and click **Next**.
- ❖ Set the method used to verify the user's identity and to retrieve the key for stored credentials in the **Configure key management** screen and click **Next**.
- ❖ Select self-service features in the **Enable self-service** screen and click **Next**.
- ❖ Provide the service location for the Key Management module in the **Key management module** screen and click **Next**.
- ❖ Provide the service location for the Provisioning module in the **Provisioning module** screen and click **Next**.
- ❖ Confirm the settings in the **Confirm settings** screen and click **Finish**.

Create a Password Manager agent installation image

- ❖ Click **Advanced Installation Tasks** on the **Main Menu** of the **Citrix Password Manager CD**.
- ❖ On the **Advanced Installation Tasks** menu, click **Create Citrix Password Manager Agent Installation Image**.
- ❖ Click **Next** in the **Welcome** screen that launches.
- ❖ Select a network installation point and click **Next**.
- ❖ Select the features that you want to install and click **Next**.
- ❖ Select the type of Central Store and click **Next**.
- ❖ Verify your selections and click **Next** to start the installation.
- ❖ Click **Finish** after the installation is complete.

Enable Self-Service Password Reset on Web Interface

- ❖ Publish **LOGOFF.EXE**, found at **c:\windows\system32**.
- ❖ Create a file for Account Self-Service and save it with a **.ICA** extension.
- ❖ Update the **WEB.CONFIG** file to add the ICA file name to the **<appSettings>** section.
- ❖ Restart the World Wide Web Publishing Service for the changes to the Web Interface configuration file to take affect.
- ❖ Add a URL to the Web Interface site by configuring **Customize appearance for user** in **Common Tasks** of the **Web Interface** node.

Configure password provisioning

Create and edit a provisioning template by clicking **Generate provisioning template** in **Common Tasks** of a user configuration node in the Access Suite Console.

Building and Testing Access Gateway Advanced Edition

Access Gateway Advanced Edition concepts

Access policies use filters to identify when a client device meets the criteria necessary to access resources in an access server farm.

Filters check to see whether a condition is true or not.

Policies control access to all resources in the access server farm by using filters to define the conditions that decide when a policy should be applied.

Resources are the tools available on the network that users employ to help them accomplish tasks.

- ❖ Access Gateway Advanced Edition provides the following types of resources: Web sites, web pages, web applications, portals, published applications, file shares, networks, subnets, servers, services, email and email synchronization.
- ❖ By default, a user cannot access resources until an administrator applies a policy that grants them access permissions through action controls.

Endpoint analysis scans verify whether or not a client device meets the minimum requirements necessary to access the logon page in an access server farm.

- ❖ The endpoint analysis scan is performed before the user sees the logon page.
- ❖ Endpoint analysis scans are specified in logon points and access policies, control access to the logon page, control access to resources, are configured to run only when specific conditions exist on the client device and require the use of an endpoint analysis scan client on the client device.

Install and configure Access Gateway Advanced Edition

- ❖ Insert the **Access Gateway Access Control Option CD**.
- ❖ The **Welcome** screen will launch.
- ❖ In the **Welcome** screen, click **Product Installations**.
- ❖ In the **Product Installations** screen, click **Advanced Access Control**.
- ❖ Click **Next** in the **Welcome** screen.
- ❖ Read the **License Agreement**, click **I accept the license agreement** and click **Next**.
- ❖ Click **Next** to install all components.
- ❖ Click **OK** in the warning message.
- ❖ Click **Next** to begin the installation.
- ❖ Click **OK** in the **Advanced Access Control Installation** dialog box.
- ❖ Verify the selected options are displayed in the **Start Installation** screen and click **Next**.

- ❖ Ensure that **Run Server Configuration** is selected and click **Finish**.
- ❖ The **Advanced Access Control Server Configuration** wizard will launch.
- ❖ Select **Create a new access server farm** and click **Next**.
- ❖ Use administrator credentials for the service account and click **Next**.
- ❖ Choose the database to use (**Microsoft SQL** or **Microsoft SQL Server Database Engine**) and click **Next**.
- ❖ Verify that **I would like to use an existing license server** is selected, type the name of the license server in the **Host name** field and click **Next**.
- ❖ Verify that the correct options are selected and click **Next**.
 - ◆ Choose from **Agent Server**, **Web Server** and **HTML Preview**.
- ❖ Click **Next** to use **C:\INETPUB\WWWROOT** as the default site path.
- ❖ Verify the information in the **Ready to Configure** screen and click **Next**.
- ❖ Click **Finish**.
- ❖ After installation and configuration is finished, run **Discover** in the Access Suite Console.

Access Suite Console 4.2 update

- ❖ Run **ASC400W004.MSP** to install the Access Suite Console 4.2 update.
 - ◆ Must be done along with version 4.2 of Web Interface and Advanced Gateway with Advanced Access Control.
 - ◆ For more information, see Citrix Knowledge Base article CTX108237.

