Citrix® Password Manager
Supplement to the Administrator's Guide

.

Citrix Password Manager

Citrix Password Manager™ 4.1
Citrix Access Suite™

Document Code: March 2, 2006 (LBL)

Contents

Chapter 1 Welcome

Getting More Information and Help 5
- Product Documentation 5
- Accessing Documentation 6
- Document Conventions 7
- Getting Service and Support 7
- Subscription Advantage 8
- Citrix Developer Network 8
- Education and Training 9
- About this Document 9
- Audience and Assumptions 9
- Providing Feedback about this Document 9

New Features in this Release 10

Chapter 2 Installing Service Pack 1

- Step 1—Update the Password Manager Service 12
- Step 2—Update the Password Manager Console 12
- Step 3—Update the Agent Software 13

Chapter 3 Configuring Features in Service Pack 1

Resetting Your Users' Password Data 16
Allowing Users to Reregister Answers to Their Security Questions 17
Securing the Path to Applications in Your Environment. 18
Increasing Password Strength. 19
Excluding Specific Characters 19
Allowing Specific Types of Characters 20
Preventing Password Reuse 21
Testing Your Password Policies. 22
Preventing Application Logon Loops 22
Designating Domain Controllers for Users and User Groups 23

Chapter 4 Documentation Errata

Password Sharing Groups 25
Agent Software 25
Uninstalling Password Manager 27
Hot Desktop. 27
Managing User Data 27

CHAPTER 1

Welcome

Citrix Password Manager provides password security and single sign-on access to Windows, Web, and host-based applications. Users authenticate once with a single password and Password Manager authenticates the users to all other password-protected applications—providing one, easy-to-remember, secure way to log on everywhere. This guide is a supplement to the main documenation provided for Password Manager, covering the features and enhancments available with Service Pack 1 for Password Manager 4.1.

This chapter provides:

- A list of all Password Manager documentation available with brief descriptions of each document
- A comprehensive list of online resources for Password Manager and Citrix
- Getting more information and help
- Information about this document
- New features in this release

Getting More Information and Help

This section describes how to get more information about Password Manager.

Product Documentation

The documentation for Password Manager includes online guides, known issues information, and online help.

- Online guides are provided as Adobe Portable Document Format (PDF) files. To view, search, and print the PDF documentation, you need to have Adobe Acrobat Reader 5.0.5 with Search, or Adobe Reader 6.0 through 7.0. You can download these products for free from Adobe Systems' Web site at http://www.adobe.com/.
- Be sure to read the readme files and the installation checklist before you install Password Manager or when troubleshooting. These files contain

important information that includes last-minute documentation updates and corrections.

- Online help is available in many components. You can access the online help from the Help menu or Help button.

Accessing Documentation

The documentation for Password Manager is available in the Documentation directory on the product CD and for download on Citrix's Web site: http://www.citrix.com.

The following documentation is included with Password Manager:

- The Readme file provides the latest information about Password Manager functionality, known issues, and documentation changes. Be sure to read this document for important information before you install Password Manager.
- This manual, the *Supplement to the Password Manager Administrator's Guide*, provides conceptual information, procedures for update and implementation for system administrators who install, configure, and test the components of Password Manager 4.1, Service Pack 1.
- The *Password Manager Administrator's Guide*, available from the Product Documentation section of the Knowledge Base on the Citrix Web site, provides conceptual information, procedures for deployment, and implementation for system administrators who install, configure, and test the components of Password Manager.
- Online, context-sensitive help is available for administrators and users of Password Manager. Administrators can view information about common tasks, workflow, and settings on screen or by accessing specialized help topics. Users can get information about common tasks, including creating logons for applications, using the Logon Manager, and setting Password Manager automatic features.View this help by clicking the Help buttons, or selecting help options from product menus.

Note If you are new to Password Manager, read the *Password Manager Evaluator's Guide* for instructions about setting up and running a small-scale deployment of the product. This guide provides you with a practical overview of Password Manager features and functionality.

Document Conventions

Documentation for Citrix products uses the following typographic conventions for menus, commands, keyboard keys, and items in the program interface:

Convention	Meaning
Boldface	Commands, names of interface items such as text boxes, option buttons, and user input.
Italics	Placeholders for information or parameters that you provide. For example, *filename* in a procedure means you type the actual name of a file. Italics are also used for new terms and the titles of books.
%SystemRoot%	The Windows system directory, which can be WTSRV, WINNT, WINDOWS, or any other name you specify when you install Windows.
`Monospace`	Text displayed in a text file.
{ braces }	A series of items, one of which is required in command statements. For example, **{ yes | no }** means you must type **yes** or **no**. Do not type the braces themselves.
[brackets]	Optional items in command statements. For example, **[/ping]** means that you can type **/ping** with the command. Do not type the brackets themselves.
| (vertical bar)	A separator between items in braces or brackets in command statements. For example, **{ /hold | /release | /delete }** means you type **/hold** or **/release** or **/delete**.
… (ellipsis)	You can repeat the previous item or items in command statements. For example, **/route:***devicename***[,…]** means you can type additional *devicenames* separated by commas.

Getting Service and Support

Citrix provides technical support primarily through the Citrix Solution Advisor program. Contact your supplier for first-line support or check for your nearest Solution Advisor at http://www.citrix.com/site/partners.

In addition to the Citrix Solution Advisor program, Citrix offers a variety of self-service, Web-based technical support tools from its Knowledge Center at http://support.citrix.com/. Knowledge Center features include:

- A knowledge base containing thousands of technical solutions to support your Citrix environment.
- An online product documentation library.
- Interactive support forums for every Citrix product.
- Access to the latest hotfixes and rollup packs.
- Security bulletins.
- Online problem reporting and tracking (for users with valid support contracts).
- Citrix Live Remote Assistance. Using Citrix's remote assistance product, GoToAssist, a member of our support team can view your desktop and share control of your mouse and keyboard to get you on your way to a solution.

Another source of support, Citrix Preferred Support Services, provides a range of options that allows you to customize the level and type of support for your organization's Citrix products.

Subscription Advantage

Subscription Advantage gives you an easy way to stay current with the latest server-based software functionality and information. Not only do you get automatic delivery of feature releases, software upgrades, enhancements, and maintenance releases that become available during the term of your subscription, you also get priority access to important Citrix technology information.

You can find more information on the Citrix Web site at http://www.citrix.com/services/ (select Subscription Advantage). You can also contact your Citrix sales representative or a member of the Citrix Solution Advisor program for more information.

Citrix Developer Network

The Citrix Developer Network (CDN) is at http://www.citrix.com/cdn/. This open-enrollment membership program provides access to developer toolkits, technical information, and test programs for software and hardware vendors, system integrators, ICA licenses, and corporate IT developers who incorporate Citrix computing solutions into their products.

Education and Training

Citrix offers a variety of instructor-led training and Web-based training solutions. Instructor-led courses are offered through Citrix Authorized Learning Centers (CALCs). CALCs provide high-quality classroom learning using professional courseware developed by Citrix. Many of these courses lead to certification.

Web-based training courses are available through CALCs, resellers, and from the Citrix Web site.

Information about programs and courseware for Citrix training and certification is available from http://www.citrix.com/edu/.

About this Document

The overall objectives of this supplemental guide are:

- To provide you with a good understanding of the features and functionality of Service Pack 1 for Password Manager 4.1
- To provide you with guidelines for deploying and implementing Service Pack 1 for Password Manager 4.1 in your organization

Audience and Assumptions

This document is intended for use by system and security administrators who are implementing Password Manager. It is assumed that you, the reader, have an administrator-level understanding of Windows.You must have working knowledge of Novell NetWare if this is the platform you are using to install or maintain Password Manager.