Specify a Presentation Server farm

- ❖ In the Access Suite Console, click the **CitrixAAC** node and click **Edit farm properties** in **Common Tasks**.
- ❖ Click **Presentation Server Farms** in the properties window.
- ❖ Click **New**.
- ❖ Type the server farm name in the **Citrix Presentation Server farm name** field and click **Next**.
- ❖ Click **Add** to add a farm server.
- ❖ Type the farm server's name and click **OK**.
- ❖ Click **Next**.
- ❖ Click **Finish** in the **Configure Address Mode** screen.
- ❖ Click **OK**.

Configure event logging

- ❖ In the **CitrixAAC** node of the Access Suite Console, click **Edit farm properties** in **Common Tasks**.
- ❖ Click **Event Logging**.
- ❖ Select the type of logging desired and click **OK**.

Create a Web Interface site

- ❖ In the Access Suite Console, expand **Suite Components > Configuration Tools** and click **Web Interface**.
- ❖ Click **Create site** in **Common Tasks**.
- ❖ The **Create Site** wizard launches.
- ❖ Click **MetaFrame Presentation Server** and click **Next**.
- ❖ Specify the IIS location and click **Next**.
- ❖ Specify the server farm and click **Next**.
- ❖ Confirm the information and click **Next**.
- ❖ After the new site is created, click **Finish**.

Create a resource

- ❖ To create a resource for access through Access Gateway Advanced Edition, expand the **CitrixAAC** node in the Access Suite Console.
- ❖ Expand the **Resources** node and click the desired resource node under the **Resources** node.
- ❖ Click the link in **Common Tasks** to create the resource using the wizard.

Create a web resource

- ❖ Open the Access Suite Console.
- ❖ Expand the **Resources** node under the **CitrixAAC** node.
- ❖ Click the **Web Resources** node.
- ❖ Click **Create Web resource** in **Common Tasks**.
- ❖ The **New Web Resource** wizard launches.
- ❖ In the **Name** screen, type the name of the web resource in the **Name** field and a description in the **Description** field and click **Next**.

- ❖ In the **Configure Addresses** screen, specify the URL addresses and authentication type to include by clicking the **New** button and adding the URL addresses and choosing the authentication type.
 - ◆ Authentication types are **Basic, Digest authentication** or **Integrated Windows authentication**.
- ❖ Also configurable on the **Configure Addresses** screen:
 - ◆ **Publish for users in their list of resources**
 - ◆ **Bypass Web Proxy URL rewriting**
 - ◆ **Use the interface that is common for all browser types**
- ❖ Click **Next**.
- ❖ In the **Add Policy** screen, choose either:
 - ◆ **Create a default policy granting access to all users**
 - Or
 - ◆ **I will create a policy to grant access later**
- ❖ Click **Finish**.

Web resource application types

When configuring a new web resource, in the **New URL** pop-up screen, choose **Citrix Web Interface 4.2 or later, Share Point, Share Point with Web Interface Web Part, Web Application** or **Web Application (requires session cookies)** in the **Application Type** drop-down list.

Create a file share resource

- ❖ Expand the **Resources** node in the Access Suite Console, click the **File Shares** node under the **Resources** node and click **Create file share** in **Common Tasks**.
- ❖ The **New File Share** wizard launches.
- ❖ In the **Define File Share** screen, type the name of the file share name, type a description if desired and click **Next**.
- ❖ In the **Configure Share Locations** screen, click **New**.
- ❖ The **File Share** pop-up window launches.
- ❖ In the **File Share** pop-up window, type the display name and type the file share location.
- ❖ Select **Publish for users in their list of published resources** if desired and click **OK** to close the **File Share** pop-up window.
- ❖ Click **Next** in the **Configure Share Locations** screen.

- ❖ In the **Add Policy** screen, select either **Create a default policy granting access to all users** or **I will create a policy to grant access later** and click **Finish**.

Create a default logon point

- ❖ Expand the **CitrixAAC** node in the Access Suite Console and expand the **Logon Point** node.
- ❖ Click the **SampleLogonPoint** node and click **Edit logon point** in **Common Tasks**.
- ❖ Click **Presentation Server Farms** in the left pane of **Logon Point Properties**.
- ❖ Add the appropriate server farm and click **OK**.

Configure the default logon point

- ❖ In the Access Suite Console, under the **CitrixAAC** node, expand the **Logon Points** node and click the **SampleLogonPoint** node.
- ❖ Click **Presentation Server Farms**.
- ❖ Select the desired Presentation Server Farm and click **Add**.
- ❖ Click **OK**.

Delete the default logon point policy

- ❖ Expand the **CitrixAAC** node in the Access Suite Console and click the **Policies** node.
- ❖ Right-click **Default Logon Policy for: SampleLogonPoint** in the right pane and choose **Delete policy**.
- ❖ Click **Yes**.