Providing Feedback about this Document

To provide feedback about the documentation, go to www.citrix.com and click **Support > Knowledge Center > Product Documentation**. To access the feedback form, click the Submit Documentation Feedback link.

New Features in this Release

Password Manager 4.1, Service Pack 1 includes the following new features:

Reset User Data. Should users forget the answers to their security questions, or need to be released from an invalid state, use the Password Manager Console to reset their credential data quickly and easily using the Password Manager console.

Application identification security. Application definitions can now specify the full path of the application to be recognized by Password Manager. This prevents the submission of credential information stored by Password Manager to an unauthorized version of an application.

Password policy enhancements. Improvements and enhancements to the way you define password polices make it easier for you to define and test your password policies for use within your organization. Limit or require the use of specific characters or groups of characters for more secure password requirements.

User reenrollment. This feature allows your users to reregister answers to their security questions and create a new secure key to protect their password data. Users can start the Security Questions Registration wizard from within the agent software, and can quickly and securely submit new answers to their security questions without intervention of an administrator.

Log on and log off detection. Application definitions are enhanced to recognize and treat requests for credentials intelligently. A user who logs off from an application and is returned to the logon screen will not be logged back on to the application automatically.

Improved Active Directory functionality. You can now bind individual users and user groups to specific Domain Controllers within your Active Directory environment. This allows you to eliminate synchronization delays because of Active Directory replication that occurs in environments where users access Password Manager in multiple Active Directory sites simultaneously.

CHAPTER 2

Installing Service Pack 1

Service Pack 1 for Password Manager 4.1 can be installed only after you install Password Manager 4.1. For more information about installing or upgrading to Password Manager 4.1, see the *Password Manager Adminstrator's Guide*.

Installing Service Pack 1

To update your Password Manager 4.1 environment to Service Pack 1 for Password Manager 4.1, follow these steps and update each system component in the following order:

Step 1—Update the Password Manager Service (if applicable). If your Password Manager 4.1 environment includes the Data Integrity feature, Self-Service features, or Automatic Key Recovery, you use the Password Manager Service and therefore must update the service first.

Step 2—Update the Password Manager Console.

Step 3—Update the Password Manager Agent software.

Step 1—Update the Password Manager Service

If your environment uses the Password Manager service, you must select all modules you are using when you update the service. You must provide service-configuration information, such as settings, service account user name and password, and the location of your central store as part of the update process.

Note If you are not using the Password Manager service in your Password Manager 4.1 environment, you need to update only the console and agent software.

To update the Password Manager service

1. Copy the hotfix package to an empty folder on the hard drive of the server you want to update.
2. Close all applications.
3. Run the executable file.
4. Shut down and restart the server.
5. When the installation wizard is finished, the Service Configuration Wizard may open. Provide the information needed to configure the service, such as connection settings, certificate name, service user account name and password, and the location of your central store.
6. Close any open screens and verify the service is running.

Step 2—Update the Password Manager Console

The console you use to manage your Password Manager 4.1 environment is removed when you install the console provided with Service Pack 1 for Password Manager 4.1. For best results, update all installed consoles and the Application Definition Tool.

To update the Password Manager Console

1. Copy the hotfix package to an empty folder on the hard drive of the server you want to update.
2. Close all applications.
3. Run the executable file.
4. Shut down and restart the server.

Step 3—Update the Agent Software

The agent software provided with Password Manager 4.1 provides basic functionality to users connecting to an updated central store. You can delay agent updates if necessary; however, to realize the full functionality of Service Pack 1 for Password Manager 4.1, you must update the agent software deployed in your environment.

To update the agent software

1. Copy the compressed hotfix package to an empty folder on the local computer.
2. Extract the contents of the hotfix package.
3. Close all applications.
4. Run AgentSetup.exe.
5. When prompted, restart the computer. The agent software will not update properly until the computer is restarted.

CHAPTER 3

Configuring Features in Service Pack 1

This chapter describes the new features and enhancements included in Service Pack 1 for Password Manager 4.1, and explains how to implement these features in your environment. It assumes that you installed both Password Manager 4.1 and Service Pack 1 for Password Manager 4.1, and are familiar with user data, creating application definitions, creating password policies, and creating user groups.

For more information about installing Service Pack 1 for Password Manager 4.1, see the installation chapter of this guide. For more information about using Password Manager, see the *Administrator's Guide for Password Manager 4.1*.

The topics covered in this chapter include:

- Resetting Your Users' Password Data
- Allowing Users to Reregister Answers to Their Security Questions
- Securing the Path to Applications in Your Environment
- Increasing Password Strength
- Preventing Password Reuse
- Testing Your Password Policies
- Preventing Application Logon Loops
- Designating Domain Controllers for Users and User Groups

Resetting Your Users' Password Data

Password Manager 4.1 introduced credential provisioning to Password Manager environments. This allows you to create an XML file that you use to import credential information, or delete, add, and reset user information.

Service Pack 1 expands that functionality by allowing you to easily reset an individual user's data using the Password Manager Console. Should users forget the answers to their security questions or need to be released from an invalid state, use the console to reset their credential data.

The option to reset a user's data using the console is available only in environments where provisioning is enabled. Additionally, a user's data will not be reset unless the selected user logs on to Password Manager using agent software provided with Password Manager 4.1 or later..

Important Password history is retained on a per-user basis. If you reset the user data for a user, the password history is removed and password history cannot be enforced for the deleted passwords.

To reset a user's data

1. Select the **User Configurations** node in the Password Manager Console.
2. From the **Action** menu, select **Reset user data** from the **All Tasks** menu.
3. The **Reset User Data** wizard opens, displaying the users active in your environment.
4. Expand the nodes and select the user whose data you want to reset.
5. Click **Reset**.
6. Verify that any users who may be running Password Manager as an application hosted by Citrix Presentation Server are logged off and click **Continue** to flag the user's data for reset.

7. A dialog box appears when the user's information is verified; click **OK** to close the dialog box when the process registers success or failure.
8. The user's data is reset the next time the user logs on to Password Manager using agent software provided with Password Manager 4.1 or later.

Note Previous releases of Password Manager kept user data for 30 days when the data was marked for deletion. Any user data marked for deletion in an environment running Service Pack 1 will be kept in the central store for 180 days. If a user connects to Password Manager before the 180 day time period expires, any credentials stored locally will be deleted.

Allowing Users to Reregister Answers to Their Security Questions

Password Manager 4.1 introduced several self-service features designed to give users more control over their accounts and reduce the need for administrator and help desk assistance. Service Pack 1 extends these self-service options, allowing your users to reregister answers to their security questions at any time without intervention of an administrator.

If your environment includes security questions or account self-service features, users who register security questions and answers can use the agent software supplied with Service Pack 1 to provide new answers to their available security questions.

Users can select **Security Questions Registration** from the **Tools** menu in Logon Manager or from the shortcut menu associated with the notification icon for the agent software. Selecting this option starts the Security Questions Registration wizard; from there users can reregister answers to their security questions. Once users successfully provide their answers and receive confirmation that the new answers are saved to the central store, their old answers are no longer valid.

This feature is available only to users connecting to Password Manager using the agent software provided with Service Pack 1 and who previously registered answers to their security questions.

Securing the Path to Applications in Your Environment

You can specify the exact, secure path to applications using Service Pack 1. Securing the paths to application executables prevents rogue attackers from using unauthorized applications to gain access to user name and password data users store within Password Manager.

To allow users to access and submit credential information for a specific version of an application within your environment, simply add the secure path or paths to the application to your application definition. If users launch the application from a different path, Password Manager does not submit the credential information.

Additionally, you can add or change the paths to authorized applications at any time by editing the application definition in the Password Manager Console.