Managing access and connection policies

You may edit, delete, copy or refresh the access and connection policies in the **Policy** node by right-clicking on them.

Create an access policy

- ❖ Click the **Policies** node in the Access Suite Console.
- ❖ Click **Create access policy** in **Common Tasks**.
- ❖ The **New Access Policy Wizard** launches.
- ❖ In the **Define Policy** screen, type the policy name and description and click **Next**.
- ❖ In the **Select Resources** screen, select the resources for which this policy applies and click **Next**.
- ❖ In the **Configure Settings** screen, configure access settings for each resource type.

- ◆ Right-click on each setting to enable, disable, allow or deny the setting.
- ❖ In the **Select Filter** screen, select from the available filters in the drop-down list or create a new one by clicking **New**.
- ❖ If you click **New** to create a filter, the **New Filter** wizard launches.
- ❖ In the **Define Filter** screen, type the filter name and description, and click **Next**.
- ❖ In the **Choose Filter Type** screen, select **Create a typical filter** or **Create a custom filter** and click **Next**.
- ❖ In the **Select Logon Points** screen, select logon points and click **Next**.
- ❖ In the **Select Authentication Strength** screen, select authentication strength and click **Next**.
 - ◆ Choose among **Do not filter by authentication**, **Windows authentication**, **Windows authentication with advanced authentication**, **RSA or SafeWord**, **RADIUS authentication profile** or **LDAP authentication profile**.
- ❖ Click **Next** in the **Select Endpoint Analysis Outputs** screen.
- ❖ Set the client certificate requirements in the **Set Client Certificate Requirements** screen and click **Finish** to close the **New Filter** wizard.
- ❖ Click **Next** in the **Select Filter** screen in the **New Access Policy Wizard**.
- ❖ In the **Select Users** screen, select the users to apply this policy to and click **Finish**.

Create a connection policy

- ❖ Click the **Policies** node in the Access Suite Console.
- ❖ Click **Create connection policy** in **Common Tasks**.
- ❖ The **New Connection Policy Wizard** launches.
- ❖ In the **Define Policy** screen, type the policy name and description and click **Next**.
- ❖ Configure the connection policies to be enforced in the **Configure Settings** screen.
- ❖ Assign a unique IP address alias to each client device in the **Define IP Pool** screen.
- ❖ In the **Select Filter** screen, select from the available filters in the drop-down list or create a new one by clicking **New**.
- ❖ If you click **New** to create a filter, the **New Filter** wizard launches.
- ❖ In the **Define Filter** screen, type the filter name and description, and click **Next**.
- ❖ In the **Choose Filter Type** screen, select **Create a typical filter** or **Create a custom filter** and click **Next**.
- ❖ In the **Select Logon Points** screen, select logon points and click **Next**.
- ❖ In the **Select Authentication Strength** screen, select authentication strength and click **Next**.

- ◆ Choose among **Do not filter by authentication, Windows authentication, Windows authentication with advanced authentication, RSA or SafeWord, RADIUS authentication profile** or **LDAP authentication profile**.
- ❖ Click **Next** in the **Select Endpoint Analysis Outputs** screen.
- ❖ Set the client certificate requirements in the **Set Client Certificate Requirements** screen and click **Finish** to close the **New Filter** wizard.
- ❖ Back in the **Select Filter** screen, select from the available continuous scan filters in the **Continuous scan filter** drop-down list or create a new one by clicking **New**.
- ❖ Click **New** to create a continuous scan filter and the **New Continuous Scan Filter** wizard launches.
- ❖ In the **Configure Requirements** screen, combine the expressions **AND, OR, and NOT** to create requirements.
- ❖ Click **Finish** to close the **New Continuous Scan Filter**.
- ❖ Click **Next** in the **Select Filter** screen in the **New Access Policy Wizard**.
- ❖ In the **Select Users or Groups** screen, select the users or groups to apply this policy to and click **Finish**.

Create an endpoint analysis scan

- ❖ Expand the **CitrixAAC** node, expand the **Endpoint Analysis** node, expand the desired scan group node below the **Endpoint Analysis** node and click the desired scan package below the scan group node.
 - ◆ The scan groups below the **Endpoint Analysis** node include: **Antivirus, Browser, Custom, Firewall, Machine Identification, Miscellaneous** and **Operating System**.
- ❖ Click **Create scan** in **Common Tasks**.
- ❖ The **Create Scan** wizard launches.
- ❖ In the **Define Scan Name** screen, type a name for the scan and click **Next**.
- ❖ In the **Select Conditions** screen, select the conditions of the scan (**Client Device Regional Locale** and/or **Logon Point**) and click **Next**.
- ❖ In the **Define Rule** screen, type the rule name and click **Next**.
- ❖ In the **Configure Conditions - Operating System** screen, select the operating systems that the scan package will scan and click **Next**.
- ❖ If **Client Device Regional Locale** was selected earlier, in the **Configure Conditions - Client Device Regional Locale** screen, choose the languages to use and click **Next**.
- ❖ In the **Configure Conditions - Logon Point** screen, select the logon point and click **Next**.
- ❖ In the **Define Property to Verify** screen, enter the property values that the scan will check on the client device and click **Finish**.