To add or edit a secure path to an application

1. Click to select an application definition in the left pane of the Password Manager Console.
2. From the **Action** menu, select **Edit application definition**.
3. The **Edit Application Definition** wizard appears. Select **Application Forms** from the options on the left of the wizard screen.
4. Click to select a defined application form, then click **Edit**.
5. The **Edit Application Form** wizard appears. Select **Form Identity** from the options on the left of the wizard screen.
6. Click to select the application listed under **Executable file names and paths**, then click **Edit** to add a secure path for this application.
7. In the window that opens, enter absolute paths, such as **D:\application** or paths with variables, such as **%system root%\application**. Separate multiple paths using semicolons.
8. Click **OK** until all windows are closed and save your changes to the central store.

Application definitions that include secure path information can be used to create an application definition template; however, the secure path is not included as part of the template.

Note To provide secure paths for applications installed on servers or client devices running 64-bit operating systems, you can use the variable **%programfiles%** in your secure application path. Client devices or servers running Windows NT 4.0 may need the absolute path **C:\program files** explicitly defined.

Increasing Password Strength

Password Manager allows you to define the rules for creating and managing passwords used within your environment. You can further design password policies to meet various system and business requirements, such as limiting or requiring the use of specific characters or groups of characters for more secure password requirements.

Excluding Specific Characters

Service Pack 1 allows you to customize an exclusion list for all password policies. You can prevent specific characters or groups of characters from being used in your passwords, such as common words or easily-guessed sequential groups of characters, such as **abc123**, or **asdfjkl**. Additionally, you can prevent the use of passwords that include all or part of Windows and individual application user names.

You can specify up to 256 different groups of characters to be excluded; each group of characters can be up to 32 characters long. The characters within the groups are case-insensitive; an exclusion list that includes **abcdefg** also prevents the use of **AbCDefG** in a password. Additionally, an exclusion list that includes a group of characters such as **defg** also prevents the group of characters **abcdefg** from use.

To create custom exclusion lists for existing password policies

1. Select a password policy in the left pane of the Password Manager Console.
2. From the **Action** menu, select **Edit password policy**.
3. The **Edit Password Policy** wizard opens. Select **Exclusion Rules** from the options on the left of the wizard screen.
4. Click **Edit List** then enter the characters or groups of characters you want to exclude from passwords.
5. Enter characters or groups of characters in the field provided, or copy and paste a list from any standard text editor. Separate individual entries by pressing the **Enter** key.
6. Click **OK** to save your changes and close the exclusion list editor.

   Optionally, you can choose to exclude all or part of user names by selecting **Do not allow application user name in password** or **Do not allow Windows user name in password**.
7. Click **OK** to save your changes.

Allowing Specific Types of Characters

You can define the use of uppercase and lowercase characters for users' passwords. Additionally, you can require the use of specific types of characters, as well as allow or disallow their use at the start or end of passwords.

To allow the use of uppercase and lowercase characters in password policies

1. Select a password policy in the left pane of the Password Manager Console.
2. From the **Action** menu, select **Edit password policy**.
3. The **Edit Password Policy** wizard opens. Select **Alphabetic Character Rules** from the options on the left of the wizard screen.
4. Select the uppercase and lowercase character rules for use in this policy.

   Optionally, define the minimum number of uppercase and lowercase characters required by this policy.
5. Click **OK** to save your changes.

To allow the use of numeric characters in password policies

1. Select a password policy in the left pane of the Password Manager Console.
2. From the **Action** menu, select **Edit password policy**.
3. The **Edit Password Policy** wizard opens. Select **Numeric Character Rules** from the options on the left of the wizard screen.
4. Select the numeric rules for use in this policy.

   Optionally, define the minimum and maximum number of numeric characters allowed by this policy.
5. Click **OK** to save your changes.

To allow the use of numeric characters in password policies

1. Select a password policy in the left pane of the Password Manager Console.
2. From the **Action** menu, select **Edit password policy**.
3. The **Edit Password Policy** wizard opens. Select **Special Character Rules** from the options on the left of the wizard screen.

4. Select the special character rules for use in this policy.

   Optionally, define the minimum and maximum number of uppercase and lowercase letters allowed by this policy.

5. Define the special characters allowed for use with this policy.

6. Click **OK** to save your changes.

Preventing Password Reuse

Service Pack 1 allows you to enforce the use of new passwords when older passwords expire. When creating or updating a password policy, you can optionally prevent users from reusing up to 24 passwords previously used within your Password Manager environment. The password history is maintained for each application managed by Password Manager.

To edit a password policy to prevent password reuse

1. Select a password policy in the left pane of the Password Manager Console.

2. From the **Action** menu, select **Edit password policy**. The **Edit Password Policy** wizard opens.

3. Select **Password History and Expiration** from the options on the left of the wizard screen.

4. Click to select **New password must not be the same as previous passwords**.

5. Define the number of passwords Password Manager retains for password comparison; you can select between one and 24 passwords.

6. Click **OK** to save your changes.

This feature is available to all users running the agent software included with Service Pack 1. After this option is applied to an application or application group, any password changes made after the policy is active is retained in the user's password history. Password changes made before the policy is active are not retained or used to prevent password reuse.

Important Password history is retained on a per-user basis. If you reset the user data for a user, the password history is removed and password history cannot be enforced for the deleted passwords.

Testing Your Password Policies

Service Pack 1 allows you to test your policies before rolling them out in your environment so that you can be sure they work as intended, and that a reasonable pool of passwords is available to your users.

Using the **Test Password Policy** page, you can manually test a single password, have Password Manager generate a single password policy-compliant password, or generate a list of passwords that meet the settings you defined for this password policy.

To test a password policy

1. Select a password policy in the left pane of the Password Manager Console.
2. From the **Action** menu, select **Edit password policy**.
3. The **Edit Password Policy** wizard opens. Select **Test Password Policy** from the options on the left of the wizard screen.
4. Use any of the three available password test options to test your password policy.
5. Click **OK** to close the **Edit Password Policy** wizard.

Preventing Application Logon Loops

Service Pack 1 includes several agent software enhancements that prevent credential submission or credential change loops. Using the Password Manager Console provided with Service Pack 1, you can create a new application definition or modify an existing application definition to prevent applications from causing such loops.

Credential submission loops. If users log off from an application and are returned to a logon screen, the agent software prompts the users to choose to log on again or to ignore the logon form. Closing the application terminates the session; Password Manager submits the credentials the next time the application is opened.

Credential change loops. Users who attempt to change their passwords multiple times while accessing a specified application are asked to verify subsequent password changes.

Edit an application definition to prevent an application log on loop

1. Select an application definition in the left pane of the Password Manager Console.
2. From the **Action** menu, select **Edit application definition**. The **Edit Application Definition** wizard appears.
3. Select **Advanced Detection** from the options on the left of the wizard screen.
4. Select **Process only the first logon for this application**.
5. Click **OK**.

Edit an application definition to prevent multiple password changes in a single session

1. Select an application definition in the left pane of the Password Manager Console.
2. From the **Action** menu, select **Edit application definition**.
3. The **Edit Application Definition** wizard appears. Select **Advanced Detection** from the options on the left of the wizard screen.
4. Select **Process only the first password change for this application**.
5. Click **OK**

Designating Domain Controllers for Users and User Groups

Service Pack 1 allows you to designate the domain controllers your users and user groups can bind to within your Active Directory environment.This allows you to eliminate synchronization delays because of Active Directory replication that occurs in environments where users access Password Manager in multiple Active Directory sites simultaneously.

When you create a user configuration, you can select a domain controller from a list of available domain controllers; for example, you can require users be bound to a domain controller within their physical location. After you have specified a domain controller, users are bound to that domain controller the next time they log on to Password Manager.