Use a data set in an endpoint analysis scan

To use a data set, such as MAC addresses, in an endpoint analysis scan, add the data to a file in comma-separated form and save the data as a CSV file. The file can then be chosen while creating an endpoint analysis scan.

Default endpoint analysis scan groups

In the Access Suite Console, under the **CitrixAAC** node, expand the **Endpoint Analysis Scan** node and you will see the default scan groups: **Antivirus, Browser, Custom, Firewall, Machine Identification, Miscellaneous** and **Operating System**.

Configure a new logon point

- ❖ Click the **Logon Points** node under the **CitrixAAC** node in the Access Suite Console.
- ❖ Click **Create logon point** in **Common Tasks**.
- ❖ The **New Logon Point Wizard** launches.
- ❖ The **New Logon Point Wizard** contains 10 steps to configure a new logon point.
 - ◆ The steps, in order, are: **Define Logon Point, Select Home Page, Configure Authentication Strength, Configure Group Authorization, Add Citrix Presentation Server Farms, Select Sound and Window Settings, Configure Workspace Control, Configure Clients, Select Session Settings** and **Visibility**.

Deploy a logon point

- ❖ Click **Start > All Programs > Citrix > Access Gateway > Server Configuration**.
- ❖ The **Advanced Access Control Configuration** console launches.
- ❖ Click **Configured Logon Points** in the left pane and select the desired logon point on the right.
- ❖ Click **Deploy**.
- ❖ Click **OK** to close the **Advanced Access Control Configuration** screen.

URL to access a logon point inside a secure network

- ❖ **http://<Access Gateway Advanced Edition Server Name>/citrixlogonpoint/<Logon Point Name>**
 - ◆ Replace **<Access Gateway Advanced Edition Server Name>** with the NetBIOS name of the Access Gateway Advanced Edition Server.
 - ◆ Replace **<Logon Point Name>** with the name of the logon point.
 - For example, a logon point named SalesPortal on a server named AGServer01 would utilize the URL **http://AGServer01/citrixlogonpoint/SalesPortal**.

Add an endpoint analysis scan to a logon point

- ❖ In the Access Suite Console, expand the **CitrixAAC** node, expand the **Logon Points** node and click on the desired logon point under the **Logon Points** node.
- ❖ Click **Edit logon point** in **Common Tasks**.
- ❖ The **Logon Point Properties** window launches.
- ❖ Select **Visibility** in the left pane.
- ❖ Click **Endpoint Analysis Output**.
- ❖ The **Select an Endpoint analysis** window launches.
- ❖ Select the desired endpoint analysis in the window and click **OK** to close the **Select an Endpoint analysis** window.
- ❖ Click **OK** to close the **Logon Point Properties** window.

Use a filter to grant access to a published application

- ❖ Expand the **Applications** node in the Presentation Server Console.
- ❖ Right-click the desired published application and select **Properties**.
- ❖ In the published application's properties screen, select **Access Control**.
- ❖ Select **Any connection that meets any of the following filters**.
- ❖ Click **Add**.
- ❖ The **Add MetaFrame Secure Access Manager Filter** pop-up window launches.
- ❖ Type or select the name of the MetaFrame Secure Access Manager farm.
- ❖ Type or select the name of the MetaFrame Secure Access Manager filter and click **OK**.
- ❖ Click **OK** in the published application's properties screen.
- ❖ Click **OK** in the **XML Trust Warning** message.

Apply a Presentation Server policy using an access control filter

- ❖ In the Presentation Server Console, click the **Policies** node.
- ❖ Right-click the desired policy in the right pane and select **Apply this policy to**.
- ❖ The **Policy Filters** window launches.
- ❖ Click **Access Control**.
- ❖ Select **Filter based on Access Control**.
- ❖ Select **Apply to connections made through MetaFrame Secure Access Manager**.

- ❖ Click **Any connection that meets any of the following filters**.
- ❖ Click **Add**.
- ❖ The **Add MetaFrame Secure Access Manager Filter** pop-up window launches.
- ❖ Select the MetaFrame Secure Access Manager farm from the drop-down list.
- ❖ Select the MetaFrame Secure Access Manager Filter from the drop-down list and click **OK**.
- ❖ Click **OK** in the **Policy Filters** window.
- ❖ Click **OK** in the **XML Trust Warning** message.