By default, users bind to any writeable domain controller until you select a domain controller they must bind to. You can change the domain controller setting at any time by updating the user configuration as needed while maintaining the integrity of user data.

Note When choosing a domain controller for binding, verify that the resources available on the domain controller can accept the communication traffic users generate when connecting to the domain controller during peak operational times.

Specifying a domain controller for an existing user configuration

1. Select a user configuration in the left pane of the Password Manager Console.
2. From the **Action** menu, select **Edit user configuration**.
3. The **Edit User Configuration** wizard appears. Select **Specify Synchronization Server** from the options on the left of the wizard screen.
4. Select an available domain controller or select **Any writeable domain controller**.
5. Click **OK** to save your changes.

   Depending on the setting you select, the next time users in the specified user configuration log on to Password Manager, they will bind to the newly designated domain controller or writeable domain controller.

CHAPTER 4

Documentation Errata

This chapter describes items that may have changed in the documentation released with Password Manager 4.1. For the most up-to-date information about Password Manager, visit the Product Documentation section of the Knowledge Center at the Citrix Web site at http://www.citrix.com.

Password Sharing Groups

Removing an application from a password sharing group. If an application is removed from a password sharing group, the application and credential information cannot later be again added to the password sharing group. [129976]

Agent Software

Suppressing agent software startup in a Citrix Presentation Server environment. In some situations, you may not want Password Manager to launch for certain published applications. In these cases, it is possible to enable SSOLauncher on an application-by-application basis. The process to enable SSOLauncher for specific applications requires disabling the default SSOLauncher behavior.

Caution Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

Make sure you back up the registry and update your Emergency Repair Disk (ERD) before you edit it.

To disable the default SSOLauncher behavior

1. Open Regedit.
2. Navigate to the key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup

3. Right click the AppSetup key and choose **Modify**.
4. Remove the following path in the string:

   C:\Program Files\Citrix\MetaFrame Password Manager\wts\ssolauncher.exe /nossoshutdown

Caution Remove only the path listed above, not the entire string.

Note This is the default location. If you installed Citrix Password Manager in a different location, your path is different.

5. Close Regedit.

After you disable the default SSOLauncher behavior, you can enable the SSOLauncher for Citrix published applications on a per-application basis.

Modify each published application's command line properties using the Citrix Management Console by highlighting the application(s), then selecting **Properties > Application Location** and modifying the command-line properties to read:

```
"C:\Program Files\Citrix\MetaFrame
PasswordManager\wts\ssolauncher.exe" /application
"C:\foldername\applicationname"
```

An example using Windows Notepad is:

```
"C:\Program Files\Citrix\MetaFrame Password
Manager\wts\ssolauncher.exe" /application "C:\Program Files"
```

The working directory does not change; continuing with the example above, it would be:

```
C:\Program Files
```

Ssolauncher.exe must come first in the command line. It needs to be started prior to the actual application launch. [128732]

Uninstalling Password Manager

Uninstalling the Password Manager Console. To uninstall the Password Manager Console, select Password Manager from the Add or Remove Programs wizard in the Control Panel of your server. Click **Change** to start the Citrix Password Manager Console Setup wizard. Select **Remove**, then click **Next** to begin the removal process. [129011, 125055]

Hot Desktop

Hot desktop in a Windows XP workgroup environment. If hot desktop is installed on a client device running Windows XP that belongs to a workgroup, the option for fast-user switching is disabled. [128930].

Managing User Data

Removing user data after the agent software is removed from a client device. When you uninstall the Password Manager agent software from a client device, some data remains on the client device; in some circumstances this data may cause a new installation of the agent software to direct a user to an incorrect central store in a multiple central store environment.

To prevent this from occurring, delete the .mmf files created for each user on the client device, as well as the HKEY_CURRENT_USER information for each user from the client device. [128293, 128929]